COST OF A CYBER INCIDENT: SYSTEMATIC REVIEW AND CROSS-VALIDATION

Publication: October 2020
Cybersecurity and Infrastructure Security Agency

Acknowledgements

We are grateful to Dr. Allan Friedman, Dr. Lawrence Gordon, Jay Jacobs, Dr. Sasha Romanosky, Matthew Shabat, Kelly Shortridge, Steven Surdu, David Tobar, Brett Tucker and Sounil Yu for the review comments and helpful feedback on the earlier draft of the report.

The authors would like to thank CISA staff for support and advice on this project.

Table of Contents

List of Tables

List of Figures

List of Acronyms

BAML	Bank of America Merrill Lynch
BEC	Business Email Compromise
CEA	Council of Economic Advisers
CI	Confidence Interval
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CSD	Cybersecurity Division
DBIR	Data Breach Investigations Report
DDoS	Distributed Denial of Service
DGP	Data Generating Process
EAC	Email Account Compromise
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Management Act
GDP	Gross Domestic Product
IC3	Internet Crime Complaint Center
IP	Intellectual Property
IRS	Internal Revenue Service
IT	Information Technology
OCE	Office of the Chief Economist
OPM	Office of Personnel Management
PCI	Payment Card Industry
PHI	Personal Health Information
PII	Personally Identifiable Information
PR	Public Relations
PRC	Privacy Rights Clearinghouse
PSA	Public Service Announcement
RBS	Risk Based Security
ROI	Return on Investment
SD	Standard Deviation
SEC	Securities and Exchange Commission
SIR	Self-insured Retention
SLTT	State, Local, Tribal, and Territorial

SMB	Small- and Medium-Sized Business
TVaR	Tail Value at Risk
VaR	Value at Risk
WEF	World Economic Forum

1. OBJECTIVES

This study is part of an analysis by the Cybersecurity and Infrastructure Security Agency's (CISA's) Office of the Chief Economist (OCE) to understand the impacts, costs, and losses from cyber incidents to enable cyber risk analysis and inform cybersecurity resource allocation decisions.

Given limited resources, important decisions must be made about how much the Federal Government should invest in cybersecurity. Furthermore, important decisions must be made about prioritizing prevention, detection, and other cybersecurity functions. In addition, resource allocation decisions require careful consideration regarding which assets and systems should be prioritized for improving cyber defenses and to what degree cybersecurity should be enhanced. Understanding the impacts and costs of eradication and recovery as well as the indirect losses from cyber incidents can help to inform these and other essential decisions.

The quantification of the financial value of avoidable losses is fundamental in an analysis supporting such decisions. This value can be weighed against the costs incurred to implement additional cybersecurity measures to minimize such losses, thus serving as a measure of the benefit of cybersecurity investment. For example, a cost-benefit analysis for vulnerability management could be informed by comparing the investment in vulnerability management with the number of vulnerabilities that investment identified and eliminated, the number of incidents those vulnerabilities could have enabled, impacts that would have ensued, and the range of costs and losses that would result from those incidents and associated impacts. Alternatively, the ratio of the investment in vulnerability management capabilities to the cost per incident can inform a break-even analysis, that is, the number of incidents and number of vulnerabilities that would need to be eliminated for the costs of the investment to break even with the costs and losses that would be avoided. In addition, there is a recognized incentive problem where vulnerability management vendors tend to overstate the severity and likelihood of the impacts resulting from the vulnerabilities surfaced by their specific tools. Therefore, discerning the likely impact of a particular vulnerability is often fraught with bias. This issue is not exclusive to the vulnerability management space, but extends to the cyber security industry in general, where vendor-provided estimates could benefit from more transparency and defensibility.

A prerequisite for a meaningful, evidence-based analysis of benefits is the availability of historical data on the impacts of cyber incidents as well as substantiated estimates of the associated costs and losses. Given the recognized challenge of data sparsity in this field (A.M. Best, 2018; Bermuda:Re+ILS, 2018; PwC, 2018; Romanosky et al., 2019), the purpose of this report is to conduct a systematic analysis of existing cyber incident cost studies and to document the loss estimates that could provide a defensible basis for evaluating loss avoidance.

The goal is to provide a systematic review that contains a thorough characterization of the current state of the literature and a meaningful synthesis of the published results. More specifically, OCE's analysis has three primary objectives. The first objective is to conduct an in-depth survey of the cyber loss literature and to identify the extent to which the costs of cyber incident losses have been tracked and analyzed within the private and public sectors. The second objective is to identify defensible estimates of cyber losses that are based on historical data and can be used to inform prospective analyses of cybersecurity investment benefits. The third objective is to clearly understand the limitations of the currently available estimates and identify a potential approach to resolving the informational and methodological gaps.

This report aims to compare and reconcile the estimates of cyber incident costs for three sets of studies (i.e., per-incident, national or sectoral, and hypothetical scenario-based) by analyzing hundreds of publications from multiple sources. In addition, the report pursues an explicit cross-validation of the loss estimates from secondary data sources with the primary cost and loss data independently collected by OCE for large and small cyber incidents.

OCE establishes a defensible set of estimates suitable for the analysis of federal-sector cyber incident costs by reconciling loss estimates in three sets of studies, conducting a detailed comparison of assumptions and limitations, and independently cross-validating cost and loss studies and commercial databases with data collected by OCE. The identification of suitable estimates will be supported by a detailed discussion of issues related to incident counts, scaling, and frequency data sources and a reconciliation with the aggregate loss and cost estimates at the national or sectoral level. The results of this analysis will serve as technical basis for quantifying cyber risk, and they will further provide a foundation for assessing the benefits of cybersecurity investment in the context of the mission of CISA's Cybersecurity Division (CSD).

A methodological discussion of CISA's approach to quantifying the potential losses and assessing the trade-offs is left for a subsequent technical report. The primary focus of this study is a systematic review of recent cyber incident cost and loss estimates available in the current literature on cybersecurity economics and investment, impact assessment, cyber risk management, and cyber resilience. A detailed description of the literature search and review protocol is included in Appendix A, Sources and Methods.

The remainder of the report is organized in the following manner. Section 2 present a summary of the results of the analysis. Section 3 summarizes the three major groups of studies and explains the assumptions, methodology, results, and limitations of the key studies that provide estimates of the per-incident costs, aggregate losses on the national scale, and cumulative losses for several pre-specified scenarios. Additionally, Section 3 discusses the short- and long-term market performance of breached companies. Section 4 contains a synthesis of defensible estimates suitable to support potential loss quantification across federal agencies and explains some of the issues with scaling per-incident estimates to reconcile with national aggregate impact estimates. Section 5 identifies the remaining challenges and provides potential solutions for resolving the methodological and informational gaps.

2. RESULTS IN BRIEF

To establish a defensible set of cost and loss data that is suitable for the analysis of cyber incident costs in the federal sector, this report analyzes three sets of cyber loss estimates. The first set includes per-incident estimates that heavily rely on a bottom-up analysis of cyber losses, which relies on statistical microdata (i.e., loss data per individual cyber incident for a large number of incidents) and is typically used in actuarial analyses to assess risk. The second set includes aggregate estimates of cyber losses at the national scale. These aggregate estimates are often used by cybersecurity vendors to urge investment in cybersecurity; however, such use of aggregate estimates of cyber losses often lacks explicit evidence on the effectiveness of the proposed products or a clear linkage between the proposed solution and the size of the problem it is intended to address. The third set of estimates are scenario-based and intended to emphasize extreme events and the potentially crippling magnitude of the resulting losses. OCE discusses the summary results for each set below.

Per-Incident Estimates

The datasets that contain the most relevant per-incident cost information are Advisen (cited in Romanosky [2016] and Cyentia [2020]), SAS OpRisk (cited in Biener et al. [2015]), Risk Based Security (RBS), and NetDiligence. A second set of sources includes industry studies commissioned by various organizations that attempt to gather similar information from entities directly impacted by adverse cyber activities. While the first four sources deal in microdata over an extended period of time, the industry reports and surveys typically offer snapshots and summary statistics only. A summary of the per-incident loss estimates across multiple sources

analyzed in this study is included in Table 1,[1] with the primary five datasets highlighted in gray (i.e., Advisen, Cyentia, SASOpRisk, NetDiligence, and RBS).

The average and median per-incident estimates both vary significantly across the primary datasets. The average per-incident cost in the commercial databases (i.e., those highlighted gray in Table 1), ranges from $394,000 to $19.9 million in the U.S. data and exceeds $40 million in the global data. The median estimate ranges from about $56,000 to almost $1.9 million.[2] Notably, losses from cyber incidents are significantly lower than losses from other operational risks such as improper business or market practices, disaster and other events, product flaws, theft and fraud (Biener et al., 2015; Romanosky, 2016). Only the most recent high loss magnitude events in Cyentia (2020) are starting to level with or exceed the operational losses in Biener et al. (2015).

The implications of the study findings are threefold: (1) the mean is not a good representation of cyber losses for the purposes of this analysis, as it is strongly impacted by extreme values; (2) losses from cyber and non-cyber risk events come from two different data generating processes (DGPs),[3] thus dictating the need to model, analyze, and manage cyber risks separately from other operational risks; and (3) the prioritization of resources towards cyber risk management will remain challenging as the empirical valuation of limited historical data on cyber losses show that other operational losses are a more dominant source of risk.

Although all of the sources presented in Table 1 attempt to collect primary data on the costs and losses of cyber incidents, the differences in the assumptions, approaches to data collection, and specific incidents included in the datasets result in a high degree of variability among the loss estimates. In addition to comparing the data sources, methodologies, assumptions, and limitations, this study includes a cross-validation of the analyzed data sources with the primary cost and loss data independently collected by OCE. Specifically, OCE's study explores the losses and cost-to-revenue ratios for large and small incidents, and it identifies a set of estimates that are suitable for the analysis of cyber incident costs in the federal sector as well as in the State, Local, Tribal, and Territorial (SLTT) community.

A clear understanding of the appropriate ranges of per-incident costs is essential for constructing a justifiable cost-benefit analysis to inform the decisions regarding future cybersecurity investment as well as to communicate the benefit of the CSD capabilities.

[1] Some of the studies had data that was granular enough to support segmentation into smaller subsets, (e.g., for the government sector or by organization size).
[2] The median is a mid-point of the dataset. That is, it indicates that costs for 50% of the incidents in the respective dataset fall below the shown number.
[3] The DGP is the true, underlying phenomenon that is creating the data.

Table 1: Summary of the Key Per-Incident Loss Estimates

Study	Data Subset	Number of Cases	Per-Incident Cost [a] ($ Thousands)		
			Mean	Median	Max
NetDiligence (2017)	U.S. Data	514	$394	$56	$16,849
NetDiligence (2018)	U.S. Data	1,201	$604	$61	$80,000
	SMB	1,011	$226	$55	$11,750
	Enterprise	82	$5,159	$1,000	$80,000
NetDiligence (2019)	SMB	2,003	$178	$48	$20,000
	Enterprise	78	$5,553	$1,000	$80,000
Romanosky (2016)	Advisen Full Dataset	921	$7,840	$250	$750,000
	Advisen Data Breach Subset	602	$5,870	$170	$572,000
	Advisen Public Sector Only	103	$1,990	$176	$39,000
Cyentia (2020)	Advisen Full Dataset	1,900	$19,100	$196	(>$1 B)
	Advisen Public Sector-Only	610	$13,000	$132	(~$1 B)
RBS (2018)	U.S. Dataset	252	$14,253	$609	$391,500
	Public-Sector Subset (Government & Education)	62	$2,569	$122	$86,300
	Government-Only Subset	38	$3,342	$200	$86,300
Biener et al. (2015)	SAS OpRisk North American Dataset	516	$19,860	$1,680	-
	SAS OpRisk Global Dataset	994	$40,530	$1,870	$89,560 [b]
Ponemon Institute (2017b)	U.S. Dataset	63	$7,350	-	-
	U.S. Dataset (Excluding Opportunity Costs)	63	$3,320	-	-
Ponemon Institute (2019)	U.S. Dataset	64	$8,190	-	-
	U.S. Dataset (Excluding Opportunity Costs)	64	$4,095 [c]	-	-
Kaspersky Lab (2017)	Enterprises (≥ 1,000 employees)	-	$1,336	-	-
	SMBs (50–999 employees)	-	$117	-	-
Kaspersky Lab (2018)	Enterprises (≥ 1,000 employees)		$1,630		
	SMBs (50–999 employees)		$149		
Cisco (2018a, 2019)	Enterprises	2,386	-	~$500	-
Cisco (2018b)	SMBs (< 250 employees)	1,816	-	-	-
Hiscox (2017)	SMBs (100 ≤ 250 employees)	-	$41	-	-
	Midsize Businesses (250–999 employees)	-	$81	-	-
	Enterprises (≥ 1,000 employees)	-	$102	-	-
Hiscox (2018)	SMBs (< 250 employees)	-	$5	-	-
	Midsize Businesses (250–999 employees)	-	$60	-	-
	Enterprises (≥ 1,000 employees)	-	$107	-	-

Note. "-" Not reported in the source.

[a] The loss estimates are as reported in the original source. OCE did not inflate the reported losses to a common dollar year because data on the duration over which the losses were accumulated is not reported.

[b] This cost reflects the 95th percentile instead of the maximum cost.

[c] In Ponemon Institute (2019), approximately 36% of the global breach cost was attributed to opportunity cost, diminished goodwill, abnormal customer turnover, customer acquisition costs, etc. However, a portion of the lost business cost is consistently higher in the U.S.-specific estimates (56% in 2017, 53% in 2018), but it is omitted from the 2019 Ponemon report. Thus, OCE applied 50% as a normalization factor for the 2019 estimate as a lower bound.

Aggregate Estimates

Special consideration should be taken to fully understand the context, underlying assumptions, and methodologies applied to estimate losses from cyber incidents on the national scale. A fundamental challenge is scaling per-incident loss estimates to assess past and future aggregate losses from malicious cyber activity in a manner that is defensible.

For historical losses, the issues are twofold. The first issue is the underreporting rate. Namely, only a portion of observed malicious cyber activity is publicly disclosed, yet no substantiating data or defensible bridging assumptions exist that would help to infer the fraction of observed cyber incidents that are not reported or publicly disclosed. The second issue stems from events which are not observed, that is, the challenge of extrapolating from the observed or reported incidents and associated consequences to the unobserved events and prevented consequences. Even with recent analytical advances in this space (e.g., Bisogni et al. [2017]), underreporting of detected incidents and the extrapolation to unobserved or undetected events complicate the estimation of aggregate costs and losses.

Projections of future potential losses suffer from additional analytical challenges. The first challenge is related to relying on historical frequency counts to inform the probability of various incidents—especially major ones. The second challenge is the inability to anticipate how adversaries will adapt to changes in the cybersecurity environment. Relying solely on observed counts and the anatomy of past incidents is not defensible as a basis for prediction, because the assumption that past adversary behavior predicts their future behavior does not hold. A separate debate on this subject raises questions on the applicability of the frequentist approach altogether and asserts that a game-theoretic framework is more appropriate for characterizing intelligent adversary and adaptive threats. Yet, if the frequency and conditional probability estimates required for a probabilistic approach present issues with defensibility, the parameterization of an adversary's utility functions in the game-theoretic framework is at least as problematic. In other words, while the implementation of game-theoretic or system dynamic approaches may theoretically appear more appropriate, their application has been fraught with a serious set of challenges. These challenges include determining an adversary's rationale, intentions, access to information, as well as an adversary's ability to understand and consistently make optimal, consequence-maximizing choices. Limitations in correctly understanding and accurately representing an adversary's behavior have implications for uncertainty and accuracy in applying these more advanced approaches (Ezell et al., 2010).

Recognizing these limitations upfront, OCE carefully examined and compared existing national cost and loss estimates and their underlying assumptions across multiple sources. Additionally, OCE separately analyzed the sources that could provide the basis for defensible scaling. OCE presents a summary of the aggregate estimates in Table 2.

The estimates vary widely depending on the estimation methodology and bridging assumptions. The aggregate annual estimates for U.S. impacts range from under $1 billion to over $242 billion, with some more extreme estimates reaching as high as $665 billion and even over $7 trillion. Estimates on the lower end of the range (i.e., those approximately in the $1 billion to $3.5 billion range) are based on historical data of complaints reported to the Federal Bureau of Investigation ([FBI], 2016, 2017; Internet Crime Complaint Center [IC3], 2017, 2019, 2020; Symantec, 2017). The highest national impact estimate, $7.7 trillion, appears in a study by the RAND Corporation (Dreyer et al., 2018). Not only is it the highest in the analyzed set of national estimates, but it is significantly higher than some of the highest global impact estimates (World Economic Forum [WEF], 2018; Bank of America Merrill Lynch [BAML], 2015; Cybersecurity Ventures, 2017, 2019). However, the study simulated a range of impacts, and this particular value is associated with the 95th percentile of the simulated distribution, while the national loss estimate of $665 billion represents the 75th percentile. A more moderate estimate, the median value of $242 billion, is much closer to the magnitude of estimates contained in McAfee studies and the White House Council of Economic Advisers (CEA, 2018) report.

To summarize, orders of magnitude separate the U.S. national loss estimates from the sources analyzed in this report. Also, there were both drastic adjustments in loss estimates from year to year from the same source (McAfee, 2013, 2014) as well as significant changes in sources, methodology, and loss estimates from version to version (McAfee, 2014, 2018; WEF, 2015, 2018). Such fluctuations and adjustments as well as distinctly different approaches to data collection and estimation methodology preclude the use of existing aggregate loss estimates—either at the sectoral or national level—as a cost or loss baseline for cost-benefit analysis. Thus, there will be a continuous need for developing bottom-up loss estimates tailored to specific research questions. However, these aggregate estimates can still serve both as anchor points in understanding the ranges of potential losses and for validating internally constructed bottom-up estimates.

The aggregate global estimates group and rank in approximately the same manner as the U.S. national estimates. The lower end of the spectrum is based on complaint data either reported to IC3 or estimated by IC3 based on other sources. The two highest global estimates, $3 trillion and $6 trillion, originate from the BAML (2015) and Cybersecurity Ventures (2017) studies. These levels of losses are difficult to reconcile with any other global estimates, as they are anywhere from 3 to 10 times higher than the rest. In fact, they are an order of magnitude above some of the highest global estimates for the hypothetical extreme scenarios (Lloyd's, 2015, 2017, 2018, 2019) which are summarized next.

Table 2: Summary of the Aggregate Loss Estimates (U.S. and Global)

Study	Data Subset	U.S. Annual Cost ($ billions)	Global Annual Cost ($ billions)		
			Lower	Best	Upper
Symantec (2017)	BEC-Only Subset [a]	~$1	-	-	-
FBI (2016, 2017)	BEC-Only Subset [b]	~$0.53	-	~$1.76	-
IC3 (2017)	BEC Subset	-	-	$0.676	-
	Cyber Subset	-	-	$0.980	-
	Total Dataset	-	-	$1.420	-
IC3 (2019)	BEC Subset	-	-	$1.298	-
	Cyber Subset	-	-	$1.885	-
	Total Dataset	-	-	$2.706	-
IC3 (2020)	BEC Subset	-	-	$1.7	-
	Cyber Subset	-	-	-	-
	Total Dataset	-	-	$3.5	-
Norton (2015)		$28.9	-	$150.0	-
Norton (2016)		$20.3	-	$125.9	-
Norton (2017)		$19.4	-	$172.0	-
McAfee (2013)		$24–$120	$300	-	$1,000
McAfee (2014)		~ $100	$375	$445	$575
McAfee (2018) [c]		$134–170	$445	-	$600
Symantec (2016)			-	$575	-
CEA (2018)		$57–$109	-	-	-
RAND Corporation (Dreyer et al., 2018)	25th percentile	$27.8	-	-	-
	50th percentile	$241.9	-	-	-
	75th percentile	$665.0	-	-	-
	95th percentile	$7,710.0	-	-	-
WEF (2015)		$100	$100	-	$500
WEF (2018)		-	-	$1,600	-
BAML (2015)		-	-	$3,000	-
Cybersecurity Ventures (2017, 2019)		-	-	$6,000 (2021 projected)	-

[a] The average annual U.S. cost was calculated by dividing Symantec's (2017) estimated cost of $3 billion from 2013 to 2016 by 3 years.
[b] The average annual U.S. and global cost was calculated by dividing the FBI's (2017) estimated cost of $1.59 billion and $5.3 billion, respectively, from October 2013 to December 2016 by 3 years.
[c] McAfee's (2018) study reports North American loss estimates ($140–$175 billion) instead of U.S. losses. However, OCE derived the U.S.-specific estimate by applying the cybercrime loss rate as share of gross domestic product (GDP; 0.69% to 0.87%) reported in McAfee (2018) to the U.S. 2017 GDP of $19.52 trillion (BEA, 2020).

Scenario-Based Estimates

The highest magnitude of the loss estimates associated with malicious cyber activity are contained in scenario-based risk studies such as Lloyd's (2015, 2017, 2018, 2019). The extreme scenarios are intentionally defined to demonstrate substantial depth, breadth, and propagation of potential consequences in order to illustrate the full magnitude of the possible damages. The emphasis is not on the likelihood of such a scenario, but rather to demonstrate the possibility of crippling magnitudes of exposure. Furthermore, the profound degree of risk accumulation in such an extreme scenario is not necessarily fully accounted for or understood by all the players in the cyber insurance markets as indicated by the current approach to computing insurance premiums and cyber insurance rate schedules (Romanosky et al., 2019).

A more detailed list of 25 scenarios exploring extreme cyber losses and risk accumulation, including industrial control systems impacts, is presented in Coburn et al. (2018). This group of studies illustrates the degree of the probable maximum loss and emphasizes the gaps between the size of the current cyber insurance premiums and the levels of potential losses if a particular scenario were to materialize. For example, Lloyd's (2017) estimated the potential losses for two cyber incident scenarios and found that the insurance gap ranged between $4 billion and $45 billion for a cloud service outage scenario and $8.9 billion to $26.6 billion for a mass vulnerability scenario. This implies that only 13% to 17% of losses were covered in the first scenario and only 7% were covered in the second scenario.

OCE analyzes Lloyd's (2015, 2017, 2018, 2019) studies, which are some of the most often-cited reports, as examples of scenario-based exposure studies. OCE presents a summary of Lloyd's scenario-based estimates in Table 3.

The estimates range from $2.8 billion to $1.0 trillion per event for the United States and from $4.6 billion to $193.0 billion on the global scale. The degree of impacts is determined by the nature of the event as well as the assumed severity, duration, and boundary of the consequences. Hypothetical scenarios that involve critical infrastructure, such as the power grid, tend to produce significantly higher estimates because of the scenario-specific assumptions. For example, the damage estimates from a single hypothetical power blackout event (Lloyd's, 2015) surpass the magnitude of the aggregate global losses from cyberattacks in McAfee (2014, 2018) that were presented in Table 2. However, Lloyd's scenario assumes malware would impact 50 generators leading to overload and burnout, which in turn is assumed to destabilize the regional grid of the Northeastern United States and cause sustained prolonged outages.

The objective of these intentionally severe scenarios is to explore extreme losses and risk accumulation. They aim to draw attention to the distinct possibility of high-consequence, low-probability cyber incidents. Thus, they are constructed with hypothetically high rates of depth, breadth, and propagation to illustrate a severe but plausible magnitude of consequences. Since the resulting impacts are extreme by design, these estimates do not constitute a defensible benchmark or baseline level of losses to serve as a standalone basis for return on investment (ROI) or cost-benefit analysis. However, they are informative for understanding the worst-case outcomes that would result in profound risk accumulation, thus highlighting the systemic risks.

Table 3: Summary of the Scenario-Based Loss Estimates

Study	Analyzed Scenario	Per-Scenario Impact ($ billions)		Region
Lloyd's (2015). *Business Blackout: The insurance implications of a cyberattack on the U.S. power grid*	Three scenarios for a single blackout event that vary by severity and duration	Scenario 1 Scenario 2 Scenario 3	$243 $544 $1,024	U.S.
Lloyd's (2017). *Counting the cost: cyber exposure decoded*	Two incident scenarios: cloud service provider hack, mass vulnerability attack. Event estimates across multiple countries for varying event severity.	Cloud Hack: Low 95% CI High 95% CI Vuln. Attack: Low 95% CI: High 95% CI:	$4.60–$53.05 $1.60–$10.85 $15.62–$121.41 $9.68–$28.72 $4.12–$15.63 $20.50–$34.22	Global
Lloyd's (2018). *Cloud down: Impacts on the U.S. Economy*	Three scenarios of outages by the largest cloud service providers (0.5–1 days; 3–6 days, 5.5–11 days).	Scenario 1 Scenario 2 Scenario 3	$2.8–$5.9 $6.9–$14.7 $11.2–$23.8	U.S.
Lloyd's (2019). *Bashe attack: Global infection by contagious malware*	Three scenarios for global malware infection	Scenario 1 Scenario 2 Scenario 3	$85 $153 $193	Global

Note. CI = confidence interval. Sources: Lloyd's (2015, 2017, 2018, 2019)

3. ANALYSIS

There is a growing body of literature dealing with cyber risk assessment and risk management. This literature identifies the lack of cost data for cyber incidents as a key obstacle to analyzing cybersecurity investment and risk management policies as well as establishing a well-functioning and transparent cyber insurance marketplace (A.M. Best, 2018; Bermuda:Re+ILS, 2018; PwC, 2018; Romanosky et al., 2019).

The few studies that attempt to explore the costs of adversarial cyber activity provide estimates that vary widely. The impacts of cyber incidents include loss of confidentiality, availability, or integrity, which in turn result in various degrees of direct and indirect costs and losses. Costs represent additional expenditures or resource requirements necessary to deal with the consequences of cyber incidents. Losses capture a subset of negative impacts that do not necessarily require immediate expenditures, but rather represent such damages as downtime, lost revenue, or loss of budget or mission. Cost and loss estimates provided in the reviewed literature range from $3.5 billion in IC3 (2020) to $3 trillion in BAML (2015). The magnitudes of these estimates diverge significantly across the reviewed sources depending on the methodology, assumptions, level of aggregation, and depth and breadth of the analysis.

Groups of Studies

After reviewing a broad range of cyber cost and loss studies, natural groupings have emerged. Most of the relevant sources containing cost estimates can be broken down into the following groups:

1. Per-incident loss estimates based on insurance claims, payout data, and activity-based incident cost estimates
2. Aggregate loss or impact estimates on the national scale
3. Academic or research papers on the short- and long-term impacts of cyber incidents
4. Individual case studies with scenario-based impact estimates

Studies with per-incident cost and loss estimates based on the insurance claims, cyber event payouts, and loss micro-data contain the most value, as they provide the empirical foundation that is essential for a defensible quantification of potential losses from cyber incidents. These studies include Romanosky (2016), Cyentia (2020), NetDiligence (2017, 2018, 2019), RBS (2018), Ponemon Institute (2013–2018), Accenture and Ponemon Institute (Richards, et al., 2017; Bissell et al., 2019), Kaspersky Lab (2016b, 2017, 2018, 2019), Cisco (2017, 2018a, 2018b, 2019), Hiscox (2017, 2018), Symantec (2016, 2017), Biener et al. (2015), and Deloitte (2016).

Industry, vendor, government, and research reports with aggregate cost and loss estimates either contain internally developed cyber loss and impact estimates or cite external data to support their assumptions. These types of studies enhance the understanding of cyber loss magnitudes on the national and global scale. While they may have limited applicability for forward-looking simulations to support specific cybersecurity portfolio allocation decisions, they nevertheless add significant value by providing additional data for anchoring the assumptions, informing parametrization, and more importantly, validating the boundary points for aggregate losses. The studies in this group include McAfee (2013, 2014, 2018), WEF (2015, 2016, 2017, 2018, 2019), Symantec (2016, 2017, 2018), Cybersecurity Ventures (2016, 2017, 2018, 2019), Norton (2015, 2016, 2017, 2018), the RAND Corporation (Dreyer et al., 2018), and the CEA (2018).

The most relevant academic and research papers dealing with the impacts of cyber incidents take an in-depth look at short- and long-term market performance in an attempt to identify and quantify significant changes in the market value of affected entities following an incident disclosure. A common theme in this group of studies is an investigation of the fluctuations in stock values immediately following a cyber incident disclosure. While a significant change may be initially detected, market performance over a longer-term horizon seems to rebound to pre-incident levels.

OCE notes three caveats to the conclusions about long-term market performance. First, these studies track the long-term performance of a handful of larger entities that have experienced a serious incident. However, the cyber incident costs as a share of revenue are not as significant, especially when compared with other types of fraud and financial losses typically experienced by such entities. Second, it is hard to make a case about long-term market performance without a control group. In addition, it is hard to decouple the effects of cyber incidents from other market factors that may have contributed to the deteriorated or improved stock performance over the long-term horizon. Third, there are attribution considerations that complicate the analysis. Tracing the impacts to the cyber incident may be less meaningful in cases where a cyber incident may not have been an isolated event, but rather an amplification of existing managerial inefficiencies. For example, less mature cybersecurity practices may be one of many symptoms of operational shortcomings. In practice, decoupling these factors is problematic not just in the cybersecurity field, as the question of impact attribution remains a consistent challenge in multiple domains beyond cyber. The most relevant research on this topic includes Kvochko and Pant (2015), Campbell et al. (2003), and Hilary et al. (2016).

Individual case studies exploring the impacts of cyber incidents for a pre-defined set of scenarios are an additional source of valuable estimates that allow for a better understanding of variability in potential losses, and as a result, the magnitude of risk. In general, the magnitude of impacts in this group of studies is higher than in the three previously mentioned groups. To properly reconcile the results for the individual case studies with the rest of the literature, it is important to understand the motivation for these studies as well as the severity of the assumed scenarios. Studies in this group share a common objective of emphasizing the aggregate level of cyber

risk that is not necessarily fully understood, because the current state of cyber risk quantification practices is limited. Key limitations include the sparse data on losses, underreporting of the incidents, lack of visibility into cybersecurity practices, and, as a result, a constrained understanding of the current cybersecurity baseline across multiple sectors and agencies. Thus, weak patterns of association among the assets, employed controls, and potential losses, among other factors, result in the continued underestimation of the cumulative exposure. Lloyd's (2015, 2017, 2018, 2019) studies are some of the most often-cited examples of scenario-based exposure studies.

The Sections 3.1 through 3.4 of the report examine the most notable studies within each group. Summary tables and reconciliation of the aggregate results are also provided to further illustrate the state of the impact estimates within the existing literature. In addition, in these sections, OCE reviews the sources that contain analysis of incident frequencies and discusses the implications of relying on these frequencies for scaling per-incident losses to the sectoral, national, or global level.

Note that all of the costs presented in this report are as they were originally reported in each study. OCE did not inflate them into a common dollar year because typically, the final tally of costs and losses is not known within the year the incident took place. Also, losses occur and accumulate over several years after the incident, especially if litigation and class action suits are involved.

3.1. Per-Incident Cost and Loss Estimates

This section contains a summary of the per-incident loss estimates available in the most widely cited published research, commercial datasets, and industry reports. It is followed by a validation step that included collection of the per-incident cost data from the open sources to compare it with the ranges of the estimates in the commercial datasets and industry reports. Reconciliation of the per-incident estimates from the analyzed studies with the primary data collected by the OCE for large and small incidents is also included in the discussion. A separate overview of the per-record cost estimates concludes the per-incident cost analysis section. A summary of the most relevant per-incident cost estimates is presented in Table 4.

A common characteristic of the five key commercial datasets containing incident cost records (i.e., those highlighted gray in Table 4) is that data breaches are the most represented incident type despite the attempt to cover various incident types as part of the data collected. Data breaches typically get more attention in datasets because breaches are more frequently disclosed and reported. State data breach notification laws and sector-specific requirements make it easier to find information about data breaches relative to other types of cyber incidents. Incidents associated with the loss of integrity or availability are not as readily disclosed and, as a result, are underrepresented in currently available datasets.

Of the cyber loss estimates from the five key commercial datasets, the lowest estimates for both the median and mean cyber losses per incident ($56,000 and $394,000, respectively) were provided by NetDiligence (2017). NetDiligence's estimates were developed based on case records for both incident totals and cyber insurance claims from underwriters.

Romanosky's (2016) estimates are based on the Advisen data, where the estimates have a slightly higher median and mean across all incident types, approximately equal to $250,000 and $7.8 million, respectively. Data breaches were the most prevalent type of incident in the Advisen data with available cost data. For the data breach subset, the median and mean estimates are slightly lower, at $170,000 and $5.9 million, respectively. For Advisen's government-sector subset—which covers all incident types with available data, not just data breaches—the median ($176,000) is about the same as in the data breach subset, while the mean ($2 million) is lower.

Although the Ponemon Institute's (2017b) average loss per incident (including opportunity costs) is close to Romanosky's (2016) estimate based on the full dataset in magnitude at $7.35 million in 2017 and $8.19 million in 2019, it includes opportunity costs which are typically not allowed in damage assessments. Excluding opportunity costs from the Ponemon Institute's (2017b) average U.S. estimate brings the per-incident average down to $3.3 million.

In Ponemon (2019), approximately 36% of the global breach cost was attributed to opportunity cost, diminished goodwill, abnormal customer turnover, customer acquisition costs, etc. However, a portion of the lost business cost is consistently higher in the U.S.-specific estimates (56% in 2017, 53% in 2018), but it is omitted from the 2019 Ponemon report. Thus, OCE applied 50% as a normalization factor for the 2019 estimate as a lower bound. This brings the adjusted U.S. per-incident cost from approximately $8.19 million down to $4.1 million.

Cyentia (2020) is an updated estimate derived from 2009–2010 Advisen data. Cyentia's loss magnitude analysis shows that the median cost in this most recent dataset is $196,000 per breach, which is higher than the median cost ($170,000) reported in the older edition of Advisen analyzed in Romanosky (2016). The report emphasizes the heavy-tailed distribution of the loss magnitude data and explains in detail why using arithmetic mean is misleading. While the average loss is about $19.1 million, 90% of the breaches cost less. As expected, median loss magnitude varies significantly by sector. The public sector has the lowest median per-incident cost of $132,000, which is lower than the median cost for public sector in the older 2005–2015 Advisen dataset ($176,000).

Table 4: Summary of the Key Per-Incident Loss Estimates

Study	Data Subset	Number of Cases	Per-Incident Cost [a] ($ Thousands)			
			Mean	Standard Deviation	Median	Max
NetDiligence (2017)	U.S. Data	514	$394	$1,531	$56	$16,849
NetDiligence (2018)	U.S. Data	1,201	$604	$3,568	$61	$80,000
	SMB	1,011	$226	-	$55	$11,750
	Enterprise	82	$5,159	-	$1,000	$80,000
NetDiligence (2019)	SMB	2,003	$178	$852	$48	$20,000
	Enterprise	78	$5,553	$12,334	$1,000	$80,000
Romanosky (2016)	Advisen Full Dataset	921	$7,840	$47,280	$250	$750,000
	Advisen Data Breach Subset	602	$5,870	$35,700	$170	$572,000
	Advisen Government-Only Subset	103	$1,990	$5,720	$176	$39,000
Cyentia (2020)	Advisen Full Dataset	1,900	$19,100	-	$196	(>$1 B)
	Advisen Public Sector-Only	610	$13,000	-	$132	(~$1 B)
RBS (2018)	U.S. Dataset	252	$14,253	$52,834	$609	$391,500
	Public-Sector Subset (Government & Education)	62	$2,569	$11,297	$122	$86,300
	Government-Only Subset	38	$3,342	$14,021	$200	$86,300
Biener et al. (2015)	SAS OpRisk North American Dataset	516	$19,860	-	$1,680	-
	SAS OpRisk Global Dataset	994	$40,530	$443,880	$1,870	$89,560 [b]
Ponemon Institute (2017b)	U.S. Dataset	63	$7,350	-	-	-
	U.S. Dataset (Excluding Opportunity Costs)	63	$3,320	-	-	-
Ponemon Institute (2019)	U.S. Dataset	64	$8,190	-	-	-
	U.S. Dataset (Excluding Opportunity Costs)	64	$4,095	-	-	-
Kaspersky Lab (2017)	Enterprises (≥ 1,000 employees)	-	$1,336	-	-	-
	SMBs (50–999 employees)	-	$117	-	-	-
Kaspersky Lab (2018)	Enterprises (≥ 1,000 employees)		$1,630			
	SMBs (50–999 employees)		$149			
Cisco (2018a, 2019)	Enterprises	2,386	-	-	~$500	-
Cisco (2018b)	SMBs (< 250 employees)	1,816	-	-	-	-
Hiscox (2017)	SMBs (100 ≤ 250 employees)	-	$41	-	-	-
	Midsize Businesses (250–999 employees)	-	$81	-	-	-
	Enterprises (≥ 1,000 employees)	-	$102	-	-	-
Hiscox (2018)	SMBs (< 250 employees)	-	$5	-	-	-
	Midsize Businesses (250–999 employees)	-	$60	-	-	-
	Enterprises (≥ 1,000 employees)	-	$107	-	-	-

[a] The loss estimates are as reported in the original source. OCE did not inflate the reported losses to a common dollar year because data on the duration over which the losses were accumulated is not reported.
[b] This cost reflects the 95th percentile instead of the maximum cost.

The lowest average cost per incident is contained in Kaspersky Lab (2017, 2018), with the average total incident cost for small- and medium-sized businesses (SMBs) at $117,000 and $149,000 respectively. The highest median and mean cost per incident are reported in Biener et al. (2015), which are derived based on the cyber-relevant risk observations in the SAS OpRisk Global dataset of operational losses. The median estimate in the North American data is about $1.68 million, with the mean of approximately $19.9 million. The more recent high loss events appearing in the updated Advisen dataset analyzed in Cyentia (2020) increased the averages to $19.1 million, thus coming close to averages for cyber events in Biener et al. (2015).

Note that the high magnitude of the estimates in the SAS OpRisk is not indicative of increased costs of cyber incidents. A more likely reason is a change in the data collection bandwidth, with a shift in data collections focusing more on larger incidents. Larger incidents typically gain more media attention, making the loss estimates more easily available in the open sources. Thus, the result is a relatively lower resource requirement associated with the data collection, but a narrower coverage with focus on larger incidents.

The implications of the study findings are threefold: (1) the mean is not a good representation of cyber losses for the purposes of this analysis, as it is strongly impacted by extreme values; (2) losses from cyber and non-cyber risk events come from two different DGPs, thus dictating the need to model, analyze, and manage cyber risks separately from other operational risks; and (3) the prioritization of resources towards cyber risk management will remain challenging as the empirical valuation of limited historical data on cyber losses show that other operational losses such as improper business practices, theft and fraud, product flaws, disaster and other events are a more dominant source of risk.

3.1.1. Cross-Validation: Primary Loss Data for Large and Small Incidents

In the subsequent sections, the per-incident estimates discussed in Section 3.1 are compared and validated with some of the primary data collected by the OCE from open sources as part of this analysis. Because it is recognized in the literature that cyber losses follow a DGP with a heavy-tail distribution, OCE collected additional data on large incidents to explore and anchor some of the tail values.

Another recognized gap in the cyber loss analysis is a lack of data for the types and scale of incidents that would be more relevant for the public sector and SLTT governments. OCE's study collected primary data from open sources regarding state-, county-, and city-level incidents as well as incidents at state schools and other public institutions. OCE's objectives are to (1) get a better understanding of the scale of costs and losses for this subset of incidents and (2) validate if the loss levels described in the key studies and commercial datasets analyzed in Section 3.1 are of the appropriate magnitude and range to support the analysis not only for federal departments and agencies, but also for SLTT stakeholders.

Large Incidents

Section 3.1 focused on the most relevant per-incident cost studies that matched OCE's search criteria. To further the understanding of the cost variability and validate the content of some of the commercially available loss datasets, OCE took a more detailed look at the 12 largest incidents that drew significant media attention over the past several years.

Typically, these incidents are treated as outliers and excluded from analyses. Recognizing that data are sparse, instead of discarding or caveating the large incidents, OCE specifically pursued additional information on this subset of incidents to better inform the analysts about the observations forming the heavy tail of the loss distribution.

There is no standardized approach or harmonized cost taxonomy that enables cohesive quantification and tracking of costs and losses to inform damage assessments. OCE relied on an activity-based costing approach

and searched open sources for the most recent partial estimates. These partial estimates were subsequently combined into an itemized total of the overall incident costs.

An overview of the large incidents and the table with itemized cost estimates per incident is contained in Appendix C along with the sources used to estimate the costs. A summary of the total cost estimates for the largest 12 incidents, along with the cost as a percentage of the annual revenue in the year of the incident, and the number of people affected is presented in Table 5.

Table 5: Costs, Cost-to-Revenue Ratios, and People Affected (Large Incident Sample)

Company Affected	Year of Incident	Total Cost ($ million)	Cost-to-Revenue Ratio	Number of People/Records Affected (millions)	Primary Source
Anthem	2015	375.5	0.48%	78.8	Anthem (2015)
Yahoo	2014	350	7.58%	500	Armerding (2018a)
Merck	2017	310	0.78%	-	Gunderman (2017)
Target	2013	292	0.41%	70	Armerding (2018a)
Home Depot	2014	252	0.30%	56	Armerding (2018b)
Sony PlayStation	2011	171	0.20%	101.6	*Sony Agrees* (2014)
Equifax	2017	164	4.88%	145.5	Equifax (2018)
Sony Pictures	2014	43	0.06%	0.047	Armerding (2018b)
Experian	2015	20	0.42%	15	Experian (2016)
Yahoo	2013	16	0.34%	1,000	Jay (2017)
Ashley Madison	2015	12.8	11.74%	37	Stempel (2017)
LinkedIn	2012	4	0.41%	6.5	Lennon (2017)

Note. The primary source column presents the primary source used to construct the total cost estimate. See Appendix C for additional details.

Most of these incidents were selected as some of the largest incidents in the Privacy Rights Clearinghouse (PRC; 2018) breach database (based on breach size), among the breaches with available breach size data.[4]

Specifically, for the 7,677 breaches included in the PRC database, 2,210 either have no entry or a 0 in the total records breached field. For the remaining 5,467 breaches, the median number of records breached was 2,200, with a mode of 1,000 records. The PRC has 468 incidents with at least 100,000 records stolen.

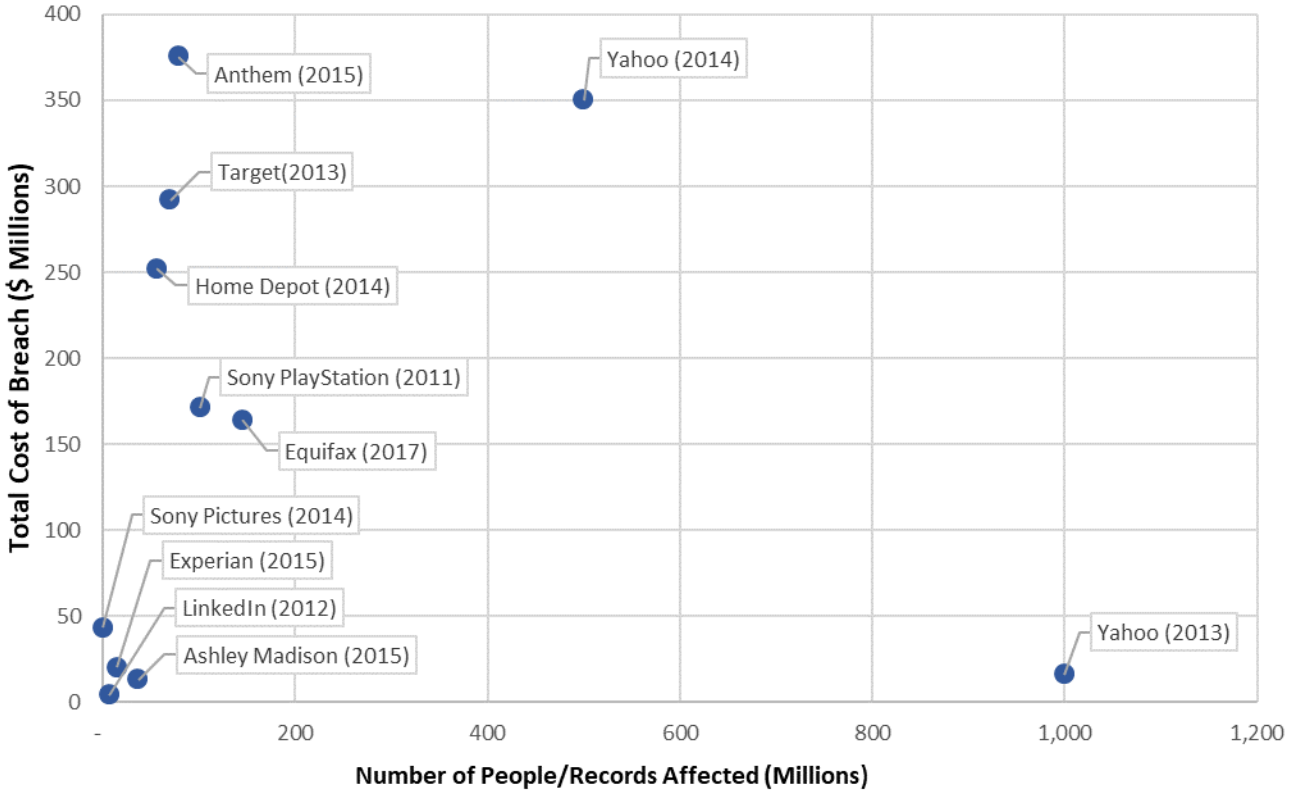
Because this is a convenience sample of self-reported estimates available in the public domain, the usual caveats about the non-representativeness of the sample and the lack of statistical significance to support formal statistical inference to the rest of the large incidents apply here as well.

Losses for the largest breaches ranged from $4 million for LinkedIn to almost $376 million for Anthem, affecting anywhere from 47,000 people in the Sony 2014 breach to approximately one billion affected individuals for the Yahoo 2013 breach.

[4] This report uses incident definition from National Institute of Standards and Technology (2012) Special Publication 800-61r2 Computer Security Incident Handling Guide. A breach is defined as an incident that resulted in an exfiltration of information.

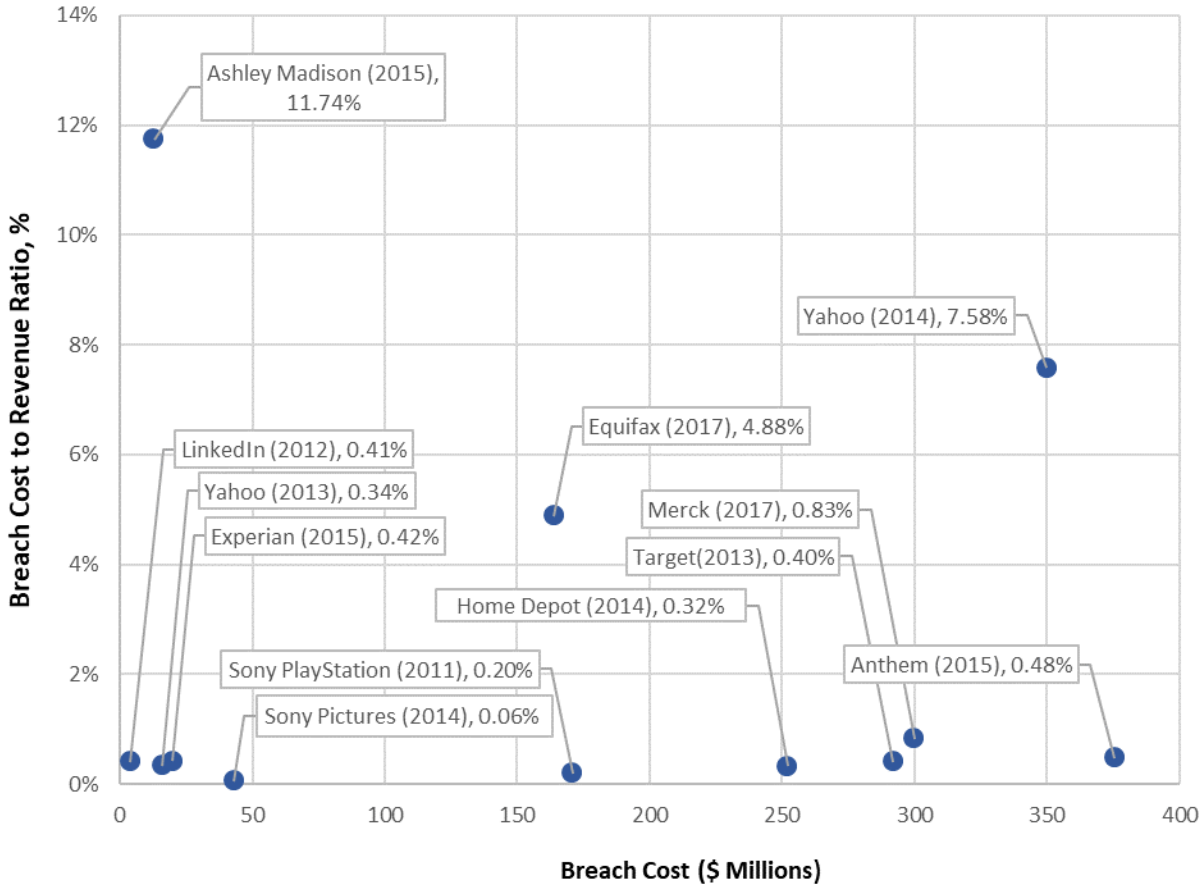
In Figure 1, OCE plots the cost of each of the largest breaches against the size of each breach (in terms of the number of people affected). As presented in Figure 1, breach cost is not strongly correlated with breach size. The weak association between the two factors implies that relying on per-record estimates to approximate total breach costs is not appropriate for very large breaches.

Figure 1: Breach Cost Versus Breach Size for the Largest Incidents



Besides breach size, another key aspect of the cost analysis is the relationship between the cost of the incidents and the cost-to-revenue ratio for the company. In Figure 2, OCE plots the costs of the 12 largest incidents along with the corresponding cost-to-revenue ratios for the affected company.

Figure 2: Cost-to-Remove Ratio Versus Breach Cost for the 12 Largest Incidents



For most of the large incidents in the analyzed group, the ratio of the incident cost to annual revenue did not exceed 1%. This aspect of low cost-to-revenue ratios for the largest breaches was discussed in detail and emphasized for the Target, Home Depot, and Sony incidents in Hackett (2015). More specifically, 8 of the 12 largest incidents had a cyber incident cost-to-revenue ratio close to or below 0.5%. For context, the average retail shrinkage cost (i.e., the cost of shoplifting, employee theft, paperwork errors, and supplier fraud) ranges between 1.38% and 1.85% of sales for the United States (National Retail Foundation, 2018; Wassel, 2018). This finding is consistent with the results in Biener et al. (2015) that show that cyber risk-related losses are significantly lower than losses from other operational risks. In addition, the most recent discussions on cyber losses and the threshold of materiality seem to indicate that the guidelines for materiality internally established by the Big 4 accounting firms range from 2% to 10% of revenue (Freund, 2020). Therefore, the cost-to-revenue ratio provides an important dimension for the loss analysis because some of the incidents with the largest loss magnitude in absolute terms may not reach the materiality threshold in relative terms.

It could be argued that such small ratios of incident costs to operating budgets or revenue is characteristic only of incidents that occur at large companies. OCE explores this aspect further in the next section on smaller incidents.

Smaller Incidents

To explore if the costs of incidents comprise a very small percentage of annual revenue only for large companies or if smaller entities also experience small cost-to-revenue ratios similar to large companies, OCE searched open sources for itemized cost estimates of smaller-scale incidents. This targeted collection of itemized cost data

allows OCE to understand the variability of costs and losses by individual cost category for smaller entities. The summary of the results is presented in Table 6.

Table 6: Costs, Cost-to-Revenue Ratios, and People Affected (Smaller Incident Samples)

Entity	Total Cost ($ millions)	Cost-to-Budget Ratio [a]	Number of People/Records Affected [b] (millions)	Primary Source [c]
Internal Revenue Service (IRS)	$30.00	0.23%	0.10	Rubin & Belkin (2017)
Maricopa County Colleges	$26.02	3.64%	2.00	Faller (2014)
South Carolina's Department of Revenue	$12.13	0.05%	0.40	Shain (2015)
Michigan State University	$9.40	0.22%	0.40	Weidmayer (2016)
State of Utah, Medicaid Server	$9.00	0.08%	0.78	Insurance Journal (Associated Press, 2013)
NationWide Insurance	$5.50	0.03%	1.27	Gallagher (2017)
Ohio State University	$4.00	0.08%	0.76	Book et al. (2010)
Bank of New York Mellon	$3.63	0.03%	0.641	State of Connecticut Department Of Banking (2009)
Rosen Hotels & Resorts	$2.34	N/A	Unknown	Brinkmann (2017)
Ingham County, MI	$1.46	0.63%	Unknown	Lacy (2017)
Georgia, State voters' data	$1.20	0.06%	6.00	Torres (2015)
Wisconsin Department of Revenue	$1.00	0.02%	0.17	Levin (2012)
Allentown, PA	$1.00	0.92%	Unknown	Blake (2018)
Orange County Transportation Authority	$0.66	0.01%	N/A	Gerda (2016)
City of Fort Lauderdale	$0.43	0.08%	N/A	Barszewski (2015)
Ferris State University	$0.38	0.13%	0.06	McVicar (2013)
Madison County, Indiana	$0.24	0.83%	N/A	Ragan (2016)
Cuesta College, San Luis Obispo	$0.16	0.34%	N/A	Lambert (2015)
University of California, Berkeley	$0.15	0.01%	0.002	Schaffhauser (2014)
University of Central Florida	$0.11	0.01%	0.06	Russon (2016)
Anderson County, TN	$0.10	0.38%	0.002	Huotari (2016)

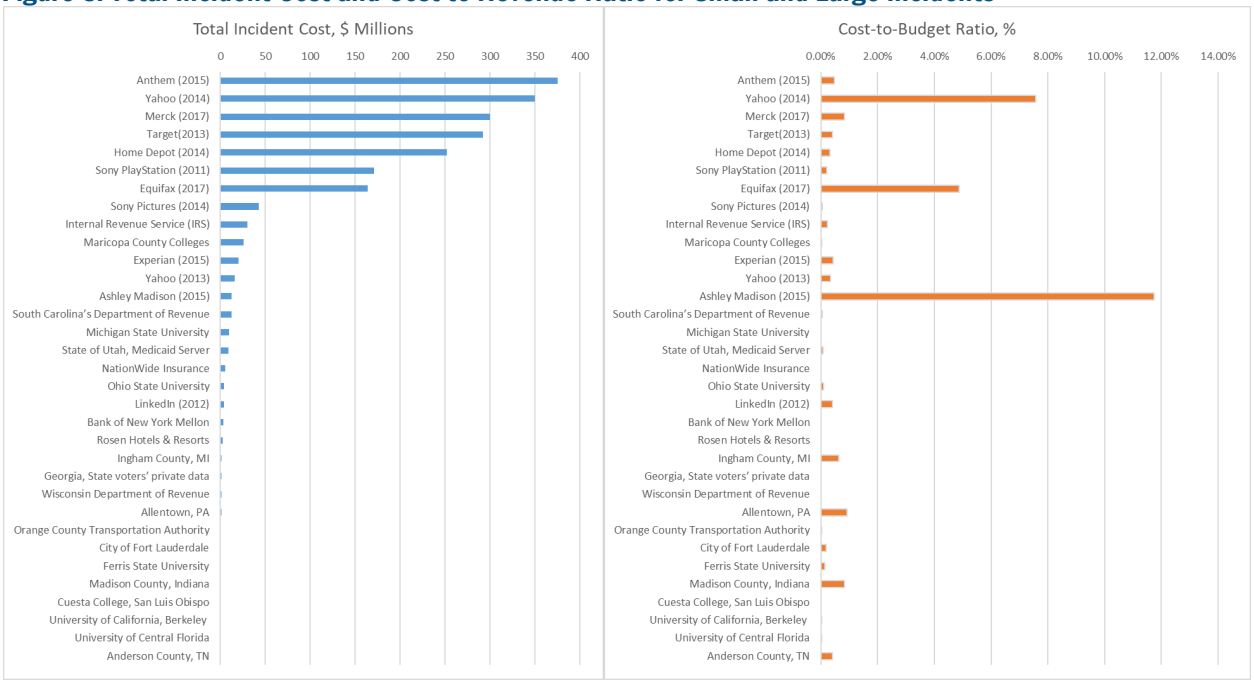
[a] This is calculated as the cost of an incident as a percentage of the annual operating budget.
[b] "Unknown" means a metric other than number of records specified, and "N/A" means no records were breached, but an incident that required cleanup still occurred.
[c] The primary source column presents the primary source used to construct the total cost estimate. See Appendix D for additional details.

While the incident costs range anywhere from $100,000 to $30 million, all of the 14 spot-checked smaller incidents had an incident cost-to-budget ratio below 1%. Moreover, 10 of the 14 spot-checked incidents had cost-to-budget ratios below 0.25%.

An additional point of interest to OCE was investigating the cost ranges for incidents relevant to state and local governments from the perspective of scale, type of the incident, targeted entity, and comparable operating budgets. An overview of the smaller, state and local government incidents is contained in Appendix D.

For comparison, total incident cost and cost-to-revenue ratio for both small and large incidents are presented side by side in Figure 3 below.

Figure 3. Total Incident Cost and Cost-to-Revenue Ratio for Small and Large Incidents



This spot-check or cross-validation is consistent with the results presented in the RAND Corporation study (Dreyer et al., 2018) for bootstrapped Advisen (2015) data.[5] The RAND Corporation study will be discussed in detail further in Appendix B, but for benchmarking purposes, it should be noted that 75% of the bootstrapped cost-to-revenue ratios for public-sector incidents in the RAND Corporation report fall under 0.2% of the revenue or operating budgets. The cost-to-revenue ratio in the underlying Advisen subset for the public sector is 0.8% for the 75th percentile, and approximately 2% for the 85th percentile. The median cost-to-revenue ratio across all of the sectors is 0.37%.

The highest cost incident in the cross validation sample is the IRS incident at $30 million (see Table 6). The reason for including the IRS in OCE's list is its comparable loss scale to the Maricopa County Colleges at $26 million and South Carolina Department of Revenue at $12 million.

Essentially, this spot check and overview of the smaller incidents across federal and state governments, state educational institutions, and county entities validates the scale of costs for the public sector in the Advisen and

[5] A more detailed description of the RAND analysis is included in Appendix B. Advisen data is resampled to form distributions of costs and distributions of loss ratios for various sectors of the economy in order to estimate the aggregate impact on the national GDP.

RBS datasets, as well as for the results of the NetDiligence (2017–2019) studies. Because these data points have been validated, OCE deems it appropriate to use these loss estimates for incidents of similar nature at the SLTT level and state educational institutions in future analyses. Therefore, the per-incident cost estimates discussed in Section 3.1 capture the variability of losses at the SLTT level and could support a bottom-up, activity-based costing analysis of cyber incidents and their associated losses for the SLTT community.

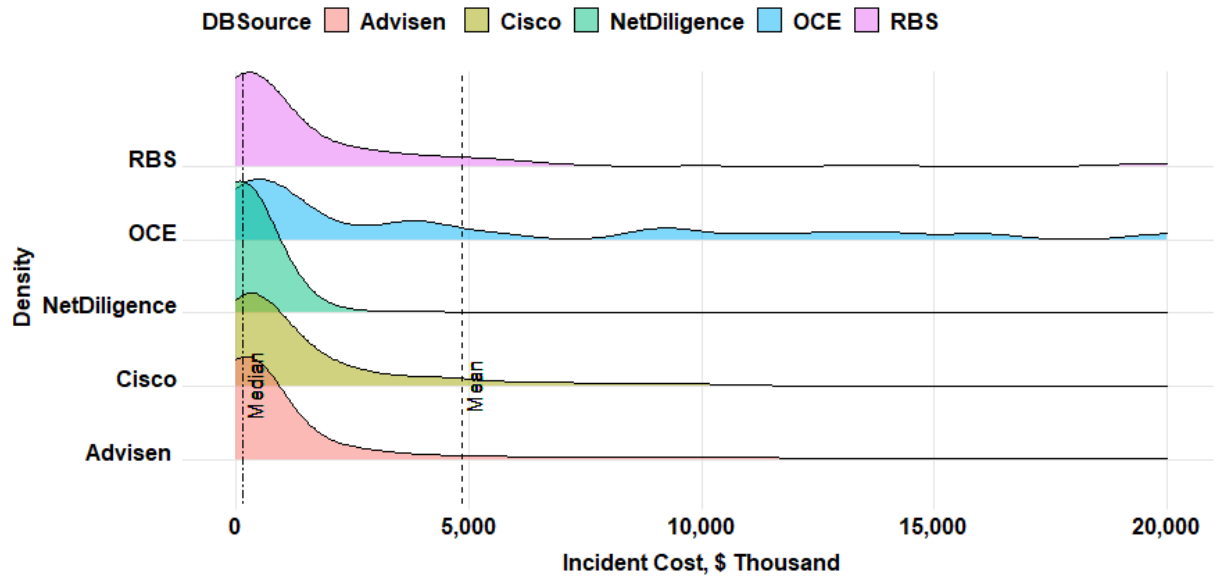
3.1.2. Reconciliation of Per-Incident Cost Studies

This section contains an overview and reconciliation of the per-incident estimates from the key studies analyzed in Section 3.1 as well as the primary data collected by the OCE team for large and small incidents discussed in Section 3.1.1.

Distributions of combined RBS, Advisen, NetDiligence, Cicso, and independently collected OCE data are shown in Figures 4 through 6 below.

To aid a visual comparison, Figure 4 zooms into the portion of the distribution with per-incident costs ranging up to $20 million. The vertical lines mark the median and average incident cost for the combined dataset.[6]

Figure 4. Distributions of Per-Incident Costs Data by Source



Technically, prior to combining the data from multiple sources into one pooled dataset, statistical testing needs to be performed to establish that all five datasets come from the same DGP. Otherwise, meshing multiple datasets into one would not be appropriate. However, because the data are very sparse with a high standard deviation in each dataset, the results of such statistical testing may not produce reliable results.

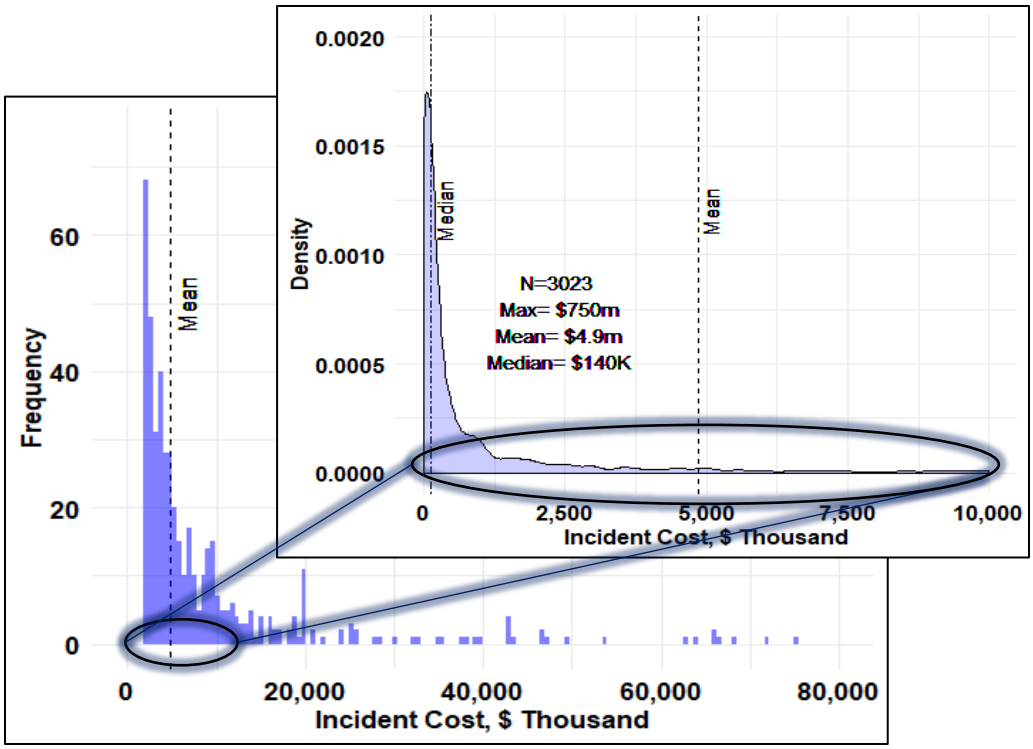
Sparse data is a recognized problem with all of these datasets. Acknowledging this limitation, OCE combines the datasets into a pooled sample because the data in primary commercial datasets are constructed in a very similar manner. That is, RBS and Advisen develop cost and loss estimates based on searching open-source publications for itemized incident costs across their own variants of cost categories similar to the analysis OCE conducted in Appendices C and D, and NetDiligence collects microdata on total cost of the incidents based on the cyber

[6] The average and median were calculated for the dataset that combined all of the available and relevant data.

insurance claims. More importantly, all of these datasets aim to describe the same phenomenon—cost of cyber incidents, even if they may pick up different segments of the disclosed cyber incidents and resulting losses. For example, the limited availability of data collection resources may lead to larger incidents being included more easily, as they receive more media attention.

The combined dataset containing 3,023 data points is shown in Figure 5.[7]

Figure 5. Distribution of the Per-Incident Cost in the Combined Dataset



The updated Office of Personnel Management (OPM) quote (over $760 million) was the maximum cost per incident, followed by an estimate in the Advisen data ($750 million). In Figure 5, OCE presented the range of costs only up to $80 million, because only a limited number of data points exceed $80 million and very few data points exceed $300 million.

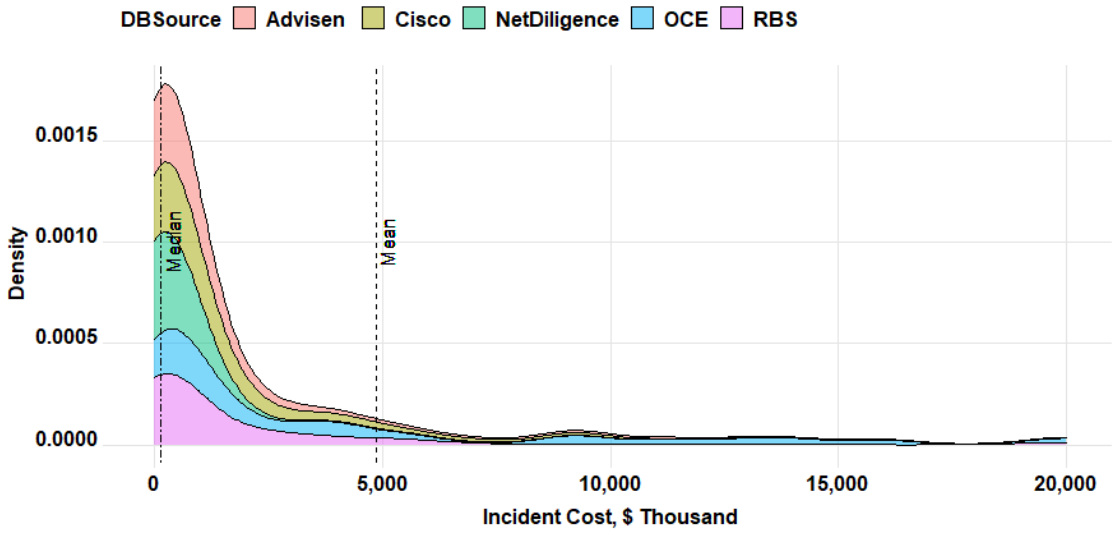
As explained in Section 3.1 and as can be seen in Figure 5, the dataset has long tail (i.e., there is a high number of extreme values). These large events can dominate the average costs per incident, and this is why OCE has put more weight on the median costs per incident in this analysis.

Overlaying the distributions allows visualization of similarities and differences across multiple datasets. Considering the data are sparse and range up to $760 million, with the maximum cost per incident in the updated OCE dataset of approximately $1 billion, this visual comparison is more meaningful for the more densely populated segments of the distribution. As presented in Figure 6, overlaying the distributions shows a similarity in the distribution's shape within the $20 million range—the portion of data that is most relevant for majority of the

[7] OCE has acquired more recent data sources (i.e., the Advisen 2009–2019 dataset and the NetDiligence [2019] report) and is in the process of updating the combined OCE dataset to reflect the newest data. This brings the overall observation count to approximately 5,000 data points.

incidents in the public sector (The average loss for the public sector in the most recent Cyentia [2020] study is approximately $13 million).

Figure 6. Overlaid Per-Incident Cost Distributions by Source, <$20 Million Segment



The OCE-pooled dataset that combines over 3,000 observations from across five sources depicted in Figures 4 through 6, updated with 2,000 additional data points from the most recent Advisen (2009–2019) and NetDiligence (2019) datasets, is the dataset that OCE will use going forward to support cost-benefit analysis of cybersecurity investments.[8] OCE will rely on this pooled dataset as a technical basis in developing bottom-up loss estimates, which in turn will support loss-avoidance analysis and business impact analysis specific to the research questions and tailored to proposed controls or mitigations.

3.1.3. Per-Record Estimates

There is a long-standing trend in cyber cost studies to normalize both impacts and costs to a per-record average, which could be used as a benchmark in estimating consequences and informing investment decisions. Examples of this approach initially appeared in the Verizon (2015) data breach report and earlier Ponemon Institute reports (2014, 2015, 2016a, 2016b). Since then, Verizon has eliminated this approach, and criticism of the method's poor fit to historical data recently appeared in Cyentia (2020). An additional disadvantage of this metric is its limited applicability, as it is relevant only to a subset of the payment card industry (PCI), personally identifiable information (PII), or personal health information (PHI) data breaches. The costs associated with many other types of breaches will not be accurately captured using this approach. For example, a per-record average would not be a suitable metric for the theft of intellectual property (IP), incidents involving the loss of integrity or availability, or incidents combining the loss of confidentiality and the loss of availability. However, per-record estimates are still a metric that is a focus of the Ponemon Institute reports (2017a, 2017b, 2018, 2019).

While an easy-to-use rule of thumb is certainly desirable, a cost-per-record approach could be misleading in that it not only discards the richness and granularity of the information necessary to truly quantify the risk, but also gives a false perception of consequences being diminutive for larger breaches when compared on a per-record basis. This is especially true for the previously discussed large breaches of PII, where the costs and damages that could be considered fixed with respect to the number of affected records constitute a significant portion of the

[8] OCE continues updating the dataset on a regular basis by appending and reconciling new data as it becomes available.

overall consequences, as compared to variable costs such as post-incident credit monitoring for impacted customers.

Following the cost-per-record logic, the fixed cost of an incident is divided by the number of records, and so the larger the size of the cyber breach, the cheaper it appears to be per compromised record. The average cost-per-record metric from the baseline incident is then used to estimate the total costs and impacts of other incidents where only the number of compromised records is known. However, there are important limitations to such an approach, which can be misleading when used to inform risk and investment analysis. For example, if the next simulated breach at the same entity is only half the size of the one used for valuation, the average cost-per-record metric would produce an estimate where the total cost and impacts would be half of the first baseline incident. Nevertheless, it is possible that only the credit monitoring costs would be half, while the fixed cost of response and cleanup may remain the same, and public relations (PR) damage, reputational losses, court fees, and fines could be much greater. Accurately quantifying this outcome would not be possible if a simplified cost-per-record average is used as a yardstick estimate to inform risk analysis or investment decisions.

The Verizon 2015 Data Breach Investigations Report (DBIR) initially explored the idea of whether PII breach costs depend strongly on the number of compromised records as demonstrated in the Ponemon Institute (2013, 2014) reports, or alternatively, if PII breach costs are dominated by the breach anatomy. This was an interesting observation, as it questioned whether intrusion mode and attack anatomy—which one would expect to dictate the immediate approach to mitigation and recovery, and therefore determine cleanup costs—were outweighed by other factors. These factors include variable per-record costs, such as notifications to affected customers, credit monitoring services, or fines and fees that may be set based on the size of the breach. Essentially, it questioned both the applicability and completeness of cost-per-record as a useful measure of impact.

More specifically, by applying the average cost-per-record approach to loss claims data, the Verizon (2015) DBIR calculated an estimate of $0.58 per record. The estimate is obtained by dividing the sum of all loss estimates by the total number of records lost. It should be noted that the Verizon DBIR analysis is based on the cyber liability insurance claims data from NetDiligence—specifically, 191 insurance claims with loss of payment cards, personal information, and personal medical records. Therefore, the previously discussed issues with insurance claims being tiered and subject to a payout limit apply here as well.

The Verizon (2015) DBIR compares its estimate of $0.58 per record with the Ponemon Institute's cost-per-record estimates for data breaches. The Ponemon Institute (2013, 2014) estimated a cost of $201 per record in 2014 and $188 the year before (for incidents with up to 100,000 records). These estimates were derived by totaling the losses for the year and dividing that by the total number of records lost in that year.

This disparity between the Verizon (2015) DBIR and Ponemon Institute (2013, 2014) estimates gave rise to a broader debate about the appropriateness of relying on the cost-per-record approach. It questioned the ability of either the Verizon or Ponemon Institute estimates to accurately predict costs of cyber breaches, for which both the size of the breach and pre-and post-insurance payouts have been publicly disclosed. Cyentia (2020) provides the most illustrative explanation of how severe the variability in the cost-per-record metric has been in historical data and the resulting pitfalls of relying on the direct scaling of per-record estimates. A summary of the discussion about how poorly per-record estimates fit to actual data is included in Appendix B.

Thus, per-record estimates and annualized normalizations done by dividing the total cost per year by the number of records exposed in a year could be misleading. Normalization within the boundaries of a specific incident is more appropriate if the correlation between the incident size and costs supports such analysis. However, even that is problematic and has a rather limited explanatory power as discussed in Appendix B.

OCE reviewed additional technical reports, academic articles, and white papers to obtain a better understanding of the cyber incident costs both at the micro and macro levels as well as of the scaling issues that impede reconciliation between the per-incident estimates based on microdata and aggregate estimates in the industry reports. OCE provides an overview of the aggregate estimates in the next section.

3.2. Aggregate Loss or Impact Estimates on the National Scale

This section discusses industry, vendor, government, and research reports that attempt to estimate the aggregate impact of cyber incidents on the U.S. or global economy. Very few studies contain estimates that are grounded in micro-data with transparent extrapolation to the national level. OCE's focus is on original studies that published first-author results based on primary data; therefore, subsequent derivative reviews and materials only citing the primary source are excluded from this discussion. This section includes an overview of estimates, methodologies, assumptions, and limitations in McAfee (2013, 2014, 2018); Symantec (2016, 2017, 2018); Cybersecurity Ventures (2016, 2017); WEF (2017, 2018); the BAML (2015); the Internet Crime Complaint Center (IC3, 2017, 2019, 2020); the FBI (2017, 2018); Norton (2015, 2016, 2017, 2018); the RAND Corporation (Dreyer et al., 2018); and CEA (2018).

A common characteristic of the industry reports is the estimation of impacts by induction from other types of operational losses; size of traditional crimes; size of underground economies; or other non-directly related factors with or without any implicit relationship to the cyber losses, their causes, or subsequent consequences. Also, the reports' partial disclosure of their underlying assumptions limits one's understanding of the analysis and applicability of the results. As such, while it is still a valuable anchor for bottom-up estimates, partial disclosure constrains the value of the estimates derived in these reports in informing a forward-looking simulation to estimate potential losses or inform resource allocation within a cybersecurity investment portfolio at the agency level.

The studies and the estimates reviewed below vary widely in the level of granularity of the assumptions and the empirical basis supporting those assumptions. As a result, studies with orders of magnitude difference should be viewed strictly within the boundaries of study-specific decision context, underlying methodological limitations, and the special interest of the sponsoring organizations.

3.2.1. Reconciliation of Aggregate Results

To make comparison easier, OCE summarizes the aggregate results from the reviewed national and sectoral studies in Table 7.

Due to different assumptions, estimation methods, and limitations, the aggregate annual estimates for U.S. impacts range from under $1 billion to over $242 billion, with more extreme estimates reaching over $7 trillion. Estimates on the lower end of the range (i.e., those in the $1 to $3.5 billion range) are based on historical data of complaints reported to the FBI (FBI, 2016, 2017; IC3, 2017, 2019, 2020; Symantec, 2017). They are followed by the group of estimates ranging from approximately $20 and $30 billion, as reported by Norton (2015, 2016, 2017), which is based on the self-reported data collected via an online survey.

The next group of estimates range from $24 to $120 billion (McAfee, 2013) to $140 to $175 billion (McAfee, 2018). CEA's (2018) impact estimates of $57 to $109 billion that were developed by extrapolating and scaling short-term stock market performance fall into the range between the two McAfee studies (2013, 2018), with the upper range of the CEA interval being close to the WEF's (2015) estimate of approximately $100 billion. WEF (2015) cites McAfee (2014), with the latter's estimates being developed by analogy from other types of proxy phenomena (e.g., other forms of crime and loss) at the national economy level. These estimates are based on self-reported loss assessment by affected companies with subsequent extrapolation to the national level.

The highest national impact estimate appears in the RAND study (Dreyer et al., 2018), where Advisen incident cost data is used to calculate cost-to-revenue ratios, which is then bootstrapped to find cost-to-revenue ratios by economy sector. National aggregate impacts are derived by applying the simulated cost-to-revenue ratios to the corresponding sector's annual GDP and summing across the sectors. This simulation approximated the median impact to be around $242 billion, with the 75th percentile being around $665 billion, and the 95th percentile being about $7.7 trillion. This is not only the highest in the analyzed batch of reports, but also higher than some of the highest global impact estimates (WEF, 2018; BAML, 2015; Cybersecurity Ventures, 2017, 2019).

The global estimates group and rank in approximately the same manner as the U.S. estimates. The lower end of the spectrum is based on the complaint data either reported to IC3 or estimated by IC3 based on other sources. It is followed by the $150 to $172 billion in losses estimated by Norton (2015, 2016, 2017). The next group of estimates is from McAfee, ranging between $375 billion and $600 billion (McAfee, 2014, 2018). Note that U.S. national impact estimates in these McAfee reports coincide with the global impact estimates in the Norton reports. The Symantec (2016) estimate falls in the McAfee (2018) range of $445 to 600 billion, because it cites BAML (2015), which in turn references McAfee studies, as do the earlier WEF reports.

Table 7: Summary of the Aggregate Estimates (U.S. and Global)

Study	Data Subset	U.S. Annual Cost ($ billions)	Global Annual Cost ($ billions)		
			Lower	Best	Upper
Symantec (2017)	BEC-Only Subset [a]	~$1	-	-	-
FBI (2016, 2017)	BEC-Only Subset [b]	~$0.53	-	~$1.76	-
IC3 (2017)	BEC Subset	-	-	$0.676	-
	Cyber Subset	-	-	$0.980	-
	Total Dataset	-	-	$1.420	-
IC3 (2019)	BEC Subset	-	-	$1.298	-
	Cyber Subset	-	-	$1.885	-
	Total Dataset	-	-	$2.706	-
IC3 (2020)	BEC Subset	-	-	$1.7	-
	Cyber Subset	-	-	_	-
	Total Dataset	-	-	$3.5	-
Norton (2015)		$28.9	-	$150.0	-
Norton (2016)		$20.3	-	$125.9	-
Norton (2017)		$19.4	-	$172.0	-
McAfee (2013)		$24–$120	$300	-	$1,000
McAfee (2014)		~ $100	$375	$445	$575
McAfee (2018) [c]		$134–170	$445	-	$600
Symantec (2016)			-	$575	-
CEA (2018)		$57–$109	-	-	-
RAND Corporation (Dreyer et al., 2018)	25th percentile	$27.8	-	-	-
	50th percentile	$241.9	-	-	-
	75th percentile	$665.0	-	-	-
	95th percentile	$7,710.0	-	-	-
WEF (2015)		$100	$100	-	$500
WEF (2018)		-	-	$1,600	-
BAML (2015)		-	-	$3,000	-
Cybersecurity Ventures (2017, 2019)		-	-	$6,000 (2021 projected)	-

[a] The average annual U.S. cost was calculated by dividing Symantec's (2017) estimated cost of $3 billion from 2013 to 2016 by 3 years.
[b] The average annual U.S. and global cost was calculated by dividing the FBI's (2017) estimated cost of $1.59 billion and $5.3 billion, respectively, from October 2013 to December 2016 by 3 years.
[c] McAfee's (2018) study reports North American loss estimates ($140–175 billion) instead of U.S. losses. OCE derived the U.S.-specific estimate by applying the cybercrime loss rate as share of GDP (0.69% to 0.87%) reported in McAfee (2018) to the U.S. 2017 GDP of $19.52 trillion (BEA, 2020).

The two highest global estimates, $3 trillion and $6 trillion, originate from the BAML (2015) and Cybersecurity Ventures (2017, 2019) studies. These two estimates share a couple similarities. First, while being abundantly referenced, the actual assessments that would contain specific details as to the supporting assumptions or methodology are not readily available. Second, their magnitudes are difficult to reconcile with any other global estimates, as they are anywhere from 3 to 10 times higher than the rest. In fact, they are an order of magnitude higher than some of the highest global estimates for the hypothetical extreme scenarios (Lloyd's, 2015, 2017, 2018, 2019), which are analyzed in Section 3.4 of this report.

This drastic difference in magnitude is difficult to explain or justify. As discussed in Section 3.1.1, the costs of some of the larger incidents with a high loss magnitude constitute only a fraction of a percentage of the impacted company's annual revenue (i.e., typically falling under 1%). The median cost-to-revenue ratio is approximately 0.37% across all sectors and incident types considered in the RAND study (Dreyer et al., 2018). These observations regarding the loss magnitude at the firm level make it challenging to defensibly establish which risk accumulation factors, systemic risks, specific economic linkages, or other shock propagation channels could amplify the consequences from the firm level to the aggregate level to the degree estimated by the BAML (2015) or Cybersecurity Ventures (2017, 2019) studies.

Furthermore, there is an ongoing debate in the recent literature questioning the longevity and severity of cyber incident-induced changes in the market performance of impacted companies, even ones suffering significant incidents with a seemingly high magnitude of losses. OCE discusses the issue of the market's reaction to cyber incidents in the next section.

3.3. Research on the Short- and Long-Term Impacts of Cyber Incidents

Multiple studies attempt to discern the short- and long-term impacts of cyber incidents on market performance. Since PII breaches and their associated costs were part of the focus in Section 3.1, it is worth looking at the research linking this specific type of incident to market value changes.

An interesting empirical result on market value losses is offered by Campbell et al. (2003) and Acquisti et al. (2006). Campbell et al. found that the stock price of companies reporting a security breach is more likely to fall if the breach leaked confidential information. Acquisti et al. conducted a similar analysis for privacy breaches. Their results show a negative impact on stock price followed by an eventual recovery.

Several more recent studies that looked into the recent data breaches found (1) no statistically significant market reaction in either the short or long term after the breaches occurred or (2) a slight stock price decrease followed by a quick recovery. Kvochko and Pant's (2015) study found that following the disclosure of a data breach, stock prices slightly decrease but then quickly recover. For example, in the case of the Target breach, while stock prices remained steady after the data breach, Target still faced about $236 million in total losses at the time Kvochko and Pant's analysis was conducted. Hilary et al.'s (2016) study analyzed recent data breaches including Target, Sony, and Home Depot and found similar results. That is, no statistically significant market reaction was observed in the short or long term. These sources argue that data breaches do not seem to significantly impact stock prices, because shareholders lack sufficient information about the breaches and tools to measure their impact and have become desensitized to news of data breaches or other types of cyber incidents.

However, a literature review by Spanos and Angelis (2016) suggests that cyber incidents have a statistically significant effect on the financial performance of affected companies. Spanos and Angelis reviewed 37 papers covering 45 studies with multiple estimation models and multiple comparison events for time interval samples between 1995 and 2012. The five types of analyzed events include Phishing, Information Technology (IT) Security Investments, Software Vulnerabilities, IT Security Legislation, and Security Breaches, with the latter being the event type most directly relevant to this analysis.

Out of 37 papers, 30 were security breach studies, with 27 out of the 30 using a one-factor model. A one-factor model is a simple comparison of performance based either on "the market return or the mean return of the stock in the previous trading days before the event or the return of a competitor of the firm" (Spanos & Angelis, 2016, p. 222). The security breach studies considered various vectors of breach impact, including the breached firms themselves, competitors of the breached firms, information security firms, IT consulting firms, responsible vendors, and related firms. Twenty-eight studies analyzed the impact of a security breach on breached firms,

which is the most relevant subset. Of those 28 studies, 20 studies identified a statistically significant negative impact to the stock price of the breached firms.

There is an important distinction between statistical significance and financial significance (i.e., materiality in financial or accounting terms). Statistical significance establishes if values of a particular metric are different between two groups, or in other words, if the difference between two values is non-zero. In the context discussed above, statistical significance indicates that there is a non-zero difference between the performance of the breached firms and the performance of its competitors, the overall market, or itself prior to the breach depending on the choice of the factors. In a regression model, statistical significance indicates if model's coefficients are statistically different from zero (i.e., statistical significance testing identifies if a variable has any detectable explanatory power). For example, in comparing the performance of the breached firms to the performance of the rest of the market, analysis may indicate that there is a 1% difference. Statistical significance refers to a numerical testing procedure that establishes if this calculated 1% is distinguishable from zero in statistical terms.[9] The outcome depends on the sample sizes and variances, which is just a measure of the variability or spread in the samples. In some instances, a 1% difference is statistically significant, while in other instances it is not. The studies discussed in the previous paragraph found the detected difference in market performance to be statistically significant.

Once a statistically significant difference in market performance is established, the next two questions of interest are (1) whether the difference in market performance (i.e., the negative impact on stock prices) results in a loss of significant magnitude (i.e., if the loss meets the materiality threshold), and (2) whether this type of loss is allowed to be included in assessed damages.

There is no official threshold for materiality; thus, the appropriate threshold may depend on multiple situation-specific factors (Eilifsen & Messier, 2015; Financial Accounting Standards Board, 1980; Holder et al., 2003; Vorhies, 2005) or the degree of precision in estimation (Financial Accounting Standards Board, 1980). Nevertheless, there are common working rules and ranges used by the major public accounting firms for determining overall materiality based on several quantitative benchmarks, including: total revenue, pretax income, net income, total assets (Eilifsen & Messier, 2015). Long-established working materiality levels or quantitative estimates of materiality are based on the following 5% rule:

> Reasonable investors would not be influenced in their investment decisions by a fluctuation in net income of 5% or less. Nor would the investor be swayed by a fluctuation or series of fluctuations of less than 5% in income statement line items, as long as the net change was less than 5%. (Vorhies, 2005, The 5% Rule section, para. 1).

In examining the materiality guidance for eight of the largest U.S. public accounting firms, Eilifsen and Messier (2015) compiled a set of ranges based on several benchmarks. Six of the eight firms "expect, suggest, or require the use of 5 percent of income before taxes" for U.S-listed entities and entities in regulated industries, with one other firm allowing a 5% to 10% range (Eilifsen & Messier, 2015, p. 15). Using total revenues as a benchmark, seven of the eight firms used a range from 0.25% to 2%, with the remaining firm applying a range from 0.8% to 5% of revenue as a condition for materiality.

Therefore, even if there is a statistically significant difference in the market performance of impacted firms as indicated by the studies reviewed in Spanos and Angelis (2016), it does not mean the statistically significant difference would translate into a financially significant magnitude, that is, a material fluctuation in performance that is high enough to influence the investment decisions as suggested by the 5% rule.

[9] For simplicity, the explanation illustrates the basic intuition behind a two-sample mean difference t-test. The literature reviewed in Spanos and Angelis (2016) relies on the t-test, Z-test, Wilcoxon sign-ranked test, and Sign Test.

Note that materiality thresholds can apply to losses from various sources, such as regulatory fees and fines; cyber incident-related changes in market performance; or direct costs and losses experienced as part of cleanup, response, and recovery following an incident (i.e., the total direct and indirect cost of a cyber incident). Freund (2020) analyzed the magnitude of cyber incident-related fees and fines and compared it with the materiality threshold guidance of the Big 4 accounting firms.[10] The objective was to understand the penalizing effect that the fees and fines may have relative to the level of losses that could be considered to materially impact the company. Freund discovered that guidelines for materiality internally established by the Big-4 accounting firms ranged from 2% to 10% of annual revenue, and this level of loss was typically over an order of magnitude higher than cyber incident-related fees and fines.

With a few exceptions, most of the large cyber incidents that occurred over the last 5 years did not reach this threshold. OCE's cross-validation of both large and small incidents is consistent with these findings. In addition, OCE's analysis of the cost-to-revenue ratios based on Advisen's 2005–2015 cyber incident cost data shows that the median cost-to-revenue ratio across all sectors is 0.37%, which is significantly lower than either the 5% accounting rule or the 2% to 10% materiality range examined in Freund (2020). Moreover, the cost-to-revenue ratio for the public sector is 0.8% for the 75th percentile and approximately 2% for the 85th percentile. In other words, the total incident cost for 85% of public-sector cyber incidents does not meet either of the discussed materiality thresholds.

However, Cyentia (2020) identifies a key difference between the loss magnitudes experienced by businesses of different sizes. A comparison of cost-to-revenue ratios by business size shows that cyber incidents are more penalizing for smaller companies, particularly SMBs. This is an important distinction and insight. According to the Council of Better Business Bureaus, SMBs face resource scarcity and lack in-house expertise and understanding for dealing with highly technical topics such as cybersecurity (Fanelli et al., 2017; Fanelli et al., 2016). According to the 2017 Council of Better Business Bureaus survey (Fanelli et al., 2017), 35% of businesses could remain profitable for more than 3 months if they lost access to essential data, with more than half becoming unprofitable in under a month.

Notwithstanding the considerations of cost-to-revenue ratios and materiality, treating fluctuations in stock prices and market performance as an incident-induced cost or loss could be problematic for another reason. Typically, unrealized losses (e.g., differences in market performance, especially short-term stock price fluctuations) and other implicit costs are not allowed to be included in damage assessments, as described in Romanosky et al. (2019). Similarly, other types of unrealized losses and indirect or implicit costs (e.g., opportunity cost, loss of customer confidence, forgone sales and revenue, potential increases in customer retention incentives, additional advertising budget to manage customer churn or influence brand image, and potential increases in PR campaign efforts and expenditures) are not allowed to be included as damages under state laws or as cyber tort damages.

For example, the recovery of opportunity costs in cyber tort damages is disfavored, in part due to the speculative nature of the harm and in part due to the economic loss rule, which holds that plaintiffs may not recover economic losses in negligence suits unless those losses arise from physical damage to the plaintiff's person or property (Johnson, 2005). The logic of economic rule would apply to the other implicit costs listed above. Specifically, one of the functions of the economic loss rule is the insistence that damages be proven with certainty (Johnson, 2005).

Another similar consideration is the valuation of harm from the theft of competitive data (Friedman, 2013; Friedman et al., 2013) or IP such as the exfiltration of data on the F-35 Lightning II Joint Strike Fighter that occurred in 2009 (Gorman et al., 2009; Greenemeier, 2009). The impact does not only depend on what specific information is exfiltrated, but also on its strategic sensitivity, timing, how it would be used in the long term, and by

[10] The Big 4 accounting firms include Deloitte, Ernst & Young, KPMG, and PricewaterhouseCoopers.

what party (Ernst & Young, 2014). Therefore, besides the known challenges with directly quantifying the value of stolen IP, the enumeration of negative consequences and resulting harm is difficult because it is strongly influenced by how it is converted by a competitor. In addition, firm-level impacts do not necessarily sum up at the national aggregate level, because there is a cumulative penalizing effect on the attractiveness of research and development investment in general, thus impacting the resource availability for research and development and stifling innovation. However, these second- or third-order effects may not be included in damage valuation because of their speculative nature and the difficulty associated with proving the damages with certainty.

In addition to conditions of materiality and the debate on whether abnormal stock market performance should be included as costs and losses from cyber incidents, there are multiple methodological limitations and disputed assumptions associated with the primary models typically used in event studies. First, the assumption that full information about the negative consequences stemming from an event was available at the time of disclosure or within the specific time window used to analyze market performance is problematic, as details typically become available as investigations progress. In other words, at the time of initial disclosure not all pertinent information is available even to the impacted company itself, let alone to the rest of the market. Second, the assumption that markets have the ability to fully absorb the disclosed information and react in a way that is a proxy for the accurate valuation of the cyber risk and consequences associated with a disclosed incident, compromised service or data, and the resulting short- and long-term implications is also problematic. Third, the ongoing and incremental desensitization of the market to cyber incidents over the last 5 years may have influenced the market response rate, thus creating the need for an updated evaluation.

In summary, the overall debate about the monetization of implicit costs and the impact of market performance is of limited relevance to this specific OCE study for the following reasons. First, market performance is relevant only for publicly traded companies, which comprise less than 0.1% of U.S. businesses (World Bank, 2017). Second, unrealized losses or implicit costs are not allowed to be included as damages. Third, even if some of the implicit loss categories were included in damage valuations, there is a significant gap between the cost-to-revenue ratios for cyber incidents and the materiality threshold (i.e., it is not clear whether the implicit costs or even the total incident cost would reach the 2% to 10% revenue threshold to fall in the material range). Finally, it has limited applicability to the public sector, where assessing reputational damages and intangible asset valuation is generally problematic. The direct quantification of losses is also problematic in part because even for well-documented instances of adversarial cyber activity, it is often difficult to tie it to a clear financial loss (Anderson et al., 2012; Anderson et al., 2019).

3.4. Individual Case Studies of Sets of Hypothetical Scenarios

Relying on historical data for reported incidents is always the preferred starting point for developing estimates of cyber incident costs and losses. However, there are several practical challenges in doing so.

First, the availability of historical data is limited. The lack of stronger disclosure requirements and clearly defined thresholds, the absence of a recognized common approach to costing, the lack of a standardized cost breakdown structure, and concerns of downward risk from disclosing any additional information resulted in a data-sparse environment with strong barriers and a lack of incentives for data sharing. As explained in Anderson (2001) and Anderson and Moore (2006), the lack of cost data and disclosure incentives severely limit the ability to analyze cyber risk and inform investment strategy. The importance of information availability for enhancing cybersecurity is also discussed in Bisogni et al. (2011).

Second, even if rich historical data were available, it would be insufficient for accurately estimating expected loss, because it is just one realization of a multitude of possible outcomes and therefore only provides a limited view. Historical data may inform a prior belief or probability distribution that initially suffices as the first step in risk quantification to support improved cybersecurity investment allocation. However, while providing an

incrementally better-informed basis for resource allocation, it would benefit from further refinement to improve the accuracy of the loss estimation by exploring variability in scenarios and associated outcomes. An analysis of counterfactuals is necessary to understand what might have instead occurred with a different level of potential severity, duration, and consequences.

Third, the reliance on synthetic scenarios is necessary in "threat casting" in order to explore the extremes of high-consequence, low-probability events and their associated cumulative exposure. In this context, synthetic scenarios are developed to explore probable maximum losses. These scenarios are based on purposefully extreme assumptions that lead to hypothetically large events in both duration and impact, thus representing a severe but plausible magnitude of loss (Coburn et al., 2018).

Therefore, studies with synthetic scenarios to explore counterfactuals and derive extreme impact estimates will persist as one of the essential methods for quantifying severe consequences. The current state of cyber risk quantification practices is limited by the sparse data on losses; underreporting of incidents; lack of visibility into cybersecurity practices; and, as a result, a constrained understanding of the current cybersecurity baseline and associated risk across multiple sectors and agencies. Weak patterns of association between assets, employed controls, and potential losses as well as a limited view of systemic risks may result in the underestimation of extreme losses and cumulative exposure. While extreme loss scenarios are not intended to serve as a standalone basis for ROI or cost-benefit analysis, studies in this group share a common objective of emphasizing risk accumulation and the aggregate level of cyber risk.

An extended list of 25 scenarios exploring extreme cyber losses and risk accumulation, including industrial control systems impacts, is contained in Coburn et al. (2018). Some of the most often-cited reports, such as Lloyd's (2015, 2017, 2018, 2019) are included in OCE's analysis as examples of scenario-based exposure studies. OCE presents a summary of the cost and impact estimates from these sample studies in Table 8.

Although the full extent of the impacts from a single event presented in Table 8 has not materialized in the past, the recent cyberattacks on the Ukrainian grid and the scale of the WannaCry[11] and NotPetya[12] infections clearly demonstrated the viability of scenarios and impact ranges comparable to Lloyd's (2017, 2018). Therefore, a more amplified breadth, depth, and rate of propagation can potentially trigger losses at the level of those estimated in Lloyd's (2015, 2019) studies, which are significantly higher than those estimated in Lloyd's (2017, 2018) studies.

However, even the highest of these hypothetical scenario-based estimates are still only a fraction of the BAML (2015) estimate that considers a potential worst-case 2020 "Cybergeddon" scenario, which stated that adversarial cyber activity could put up to $3 trillion of global economic value at risk. In turn, the BAML Cybergeddon estimate is only half of the $6 trillion annual loss projected for 2021 by Cybersecurity Ventures (2017)—another example of an assessment that is challenging to cross-validate and reconcile.

[11] WannaCry affected 200,000 computers in 150 countries (Blatnik, 2017; Donaldson, 2017) and had an impact that was estimated to range between $4 and $8 billion (Greenberg, 2018).
[12] NotPetya was estimated to exceed $1.3 billion in costs and losses for Merck, just one of many impacted companies (Griffin et al., 2019), and reach almost $10 billion in total damages (Blosfield, 2020; Greenberg, 2018).

Table 8: Summary of the Scenario-Based Study Loss Estimates

Study	Analyzed Scenario	Per-Scenario Impact ($ billions)		Region
Lloyd's (2015). *Business Blackout: The insurance implications of a cyber attack on the U.S. power grid*	Three scenarios for a single blackout event that vary by severity and duration	Scenario 1 Scenario 2 Scenario 3	$243 $544 $1,024	U.S.
Lloyd's (2017). *Counting the cost: cyber exposure decoded*	Two incident scenarios: cloud service provider hack and mass vulnerability attack. Event estimates across multiple countries for varying event severity.	Cloud Hack: Low 95% CI High 95% CI Vulnerability Attack: Low 95% CI: High 95% CI:	 $4.60–$53.05 $1.60–$10.85 $15.62–$121.41 $9.68–$28.72 $4.12–$15.63 $20.50–$34.22	Global
Lloyd's (2018). *Cloud down: Impacts on the U.S. Economy*	Three scenarios of outages by the largest cloud service providers that vary by length (0.5–1 days; 3–6 days, 5.5–11 days).	Scenario 1 Scenario 2 Scenario 3	$2.8–$5.9 $6.9–$14.7 $11.2–$23.8	U.S.
Lloyd's (2019). *Bashe attack: Global infection by contagious malware*	Three scenarios for global malware infection	Scenario 1 Scenario 2 Scenario 3	$85 $153 $193	Global

Note. CI = confidence interval. Sources: Lloyd's (2015, 2017, 2018, 2019)

To summarize, the objective of these intentionally severe scenarios is to explore extreme losses and risk accumulation. They are constructed with hypothetically high rates of depth, breadth, and propagation to illustrate a severe but plausible magnitude of consequences. Since the resulting impacts are extreme by design, they do not constitute a defensible benchmark or baseline level of losses to serve as a standalone basis for ROI or cost-benefit analysis. Instead, they are intended as stress tests to understand extreme tail risk, how it can scale, and the resulting potential gap between the total coverage and total premiums in cyber insurance (Coburn et al., 2018). Essentially, they are meant to support cyber insurance portfolio allocation decisions and risk accumulation management in the cyber insurance industry at the aggregate level. Therefore, it is not appropriate to use loss estimates from these studies to motivate increased investment in specific tools, technologies, or processes at an individual company or agency level.

4. SUMMARY OF DEFENSIBLE ESTIMATES AND SCALING LIMITATIONS

Comparing the macro (national or global) estimates of losses from adversarial cyber activity cited in the technical reports analyzed in this study as well as contrasting them with the known firm-level costs of actual cyber incidents mentioned in Section 3.1.1—notably some of the largest private-sector breaches in the last several years—emphasizes several important issues.

A few studies that attempt to explore the costs of adversarial cyber activity provide estimates that vary widely depending on the underlying assumptions, data collection, and estimation methodology. The preferred method

for developing estimates of cyber incident costs and losses requires historical data at the right level of granularity. Bottom-up calculations that derive national aggregate losses from per-incident data are more transparent, which make the results easier to comprehend, compare, and reconcile.

Nevertheless, a separate set of issues arises from the data collection methods and intermediate estimation undertaken to derive per-incident loss values. Employed methodologies often use surveys based on self-reported data of perceived losses via online poll or interviews. Some of the studies are developed by security vendors or consultants, and there is a potential concern that losses may be overstated due to possible conflicts of interest. As a result, some derived estimates have received strong criticism even from those researchers and experts listed as reviewers.

In addition, the interpretation of the per-incident results cannot be separated from the context of the loss categories and limits defined by the cyber insurance policies if the values are derived from the claims data. The loss numbers could be inflated, as they are self-reported or media-reported totals—not accounting- or audit-based estimates. However, these results only represent a portion of the loss, as they reflect only the loss categories typically included in policies, and only up to a specified sub-limit for each loss category.

Furthermore, the cost and loss estimates seem to follow a long-tail distribution. Therefore, analytic products that only report average costs or losses are of limited value. Tabulating the data in a manner that can support stochastic simulations for bottom-up, activity-based costing and presenting it in a quantile form across multiple factors that drive variability is a step in the right direction.

If the data are further manipulated to isolate the impact of specific factors, it has been a long-established standard in the analytic community to disclose model specification, indicate the estimator employed, and report results of the basic statistical testing that would allow analysts to assess the defensibility of the methods and the quality of the obtained estimates. Based on these considerations, the selection of the preferred source for loss estimates is in favor of more robust databases that collect data and proactively attempt to make the information available as either microdata at the firm and incident level or in the distribution form. Analytic output with limited disclosure of the underlying assumptions and insufficient explanation of the numerical methods does not provide as much insight and limits the transparency and defensibility of derivative products.

Reconciling the per-incident estimates with the national aggregate impact—even if the former is presented in the most desirable form with full disclosure—is complicated due to several well-known factors, including (1) historical frequencies versus probabilities and incident rates; (2) the rate of underreporting; (3) the subset of cost categories allowed to be included in the damage assessment; and (4) the monetization of fluctuations in the intangible assets value, especially in the public sector. This list of factors does not take into account more complicated issues such as an intelligent adversary, the changing threat landscape, and scaling.

One of the simpler examples to illustrate the predicament with scaling per-incident estimates is included in Appendix B using the Advisen data analyzed in Romanosky (2016). That example could be extended to consider aggregation of either per-incident costs or cost-to-revenue ratios to an industry or sector level. Most of the variability in the scaled national estimate is caused not only by underlying cost data, but by what an analyst is willing to assume for scaling factors or incident counts. Essentially, the challenge has to do with adequately capturing the variability in per-incident cost estimates as presented in Table 4 and developing a set of scaling factors, risk modifiers, or counterfactual scenarios to scale per-incident data in Table 4 up to national estimates in Table 7. This dictates the need for stochastic methods that account for potential variability across multiple dimensions and capture uncertainty around the key assumptions and parameters driving the estimation.

There are several factors that have direct and strong influence on scaling per-event estimates when obtaining aggregate values to infer the magnitude of the impact at the sectoral or national level. In Section 4.1, OCE

describes four of the main factors, and in Section 4.2, OCE illustrates these issues by developing total direct losses based on scaling per-incident and per-breach costs to a national level for the public sector. In addition, Section 4.2 discusses the implications of such issues.

4.1. Factors Influencing the Scaling of Per-Event Estimates

Several factors have a direct and strong influence on scaling per-event estimates to obtain aggregate values in order to infer the magnitude of an impact at the sectoral or national level. The four main factors include (1) the incident reporting rate, (2) differences in reporting requirements across industries, (3) analytical challenges hindering the defensible extrapolation of expected incident frequency or incident rates using historical data, and (4) the difficulties with comparing results from different datasets.

The first factor is the incident reporting rate. While the Securities and Exchange Commission (SEC; 2018) establishes regulations and guidelines regarding incident reporting for public companies, there is no clear understanding of how the reporting rate compares to the actual event rate, as only a subset of incidents meets the materiality threshold and becomes subject to disclosure. Thus, the bottom-up estimates of the direct cost at the national scale that are constructed from the individual per-incident losses reported in annual, quarterly, or other reports required by SEC regulations inherently result in underestimation.

The second factor is the difference in reporting requirements across industries, especially between the public and private sector. This aspect is illustrated and explained in detail in Verizon's (2018, 2019, 2020) DBIRs.[13] The total number of global incidents as reported in Verizon's (2018) DBIR is 53,308. The industry sector is unknown for about 35% of the total incidents. The public sector accounts for 43% (22,788) of all of the incidents, while private sector industries account for only about 22% of the incidents. The difference is even more pronounced for large incidents, where the public sector accounts for almost 92% of the total in the sample, and 4.3% remain unattributed. Thus, the private-sector share in the DBIR large incidents sample is only 4.2%.

Dissecting the totals further, out of the global number of incidents (53,308), 23,783 incidents occurred within the United States, with nearly 94% of the U.S. incidents coming from the U.S. public sector (22,245). Conversely, out of the global total incident count for the public sector (22,788), almost 98% of the incidents come from the U.S. public sector.

As explained in Verizon (2018), a large portion of the incidents consist of general policy violations or routine malware events, where an infected system gets cleaned up by a regular process without any breach of data. While mandatory reporting requires the public sector to report these incidents to the United States Computer Emergency Readiness Team, private industry does not have the same requirement. Therefore, private-sector incidents of this nature simply are not accounted for.

The discrepancy between the public- and private-sector reporting requirements is also emphasized in the total number of confirmed breaches in Verizon (2018). Nearly 57% (1,253) of all of the confirmed breaches (2,216) were reported in the United States. While the share of the reported U.S. public-sector breaches (140) in the U.S. total dataset is only about 11%, it comprises 46% of all of the confirmed breaches in the public sector (304).

Out of 140 confirmed breaches in the U.S. public sector, 71 were large (i.e., approximately 51%); 15 were small; and for 54, the size was unknown. Out of 545 large breaches globally, the largest share (over 20%) is made up of

[13] Verizon's 2018, 2019 and 2020 DBIRs contain only global summary data. U.S.-specific data for 2018 and 2019 were provided to OCE courtesy of the Verizon DBIR team. The 2018 and 2019 U.S. incident counts are of comparable orders of magnitude. However, Verizon's (2018) DBIR is used to illustrate challenges with scaling, because it contains the most directly comparable data with the Federal Information Security Management Act reports that were publicly available when OCE performed the analysis. See Section 4.2 for details.

public-sector breaches (111 large breaches), with about 64% of the large breaches in the public sector comprised of the large breaches reported in the U.S. public sector.

The third factor is the defensible extrapolation of the expected incident frequency or incident rates based on historical count data. In practice, cost and loss analysis has yet to overcome two analytical challenges associated with estimating the aggregate level of losses and associated cyber risk:

- A lack of consistent, defensible data with which to estimate current cyber risks (e.g., the scale of potential losses per incident and the probability of various incidents—especially major ones); and
- An inability to anticipate how adversaries will adapt to changes in the cybersecurity environment. (Even if analysts had access to observed counts of past incidents that were consistent across multiple sources, these would not be a defensible basis for prediction, because the assumption that past adversary behavior fully and accurately predicts their future behavior does not hold.)

Hence, cyber loss estimates and the risk and ROI estimates derived from them are repeatedly criticized for having limited defensibility. A separate debate on the subject raises questions on the applicability of the frequentist approach altogether and asserts that a game-theoretic framework is more appropriate for characterizing intelligent adversaries and adaptive threats. Yet if the frequency and conditional probability estimates required for a probabilistic approach present issues with defensibility, the parameterization of the adversary utility functions in the game-theoretic framework is at least as problematic. Irrespective of the chosen approach, the issue of scaling has direct and significant implications for any inference of the per-incident estimates to the aggregate totals for the agency, sector, or national level.

The fourth factor is the specificity in the cost and losses reported in annual datasets from various sources, as they are constrained by design-specific differences in the data collection approaches, collection coverage, the participating or contributing organizations, definitions, assumptions, and other considerations that influence the comparability of the results.

As an illustration of these factors significantly impacting loss estimates, OCE compares incident and breach counts from two leading industry reports, Symantec (2017) and the Verizon (2017, 2018, 2019) DBIR, below.

Symantec (2017)

Symantec (2017) is one of the few reports that provide statistics on the number of data breaches per month as well as an annual total. A distinctive characteristic of the Symantec data is that Symantec records a data breach when it occurs to its subscribers, as opposed to when it is reported. While this eliminates underreporting for subscribers, it excludes data from non-subscribers. Reporting is also limited to the types of activity that each specific suite of security tools is designed to detect, thus favoring certain types of incidents in the statistics and excluding data on undetected activity.

According to Symantec (2017), which reflects 2016 data,[14] the number of breaches globally equaled 1,523 in 2014, 1,211 in 2015, and 1,209 in 2016. The number of breaches that led to more than 10 million identities being exposed was similar across the three years and totaled 11, 13, and 15, respectively.

Although the number of data breaches globally has been relatively constant from 2015 to 2016 in the Symantec data, the number of impacted individuals has grown. The average number of identities stolen per breach has increased from 466,000 in 2015 to almost 1 million in 2016. Almost 564 million identities were compromised in 2015, which nearly doubled to 1.1 billion in 2016.

[14] While more recent Symantec reports are available for 2018 and 2019, Symantec (2017) is the latest edition containing specific summary statistics of interest.

Symantec (2017) reports that in 2016, about half of the compromised information was PII, with the share of Personal Financial Information a close second at 40%. The top causes of these data breaches are theft of data, phishing, spoofing, and social engineering. Theft of data was the cause in over a third of all breaches and was responsible for over 90% of the identities stolen in 2016.

U.S.-specific data in Symantec (2017) show that there were 1,023 breaches in the United States that resulted in the compromise of over 790 million identities. An interesting detail behind these numbers is that about 90% of all the identities were exposed in eight large breaches. The most affected subsectors in the private sector were Business Services with 248 breaches and Health Services with 115 breaches reported in 2016.

Out of the total incident count, Symantec (2017) observed only 6 breaches in the Public Administration sector, 75 in Transportation and Public Utilities, and 3 in non-classifiable establishments. Considering a difference in sector segmentation and groupings across various sources, this subset is be the most closely comparable to the public sector within other datasets.

Verizon DBIR (2017, 2018, 2019)

The Verizon (2017) DBIR's global sample shows a total of 21,239 reported incidents for the public sector, with almost 98% of the incidents within the sector being categorized as large (20,751). Because of the specific reporting requirements, the public sector accounts for about 50% of all the incidents and 93% of all the large incidents.

A similar trend is observed in Verizon (2018, 2019) data. Global incident data show 22,788 incidents for the public sector in Verizon (2018) and 23,399 in Verizon (2019), with 98% to 99% of the incidents typically categorized as large. The U.S. incident count for the public sector is 22,245 and 22,337, respectively.[15]

As for confirmed breaches, the Verizon (2017) global count is 1,935, increasing to 2,216 and 2,013 in Verizon (2018) and Verizon (2019), respectively.

The Verizon (2017) global number for the public sector (North American Industry Classification System code 92) was 239, with 59 large breaches, 30 small breaches, and 150 breaches of unknown size. Verizon (2018) and Verizon (2019) breach counts for the public sector increased to 304 and 330, respectively. Thus, the public sector breaches account for 12% to 16% of the total confirmed breaches reported in Verizon (2017, 2018, 2019).

Verizon (2017) reports 60% more global breaches (1,935) in its sample than the Symantec (2017) count of 1,209. The difference is even more pronounced for the number of confirmed breaches reported in the U.S. public sector. Verizon (2018) and Verizon (2019) U.S. data indicate that 140 and 146 breaches, respectively, occurred in the public sector, which is significantly different from Symantec's (2017) U.S. public sector count of 6 breaches in the Public Administration sector, or even with additional 75 in Transportation and Public Utilities, and 3 in non-classifiable establishments.

This comparison does not intend to contrast the quality of the reported results. Both reports are highly regarded sources in the cybersecurity industry, known for both data quality and thoughtful, in-depth analytics. The comparison simply aims to illustrate the variability in the incident counts as reported by various leading industry reports because of fundamental differences in the data sources, collection methods, and coverage. While there are multiple reports and databases that keep track of incidents and breaches in the various segments of the national and global economy, each one presents only part of the picture. Furthermore, it is not always possible to

[15] The Verizon (2018) incident and breach counts by sector are based on global data. U.S.-specific data were provided to OCE courtesy of the DBIR team.

reconcile various sources with overlapping boundaries to arrive at one cohesive, compact, consistent body of accurate historical data on incident counts and breach occurrences.

4.2. A Comparison of Per-Event Costs from Two Datasets Scaled to the National Level

To further emphasize the scaling issues and their implications for the public sector-specific scenarios discussed in Appendix B, Verizon (2018, 2019) U.S. incident and breach counts are used as a basis in developing an aggregate estimate of the direct incident and breach costs below. Verizon (2018) and Verizon (2019) incident and breach counts for the U.S. public sector are similar in magnitude as presented in Table 9.[16]

Table 9: Verizon (2018, 2019) Incident and Breach Counts

Event Type	Verizon DBIR (2018)	Verizon DBIR (2019)	OCE Assumption for Scaling
Incidents – U.S. Public Sector	22,245	22,337	22,000
Breaches – U.S. Public Sector	140	146	140

For a conservative estimate that avoids double counting of incident versus breach costs, OCE (1) used the lower number of breaches out of the two report years (140), (2) reduced the incident count by the breach count and then rounded it down further to 22,000 in order to have a defensible conservative lower bound that is easy to remember and to compare with other sources.

As presented in Table 10, an illustrative base estimate of total costs and losses for public sector could be constructed by summing the costs of the incidents and costs of the breaches, where cost of the incidents is estimated by multiplying the incident count (22,000) by the incident cost, and the cost of the breaches is derived by multiplying the breach count (140) by the breach cost.

[16] Verizon (2020) contains regional counts, which are of a similar order of magnitude. However, the counts pertain to all of North America. Thus, the Verizon (2019) U.S. count is used for comparison instead.

Table 10: Base Estimate of Public Sector Direct Losses, $ Thousands

		Number of Events A	Cost per Event [a] B	Breach Cost Subtotal C = A × B	Incident-Cost [b] D	Total Direct Loss E = C + D
Incidents		22,000	$3	N/A	$66,000	N/A
Breaches	Median	140	$132	$18,480	$66,000	$84,480
	75th percentile	140	$830	$116,200	$66,000	$182,200
	Average	140	$2,000	$280,000	$66,000	$346,000
	95th percentile (extreme)	140	$13,000	$1,820,000	$66,000	$1,886,000

Note. Sources: Verizon (2018, 2019), Romanosky (2016), and Cyentia (2020).
[a] The median and 95th percentile cost-per-incident estimates are based on the Cyentia (2020) public-sector subset. The 75th percentile and average cost-per-indicate estimates are based on the Advisen public-sector subset analyzed in Romanosky (2016).
[b] The incident-specific cost is calculated by multiplying the number of public-sector incidents in the OCE-adjusted Verizon (2018, 2019) data (22,000 incidents) by the cost per incident ($3,000).

While the incidents by definition do not result in a data breach and could be cleaned up as part of regular processes, there is still a cost associated with incident handling that includes the detection, ticket processing, United States Computer Emergency Readiness Team reporting, response, and recovery. Incident handling may require Enterprise Security Operations Center (ESOC) investigations that could include triaging the analysis, performing open-source intelligence gathering, performing host-based forensics, collecting and analyzing logs, analyzing malware samples, implementing blocks, and adjusting security tools. Therefore, multiplying the number of incidents in the U.S. public sector (22,000) by an average incident handing cost of $3,000 per incident, results in the direct cost estimate of $66 million.

The next step factors in the cost of the breaches, that is, incidents resulting in data exfiltration and loss of confidentiality. The cost of a breach typically includes forensics and investigation costs, PR and management costs, victim notification, credit and identification monitoring, legal guidance, regulatory fees and fines, lost business income and cost of downtime, and other response and recovery activities and expenses (see Table 19 for a detailed breakdown).

Ideally, the estimate should also account for and clearly specify the costs for other incident types that impact integrity and availability in addition to confidentiality. However, as discussed in Section 3.1, data breaches typically get more attention in datasets because breaches are more frequently disclosed and reported. Incidents involving loss of integrity or availability are not as readily disclosed and, as a result, are underrepresented in the currently available data. Thus, although other incident types are included in the datasets used to derive the public-sector cost statistics presented in Table 10, data breach records are a dominant subset.

As analyzed in Romanosky (2016), the median cost of a breach in the public subset of the older Advisen data from 2005 to 2015 is approximately $170,000. The 75th percentile is about $830,000, and the average breach cost is $2 million. A more recent analysis of the Advisen public sector data from 2009 to 2019 is included in Cyentia (2020), where the median is approximately $132,000 and the average is approximately $13 million. However, the average per-breach estimate of $2 million exceeds the 80th percentile value in the Advisen 2005–2015 public-sector breach cost dataset. In the 2009–2019 version of the dataset, the average of $13 million represents the 95th percentile and is reported as an extreme value. This yet again emphasizes the pitfalls of relying on averages in long-tail distributions.

Considering the shift in summary statistics over time between the two versions of the dataset, as well as the dispersion of the underlying data, several point estimates are included for consideration to more fully explore the range of cost variability. Multiplying the breach cost estimates for the public-sector subset by the assumed breach counts (140) results in four comparative cases for the breach cost subtotal as presented in Table 10. The total loss column is a sum of the breach cost subtotal (four cases) and the $66-million incident handling cost.

The conservative estimate for overall costs ranges between $84 million (based on the median breach cost of $132,000 in Cyentia [2020]) and $182 million (based on the 75th percentile cost of $830,000 per breach from the Romanosky [2016] public-sector subset). The total loss estimate constructed based on the average cost per breach within the older Advisen public-sector subsample ($2 million) reaches $346 million. The total loss estimate constructed based on the average cost within the newer Advisen public-sector subsample ($13 million) is approximately $1.89 billion. With the average coinciding with the 95th percentile of the distribution and with it being reported as an extreme value for the public sector in Cyentia (2020), this estimate requires a strong emphasis on all of the previously discussed caveats associated with the long-tail distribution of the DGP. Thus, the latter estimate of $1.89 billion would represent an upper-bound level of direct losses in the U.S. public sector under the assumptions specified in Table 10.

Several aspects of the estimates presented in Table 10 may benefit from further refinement. For context, the per-incident cost of $3,000 appears to represent a lower end of the range for cleanup. Hiscox (2018) cites a per-incident cost of $4,883 for small businesses with 249 or fewer employees. Based on Coburn et al. (2018), additional insight could be gained from considering an extended range of costs and losses, for example, $10,000 to $15,000 per incident as rounded from the small firm estimates ($9,000 and $14,000) in Hiscox (2019) and informed by internal U.S. Department of Homeland Security ESOC estimates to represent a conservative lower bound. These three levels of cleanup costs (i.e., $5,000, $10,000, and $15,000 per incident) serve as a basis for additional loss estimates for the U.S. public sector.

In addition, Federal Information Security Management Act (FISMA) reporting is considered the primary source for incident counts across federal civilian agencies, as opposed to DBIR reporting. The number of recorded incidents in FISMA (2019), the latest publicly available version, is 28,581. This is the lowest FISMA incident count out of three consecutive years, with FISMA (2018) and FISMA (2017) reporting 31,107 and 35,277 incidents, respectively.

With the FISMA incident count being 30% to 60% higher than what was reported in Verizon (2018, 2019), OCE incorporated additional loss estimates based on the rounded down FISMA (2017, 2019) data, while treating the 22,000 incident count informed by Verizon (2018, 2019) as a lower bound. The incident count reported in FISMA (2017), which was the highest of the three consecutive years, is treated as an upper bound.

Table 11 includes loss estimates for the U.S. public sector for three additional scenarios ($5,000; $10,000; and $15,000 per incident), as well as an additional estimate for the federal civilian agencies based on FISMA (2017, 2019) incident data.

Table 11: Annual Total Incident Cost Scenarios

Study	Number of Incidents [a]	Annual Incident Cost ($ thousands), by Per-Incident Cost			
		Low Scenario A - $3,000	Low Scenario B - $5,000	High Scenario A - $10,000	High Scenario B - $15,000
Verizon (2018, 2019)	22,000	$66,000	$110,000	$220,000	$330,000
FISMA (2019)	28,000	$84,000	$140,000	$280,000	$420,000
FISMA (2017)	35,000	$105,000	$175,000	$350,000	$525,000

[a] All of the incident counts were rounded down to the nearest thousand to avoid double counting.

Combining the Verizon (2018, 2019) and FISMA (2017, 2019) incident total cost estimates from Table 11 with each of the Advisen-based breach-specific costs from Table 10 (i.e., adding $18.5 million, $116.2 million, and $280 million, and $1.8 billion, respectively, to obtain the median, 75th percentile, average, and 95th percentile) provides the aggregate estimates for the U.S. public sector presented in Table 12.

Table 12: Additional Aggregate Loss Estimate Scenarios, $ Thousands

Incident Count Source	Cost-Per-Breach Estimate [a]	Total Direct Loss [b]			
		Low Scenario A	Low Scenario B	High Scenario A	High-Scenario B
Verizon (2018, 2019)	Median	$84,480	$128,480	$238,480	$348,480
	75th Percentile	$182,200	$226,200	$336,200	$446,200
	Average	$346,000	$390,000	$500,000	$610,000
	Extreme	$1,886,000	$1,930,000	$2,040,000	$2,150,000
FISMA (2019)	Median	$102,480	$158,480	$298,480	$438,480
	75th Percentile	$200,200	$256,200	$396,200	$536,200
	Average	$364,000	$420,000	$560,000	$700,000
	Extreme	$1,904,000	$1,960,000	$2,100,000	$2,240,000
FISMA (2017)	Median	$123,480	$193,480	$368,480	$543,480
	75th Percentile	$221,200	$291,200	$466,200	$641,200
	Average	$385,000	$455,000	$630,000	$805,000
	Extreme	$1,925,000	$1,995,000	$2,170,000	$2,345,000

[a] The median and extreme (i.e., 95th percentile) cost-per-incident estimates are based on the 2009–2019 Advisen public-sector subset analyzed in Cyentia (2020). The 75th percentile and average cost-per-incident estimates are based on the 2005–2015 Advisen public-sector subset analyzed in Romanosky (2016).
[b] For each study, the total direct loss is the sum of the breach costs (i.e., the breach count multiplied by the per-unit breach cost) from Column C in Table 10 and the incident-specific losses in Table 11.

A more appropriate method for constructing the aggregate estimate of direct losses is to bootstrap the distribution of pooled public-sector per-incident costs for the number of breaches in the DBIR. Yet, the estimate in Table 12 is intentionally oversimplified to linear scaling to illustrate the orders of magnitudes that could be substantiated by currently available data in its simplest form.

To summarize, the direct loss estimates for the U.S. public sector developed for a set of scenarios in Appendix B align with the results based on a simple scaling of the Verizon DBIR and FISMA data presented above. The magnitude of direct losses in the public sector directly depends on scaling assumptions, as illustrated in this section. Ignoring the extreme cases, losses could range from $84 million to $385 million per year, assuming a lower-bound cost of $3,000 for the cleanup of incidents that did not lead to data exfiltration or other full action

on objectives. Increasing the cost of the basic, routine cleanup to $5,000, $10,000, and $15,000 while keeping the breach-specific costs as shown in Table 10, approximately doubles the total direct loss for the year, ranging from $128 million to $805 million (again, ignoring the extreme cases), depending on the particular combination of assumptions. In the extreme case, that is, if each one of the assumed 140 annual breaches or serious incidents affecting integrity or availability were to cost around $13 million (95% of the public-sector cost in Cyentia [2020]), the total cost could range from approximately $1.89 billion to $2.35 billion.

These direct loss estimates do not include costs to consumers, externalities, spillover effects, or opportunity costs. The range only reflects direct costs at the public-sector level with the purpose of informing the approximate order of magnitude. Applying economic multipliers to this range can produce estimates for indirect and induced losses, but second- and third-order effects are typically not allowed in impact estimations (e.g., in regulatory contexts). Thus, any further scaling or application of national aggregate multipliers is omitted from OCE's analysis.

5. CONCLUSION

In this section, OCE describes its contribution to the cyber loss literature, existing challenges and proposed solutions, practical alternatives for when in-depth analysis is not feasible, as well as suggestions for further research.

5.1. OCE's Contribution

This study conducts an in-depth survey of the cyber loss literature by documenting data sources that estimate costs and losses induced by cyber incidents. It also identifies the extent to which the cyber incident costs and losses have been tracked and analyzed within the private and federal sector. The study is a systematic review that contains a thorough characterization of the current state of the literature and a synthesis of the published results.

In addition, OCE's study identifies defensible estimates of cyber losses, which are grounded in historical data and can be used to inform the forward-looking analysis of the benefits of cybersecurity investment. It clearly outlines the limitations in the currently available estimates and identifies potential approaches to resolving the informational and methodological gaps.

The overall objective was to document existing cost and loss estimates for cyber incidents, including empirically derived and scenario-based values, as well as to examine underlying assumptions and methodologies to provide a defensible technical basis for evaluating the benefits of cybersecurity investments. Loss avoidance is one of the acceptable methods for quantifying cybersecurity benefits. However, the loss estimates are only defensible to the extent that they are grounded in historical data.

5.2. Existing Challenges and Proposed Solutions

OCE's review of the cost and loss literature illustrates the primary challenges with existing data sources. Without exception, all of the data sources are based on convenience samples. This means that no statistical representativeness can be claimed about the derived estimates. Technically, this limits the ability to support inference for generalizing results beyond the studied samples.

In addition, differences in individual data collection approaches as well as differences in the threat groups and types of incidents under consideration heavily influence the content of each dataset and composition of collected and analyzed events. Relying solely on the data contained in the key commercial databases and reports

introduces a risk of overlooking an entire class of adversarial cyber activity that some data collection entities are unlikely to deal with regularly (e.g., more advanced threat groups). For situations not sufficiently represented in the sources analyzed in this study, additional expert knowledge may be necessary.

Nevertheless, that is what analysts have to rely on for supporting policy decisions, as only limited data on costs and losses are available. Therefore, OCE recommends using a pooled dataset that combines the contents of the reviewed databases meshed with the data independently collected by OCE for cross-validation purposes.

Moreover, this pooled data can serve as a seeding dataset. As other federal departments and agencies or private-sector partners choose to share their cyber incident loss estimates with OCE, their information can be appended to the over 5,000 existing data points. Appending the estimates to other data reduces the likelihood of the data being traced back to specific incidents or agencies, thus preventing re-identification. Aggregated federal agency information is likely to provide the most relevant data that would facilitate the exploration of incidence of harm for the public sector in more detail. However, this would first require the development and implementation of additional tracking and reporting principles and practices that follow (1) a common set of cost categories and (2) common business impact analysis guidelines.

An additional challenge arises from the fact that historical data only represent the observed and reported subsets of events. This issue of coverage, best illustrated in Romanosky (2016), contributes to the problem of scaling known results. Granted, there are limitations to what can be done when it comes to the observed versus unobserved adverse cyber activity (Bisogni et al., 2017). However, there is a practical solution to overcoming the limitations of operating solely with historical data constrained to only detected and identified incidents with assessed consequences and losses. Relying on counterfactual analysis and exploring multiple what-if scenarios has been a generally accepted approach to addressing this limitation. As part of this approach, a researcher develops a base case or baseline that is grounded in historically observed data. Then a set of hypothetical scenarios or counterfactuals is constructed to evaluate what the alternative would have been in the absence of the phenomenon or with intervention or mitigations introduced.

While it is a common understanding that underreporting may be a problem and reported incidents and breaches represent only a fraction of the incidents, there is no indication as to the relative size of that share despite the most recent analytical attempts at informed scaling (Bisogni et al., 2017; CEA, 2018). Unlike the issue with unobserved activity, the challenge of underreporting would be better addressed with a policy solution as opposed to a methodological work-around. The drastic difference in the number of reported incidents by the public sector as compared to the private sector in the Verizon (2018, 2019, 2020) DBIRs highlights the nature of the problem. The federal incident notification guidelines for the public sector, specifically, federal departments and agencies, require that any incident that impacts confidentiality, integrity, or availability must be reported within an hour of being identified. For the private sector, the ambiguity of the SEC reporting guidelines and the reporting threshold result in a lack of transparency or understanding on how the reporting rate compares to the actual event rate. In addition, as explained in Grotto and Markidis (2018), the SEC incident notification guidelines only apply to public companies, which comprise less than 0.1% of U.S. businesses (World Bank, 2017).

Similar challenges with disclosure are discussed in Hiscox's (2018) report, showing that about 9 out of 10 companies that rate themselves as cyber experts fully disclose cyber incidents to internal and external stakeholders. However, only half of the companies describing themselves as cyber novices report the same rate of disclosure. Considering that 73% out of 4,100 surveyed companies rated themselves as novices, it has negative implications regarding the existing disclosure practices.

Adjusting the SEC reporting guidelines in a manner similar to the Federal Energy Regulatory Commission (2017) proposed rule that would establish uniform reporting requirements for all events, but with consequence assessment being stipulated for ones exceeding a specific threshold, could improve market transparency (Grotto

& Markidis, 2018). Further, modifying the guidelines could ameliorate the challenge with underreporting as well as present a more adequate foundation for quantifying the baseline cyber risk.

The lack of sufficient historical data on costs and losses, issues with underreporting, the absence of a common risk ontology or cost categorization for assessing incidence of harm and evaluating damages, challenges with utilizing incident frequency data to characterize the processes driven by an intelligent adversary, and the constantly changing threat landscape result in inconsistencies in risk quantification approaches. These inconsistencies, in turn, lead to significant variability in the resulting estimates. Therefore, cost and loss, and subsequently, risk estimates, are only credible and defensible to the extent that detailed assumptions and estimation methodologies are clearly disclosed. Black-box estimates, however frequently cited in the popular press or vendor promotional materials, do not provide analysts with a sound technical basis for assessing risk or conducting cost-benefit analysis for supporting cybersecurity investment decisions.

Similarly, aggregate estimates (at the sectoral, national, or global level) are often used by cybersecurity vendors to urge investment in cybersecurity; however, such use of aggregate estimates of cyber losses often lacks explicit evidence on the technical effectiveness of the proposed products or a clear linkage between the proposed solution and the size of the problem it is intended to address. This criticism also extends to relying on scenario-based estimates intended to emphasize extreme events, risk accumulation, and the potentially crippling magnitude of the resulting losses. While instrumental in obtaining order of magnitude estimates for tail losses, they are not a suitable baseline for cost-benefit analysis.

Even if sufficient historical data on incident occurrences and losses were available, there are other methodological challenges to take into account. Historical data represent just one specific realization of a myriad of possible ways the incidents could have unfolded, with the costs and losses being potentially very different. Therefore, the availability of historical data is a necessary, but not sufficient condition in constructing a potential loss curve. Historical data can inform lower-bound or mid-range losses, but it is limited in supporting a full cyber risk quantification or cost-benefit analysis. Historical data may inform a prior belief or probability distribution that initially suffices as the first step in risk quantification to support improved cybersecurity investment allocation. However, while providing an incrementally better-informed basis for resource allocation, it would benefit from further refinement to improve the accuracy of the loss estimation by exploring variability in scenarios and associated outcomes. The latter requires multiple scenarios and the likelihoods associated with them, meaningful counterfactual analysis, a sensitivity analysis of the parameters, an evaluation of extreme events to assess the maximum probable loss, as well as an understanding of risk accumulation factors.

The accurate estimation of losses and risk quantification is not a trivial issue in cybersecurity. However, it is only one of multiple obstacles. Cybersecurity poses an asymmetrical problem—a small number of vulnerabilities can lead to an extensive compromise. Even with a strong defensive posture, it only takes a limited number of exceptions to result in failure. Sometimes, it is only possible to identify defensive shortfalls after the fact when those efforts fail and an incident is detected and identified. In other instances, the attackers succeed by following the path of least resistance and utilizing well-known old vulnerabilities (Solomon, 2020; Verizon, 2020). Some of these lapses are due to inconsistent execution rather than reluctance to spend on defenses. Therefore, even when an incident occurs, the underlying issue is just as likely to be suboptimal leverage of an appropriate investment than underinvestment.

Security stack optimization, correct implementation and configuration of controls, adequate staff training on the proper execution, and overall awareness training are important factors. Nevertheless, securing funding to maintain or improve existing cybersecurity capabilities is part of the constraint. This becomes even more evident when cyber risk is inadvertently compared with other operational risks in the enterprise risk management (ERM) context for resource prioritization, where operational risks are evaluated and communicated in clear financial

terms. This study attempts to establish a defensible basis for such quantification where benefit of the cybersecurity investment can be expressed in financial terms via estimation of loss avoidance.

Additional implications of the study findings include the following: (1) losses from cyber and non-cyber risk events come from two different DGPs,[17] thus dictating the need to model, analyze, and manage cyber risks separately from other operational risks; and (2) the prioritization of resources towards cyber risk management will remain challenging as the empirical valuation of limited historical data on cyber losses show that other operational losses are a more dominant source of risk. Considering these two factors, meaningful ERM that allows cyber risk to be integrated and compared with other operational risks requires a transparent and repeatable approach to cyber consequence characterization, business impact analysis, and loss quantification with subsequent cost-benefit analysis to clearly understand the trade-offs.

5.3. Practical Alternatives and Additional Research

In-depth analysis as described above is not always realistic given budget or schedule constraints (particularly for smaller federal departments and agencies) and especially considering the other existing data and methodological limitations. A practical interim solution is to rely on the OCE pooled dataset that combines over 5,000 observations as discussed in Section 3.1.2 and depicted in Figure 5 and develop bottom-up loss estimates specific to the research question and analyzed controls or mitigations. This is the approach that OCE will use going forward for cost-benefit analysis of cybersecurity investments.

Another practical alternative is treating OCE's pooled dataset that was explored as part of this analysis as a base case distribution of losses and developing risk modifiers or scalars for federal departments and agencies depending on the characterization of protected assets and systems. Given the same data and methodological challenges that CISA faces in quantifying cyber risk for the federal sector, this essentially would be an extension of what Romanosky et al. (2019) describe as a simplified approach that cyber insurance applies to private-sector entities.

A more involved solution could include a detailed business impact analysis for the systems of interest, which would fully account for system-specific characteristics, system mission and purpose, and relevant loss factors. By relying on a factor tree analysis, this approach explicitly considers incidence of harm and enables a tailored, bottom-up impact analysis of the potential loss of confidentiality, integrity, or availability (or any combination of these elements). OCE is currently developing a repeatable methodology for a tailored business impact analysis. This methodology can be extended to include mitigation decision support if coupled with data on (1) the cybersecurity controls that constitute the organization's and system's defense, and (2) the controls' effectiveness for proposed mitigations (Kambic et al., 2020). To assess economic justifiability, the business case is formulated by comparing the loss averted by a variety of cybersecurity controls to the cost of investing in those controls.

However, empirical data on the performance or effectiveness of cybersecurity controls, mitigations, and policies is even sparser than the data on cyber incident costs and counts. This may preclude a clear-cut, "before-and-after," evidence-based comparison of potential losses where the effectiveness of the controls is an input to the analysis, except for the occasions where operational data are available. Thus, the need to validate technical effectiveness and economic justifiability necessitates an ongoing evaluation of the controls' performance and mitigation effectiveness, which could be conducted via pilot studies or operational prototypes. Meanwhile, a practical interim solution is to rely on alternative metrics for evaluating the outcomes, such as the percentage of

[17] The DGP is the true, underlying phenomenon that is creating the data.

potential risk reduction or break-even analysis as recommended by the Office of Management and Budget,[18] to communicate the benefit of the cybersecurity investment and the CISA CSD's existing capabilities.

[18] According to the Office of Management and Budget (2003),

> It will not always be possible to express in monetary units all of the important benefits and costs. […] If the non-quantified benefits and costs are likely to be important, you should carry out a "threshold" analysis to evaluate their significance. Threshold or "break-even" analysis answers the question, "How small could the value of the non-quantified benefits be (or how large would the value of the non-quantified costs need to be) before the rule would yield zero net benefits?" (p. 2)

APPENDIX A – SOURCES AND METHODS

OCE used many different news sites, financial reports, and press releases to collect reported direct costs of cyber incidents to support a systematic literature review. OCE used Google to find these sources. Search terms included various combinations of phrases relating to cyber incidents, cybersecurity, cost, and data breaches as well as specific companies, industries, and studies. A comprehensive list of search terms used by OCE is included in Table 13.

Table 13: List of OCE's Search Terms

• Cost of breach study • Cost of breach study –Ponemon –IBM • Bank breach cost • Bank will spend on credit monitoring for breach • Celebrity will spend on credit monitoring for breach • Credit union will spend on credit monitoring for breach • State will spend on credit monitoring for breach • Data breach calculator • Spend * on credit monitoring for breach • Spend * on notification for breach • Spend * on notification +breach • College breach • Cost of credit monitoring after cyber attack • Credit monitoring after breach • * spend on credit monitoring after breach • University breach will cost • County breach will cost • Electric company breach will cost	• Cyber attack on * cost +$Cyber attack on * cost +news +$ • Cyber attack cost • Breach cost for * • * Breach cost to recover • * Breach cost • * cost hack • * cost cybersecurity +hack • * spent on cybersecurity +hack • * spends on computer security • After cyber attack * spent • * spent after cyber attack • * spent * after cyber • * spent * on fixes +cyber • After cyber attack * +spend • After cyber attack * will spend • * spent cleaning up after data breach • * will pay after data breach • Data breach recovery cost • Pay after hack • Pay after cyber attack • Company paid for data breach • Cost after cyber attack • Data breach will cost *[19]

Table 14 presents the criteria OCE used to identify useful and relevant sources for this literature review and estimate analysis.

[19] OCE omitted closely related search terms that yielded similar results from this list.

Table 14: List of OCE's Mandatory and Non-Mandatory Selection Criteria

Nr.	Type	Name	Description
1	Mandatory	Language	Only studies in English were considered.
2	Mandatory	Time Frame	Only incidents and reports from the past 10 years were considered.
3	Mandatory	Economic Data / Costs	Only incidents and reports that contained factual, scholarly economic data or specific estimates were considered.
4	Mandatory	Geographical Area	Only incidents which occurred in the United States or to U.S.-based companies were considered. The cause of the incident (i.e., the hacker) need not be located inside the United States.
5	Mandatory	Reputable Source	The source of information about costs and other reported numbers must come from a reputable source.
6	Non-Mandatory	Type of Costs	Incidents with a well-assessed total cost or with a comprehensive breakdown of costs were preferential.
7	Non-Mandatory	Type of Source	Peer-reviewed publications were preferential. Technical reports, industry publications, position papers, academic literature, blogs, and online articles were allowed.
8	Mandatory	Regional specificity of the estimates	International studies allowed if the estimates address U.S. or North America cyber activity in addition to global loss estimates.

Non-mandatory selection criteria represent OCE preference. However, if they were not met, that data was still retained for analysis. OCE applied the following exclusion criteria to the search:

- Theoretical studies with imaginary or synthetic data;
- Purely methodological discussions;
- Impacts assessed by applying per-record estimates from other studies (i.e., OCE retained only primary sources and original work for the review);
- Circular references without ability to establish and validate primary sources and associated assumptions;
- Aggregate estimates without disclosed methodologies or assumptions;
- Unsourced estimates such as PowerPoint presentations, executive summaries, or marketing materials containing cost or impact estimates;
- Vendor marketing materials without discussion of how the estimates were constructed; and
- Tertiary layer of references to industry reports such as online articles, blogs, and social media posts.

In its literature review, OCE reviewed over 500 articles from publicly available sources published prior to June 2020 and discarded any articles that were unsubstantiated, lacked cost data, or did not meet the criteria in Table 14. OCE found approximately 390 articles, reports, and studies to be the most relevant, and retained these for the subsequent analysis.

In order to qualitatively evaluate the relevance of the data and methods in the 390 sources, OCE conducted a subsequent round of review. OCE assessed whether these sources contained the following:

- A basis in empirical evidence or theoretical assumptions;
- A clearly defined data collection instrument and a thoroughly explained process;

- A description of the source (e.g., vendor, academia, public sector, industry reports, insurance, reinsurance, and cat-modeling) and intended use of the estimates;
- Aggregate versus bottom-up estimates;
- Incident-specific estimates based on invoices or accounting and scenarios; and
- A clear discussion of which cost and impact categories are included in the damage and loss assessment.

To keep the estimates on a comparable basis, physical disruptions, outage valuations, and any other physical cascading impacts (e.g., grid outage valuations based on value-to-customer surveys) were treated separately as scenario-specific case studies.

The subset of studies with the actual incident cost data or cyber incident cost and loss estimates is limited. Only about 150 articles, industry and government reports, and academic papers contained either historic cost data or derived cost estimates for the losses.

APPENDIX B – DETAILED LITERATURE REVIEW

This section contains a summary of the loss estimates available in the most widely cited published research, commercial datasets, and industry reports. It includes a literature review of the most notable source of the per-incident cost estimates, aggregate national and global estimates, as well as the most significant hypothetical scenario studies. In addition, it contains a detailed discussion of the issues with per-record cost estimates.

B.1 Secondary Sources: Commercial Datasets and Industry Reports

Below, OCE summarizes the per-incident loss estimates available in the most widely cited published research, commercial datasets, and industry reports.

Romanosky (2016)

A detailed analysis of cyber event costs is included in Romanosky (2016). Jointly with the overview of the cyber insurance content in Romanosky et al. (2019), it provides the most comprehensive coverage of the topic to date. Specifically, Romanosky (2016) studied 12,000 cyber events from the Advisen database to understand incident frequency, incident rate, and the cost of cyber incidents.[20] Although only 921 data points from 2005 to 2015 included cost data (7.6% of total observations), the analysis for this subset shows that the claims from cyber incidents ranged up to $750 million, with a median of $250,000 and average of $7.84 million.

Since the DGP across the incident costs is characteristic of a long-tail distribution[21], the average cost can be dominated by the costs of a few large events, while the median is a more informative statistic. The median cost of the cyber incidents captured in the relevant subset of Advisen data (i.e., the 921 observations with cost data) varied significantly across the four incident types analyzed in Romanosky (2016): data breach, security incident, privacy violation, and phishing or skimming. A summary of these results across the incident types is presented in Table 15.

While the median cost was the lowest for phishing or scamming approximately at $150,000, it increased to $170,000 for data breaches, $330,000 for security incidents, and $1.34 million for privacy violations.

Table 15: Romanosky (2016) Summary of Per-Event Costs by Event Type, $ Millions

Event Type	Number of Events	Cost per Event ($ millions)			
		Mean	Standard Deviation	Median	Max
Data Breach	602	$5.87	$35.70	$0.17	$572
Security Incident	36	$9.17	$27.02	$0.33	$100
Privacy Violation	234	$10.14	$55.41	$1.34	$750
Phishing	49	$19.99	$105.93	$0.15	$710
Total	**921**	**$7.84**	**$47.28**	**$0.25**	**$750**

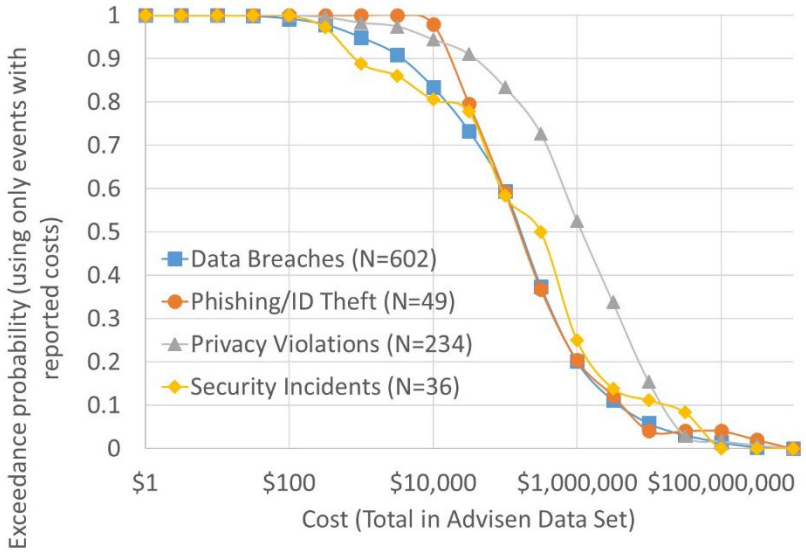
Note. Adapted from "Examining the costs and causes for cyber incidents," by S. Romanosky, 2016, *Journal of Cybersecurity*, 2, p. 129.

Another useful characterization of the data behavior within this Advisen subset is included in the RAND Corporation study (Dreyer et al., 2018). Namely, it contains exceedance probability curves for costs by the event type within the Advisen subset of records with cost. Exceedance probability curves from the RAND Corporation study for costs (on a logarithmic scale) across the four incident types are depicted in Figure 7. This curve denotes

[20] Advisen is "a US-based, for-profit organization that collects, integrates and resells loss and incident data to the commercial insurance industry regarding many different forms of corporate loss" (Romanosky, 2016, p. 122).
[21] The presence of a long tail (i.e., there are many occurrences with values that are far away from the main mass or "head" of the distribution) means there is a larger probability of getting very large values.

the probability that the costs will be greater than a given value. For example, for both data breaches and phishing/ID theft there is a 20% probability the costs exceed $1 million.

Figure 7. Exceedance Probability of Costs by Event Type



Note. Reprinted from *Estimating the global cost of cyber risk: Methodology and examples*, by P. Dreyer, K. Klima, J. Oberholtzer, A. Strong, J. W. Welburn, and Z. Winkelman, 2018, p. 45.

Note that since the Advisen data are not based a representative random sample of events, but rather a convenience sample[22], the interpretation is limited only to the underlying data—namely that the cost exceeds $1 million for 20% of only the incidents in the subset. Technically, it cannot be used for statistical inference, that is, it cannot be extended to imply that there is a 20% probability for any cyber incident to exceed $1 million in losses. However, because all of the available data on this subject comes from convenience samples, it inadvertently gets used for inference purposes.

Romanosky (2016) estimated that the total losses of the 7.6% of events in the Advisen dataset that contained cost estimates were approximately $6.5 billion. Using this total loss estimate as a crude approximation, Romanosky proportionately scaled the loss estimates to the full population of reported events in the Advisen dataset. Based on such scaling, Romanosky estimates cyber incident losses in the range of $85 billion over 10 years of data, which implies an annual average loss of about $8.5 billion.

Losses in the government sector are of particular interest for this report. Romanosky (2016) includes a breakdown of incidents by industry. The government sector has the third largest number of incidents across the Advisen dataset (i.e., 1,437 events over 10 years). That is an average of 140 to 150 cyber events per year. Note that this should not be used as a direct measure of relative risk, because the relative share of incidents within the dataset is driven by disclosure requirements and underlying differences in the reporting rates between sectors. Once normalized by the number of entities or firms within the government sector (90,107 entities) based on the U.S. Census Bureau (2013) data, the incident rate for the government sector is approximately 1.6%, which means on average 16 out of every 1,000 entities suffered an incident event within the analyzed timeframe.

[22] Convenience sampling is a type of sampling where the first available primary data sources are used for the research without additional requirements. For more information, please see https://research-methodology.net/sampling-in-primary-data-collection/convenience-sampling/

Considering all of the reporting limitations associated with this specific dataset, this annual estimate represents a lower bound.

Out of the 921 data points that contained cost information from 2005 to 2015, only 103 records (i.e., 11% of the subset with cost data and less than 1% of the overall Advisen dataset) were from the government sector. Overall, total losses for government entities across the 103 incidents approximated $205 million, which brings the average per-event estimate to about $2 million with a standard deviation of $5.72 million. Summary statistics for the government sector are included in Table 16:

Table 16: Romanosky (2016) Government-Sector Per-Incident Losses, $ Millions

Percentile	1%	5%	10%	25%	50%	75%	90%	95%	99%	Max
Cost ($ millions)	$0.000125	$0.00045	$0.0009	$0.02	$0.176	$0.833	$3.7	$16	$24	$39

A few large incidents in the subset strongly influence the average loss per event (i.e., two incidents at $20 million, one incident at $24 million, and one incident at $39 million). To illustrate this point further, consider the costs of the OPM breach. Advisen's initial estimate of the direct costs does not reflect the costs of the long-term credit monitoring contracts. While the immediate and direct losses from this incident are included in Advisen's estimate, the losses associated with extended credit monitoring and identity theft protection are not. In 2019, OPM awarded a $416 million contract for credit monitoring and identity theft protection to the security firm ID Experts on top of a previous $340 million contract (Katz, 2019). This brings the total direct cost of the OPM breach to approximately $761 million to date. Updating that single data point changes the average cost of the incident for the public sector from about $2 million to almost $7.3 million (almost 370%).

The median is not as strongly impacted by extreme observations. Thus, the median serves as a better statistic. The median loss per event for the government sector is about $176,000, which implies that the cost for 50% of the incidents within the subsample falls below this number. Additional insights can be gained by looking at the third quartile, as it excludes the handful of more extreme events. The third quartile shows that 75% of incidents in the public-sector subset have losses below $833,000.

OCE scaled up the sum of losses across the observations with cost data for the public sector (103 observations totaling $205 million in losses) to the 140 and 150 events recorded for the public sector on average per year. Doing so resulted in annual losses between $280 and $300 million. This number should be used with caution, as it represents a crude linear scaling of a subtotal in a small subset dominated by a few relatively large events. A summary of the scaled subset results is contained below in Table 17.

As explained in Coburn et al. (2018), historical data provide a view of only one specific realization of events or scenarios out of a myriad of possibilities that could have occurred instead. A short-sighted focus on only historical data limits the understanding of potential losses. Therefore, counterfactual analysis is necessary to enrich one's understanding of the full range of possible losses. Upward counterfactuals are the scenarios that are better than what was observed (i.e., losses are less than what were observed), while downward counterfactuals are the alternative scenarios that are worse than the observed ones (i.e., losses are higher than observed). A simplified exploration of six counterfactual cases developed by OCE is discussed below. The estimated average annual losses for each case are presented in Table 17.

A more conservative lower-bound loss estimate could be constructed by scaling up the median per-event estimate based on the annual event count, and then introducing several large events to balance the estimate. Given a median loss of $176,000 per incident, an average count of 140 to 150 incidents annually results in approximately $25 to $26 million in losses per year.

Table 17: Counterfactual Annual Loss Estimates for Government Subset, $ Millions

Case	Scaling Scenario	Annual Loss Estimate ($ Millions)
1	Median per-event loss ($176,000) scaled to 140–150 events per year summed with the losses from two large events ($20 million and $24 million)	$69–70
2	Median per-event loss ($176,000) scaled to the doubled number of events per year (280–300) summed with the losses from two large events ($20 million and 24 million)	$93–97
3	75th percentile value ($833,000) scaled to 140–150 events per year, no large events included	$117–$125
4	Scaling the annual estimate across all sectors down to the ratio of government losses to the sample total (3.2% of $8.5 billion)	$270
5	Total across Government subset ($205 million for 103 events) scaled to 140–150 events per year	$280–$300
6	Average per-event loss for the Government subset average ($2 million) scaled up to 140–150 events per year summed with the losses from three large events added in ($20 million, $24 million, and $40 million)	$364–$384

Adding two large events with losses between $20 and $24 million each brings the annual loss estimate for the government sector to about $69 to $70 million (see Case 1). If the average annual event count is doubled, this increases the annual loss estimate from $93 to $97 million (see Case 2). If instead of the median, the 75th percentile value is scaled up to the average annual event count of 140 to 150, but large events are treated purely as outliers (therefore, excluded from scaling), the annual loss estimate increases from about $117 to $125 million (see Case 3).

As mentioned earlier, summing the losses across all events included in the Government subset results in a total loss of about $280 to 300 million, which is captured in Case 5 (103 observations totaling $205 million in losses scaled up to the 140 and 150 events per year). Additional benchmark points can be established by comparing government records with total losses ($205 million) to the full losses in the subset with available cost data ($6.5 billion), and then taking the same ratio (i.e., approximately 3.2%) off of the estimated annual total of $8.5 billion across all sectors. The estimate for this case is similar to the initial crude scaling scenario and equals approximately $270 million (see Case 4).

If the subset average of approximately $2 million is taken to represent a less conservative scenario, when scaled up to 150 incidents per year with the same three large events included on top, the estimate starts to approach $400 million (see Case 6).

The objective of this scaling exercise is to emphasize how the aggregate estimates can vary considerably depending on the scenario assumptions, even when the underlying empirical basis for the cost values is identical. Factoring in the current state of cyber loss data tracking and reporting (i.e., multiple sparse datasets across a large number of agents with narrow focuses) further highlights the potential for distortion within various loss calculations and derived risk estimates. This point is discussed in more detail in Section 4.

It is important to clarify what costs and losses are reflected in the collected event and incident data in order to use the loss estimates within the proper context. The loss data in the Advisen dataset represents only the subset of incidents that were detected, disclosed in the publicly available data sources, and recorded in the database. The database is constructed by a team of analysts who continuously collect cyber-event-related information from media and public sources. As discussed in Romanosky (2016), cost and loss estimates are available only for a

small fraction of records in the database—specifically, (1) only for disclosed incidents and (2) only if the claims were filed or if the entity chose to disclose the impact values in publicly available sources. Thus, estimates included in the analysis are a convenience sample that lacks the representativeness required to support statistical inference. This means results are only valid within the context of the specific observations and should not be applied to the rest of the population. This is another way to say that scaling, extrapolation, or any out-of-sample inference is not appropriate.

Per-event loss values should be treated as a lower-bound estimate of potential losses, not only because of reporting limitations with respect to event occurrences versus disclosure guidelines, but also from the standpoint of the loss types reflected in the damage assessment.

As shown in Romanosky et al. (2019), the damage estimates typically include first- and third-party losses that are not accounting- or invoice-based actuals, but mostly self-reported estimates. While the values for reported loss categories could be overstated, not all relevant loss categories get factored in. Typically, lost revenue, opportunity costs, goodwill, market reputation, change in market value, consumer confidence, or loss of competitive advantage do not get included in the estimates. Neither do the costs to consumers, externalities, or impacts to the larger economy. While the values in individual loss categories may be overstated, the estimates presented in the analyzed dataset underestimate the overall level of costs, losses, and impacts from the cyber events and incidents. Therefore, the per-event estimate, either for the government sector or across all incident types and sectors, should only serve as a notional lower bound.

Cyentia Institute (2020)

A more recent analysis of the Advisen dataset is included in the Cyentia (2020) report. The report dissects the 2009 to 2019 data by various segments, including Fortune 1000 companies and SMBs. The report also compares incident frequency and loss magnitude by sector. For context, out of the 52,000 cyber events comprising the 2009–2019 version of the dataset, only 1,900 records include loss magnitude data. The latter subset is of special interest, as it contains specifics relevant to public-sector incidents (i.e., those classified under the North American Industry Classification System code 92).

When comparing incident frequencies across sectors within a rolling 1-year window, the public sector has the highest rate. For the public sector, the annual probability that any given organization will experience a breach is about 5%. For remaining sectors, the annual probability is below 1%. Note, this result is heavily caveated by the fact that while incidents and breaches are underreported in the private sector, the public sector has a more mature set of disclosure requirements and guidelines, which is similar to the traditional disclosure in the Verizon (2018, 2019, 2020) DBIRs.

An additional cross section of value is the comparison of the breach frequency by revenue, which is used as a proxy for the organization size. The results indicate that organization size as expressed by annual revenue is the strongest single factor explaining significant differences in incident frequencies. For organizations with over $100 billion in revenue, the incident likelihood is approximately 75%, while it drops to about 23% for revenues between $10 billion and $100 billion, and down to 10% for revenues between $1 billion and $10 billion. In addition, the Cyentia (2020) report offers a detailed breakdown of incident likelihood for multiple incidents by organization size. However, the same caveats about interpreting the results apply here as well—the relative event frequency calculation is limited by the extent it is reflected in the disclosed incident data.

Cyentia's (2020) loss magnitude analysis shows that the median cost in this most recent dataset is $196,000 per breach, which is higher than the median cost of $170,000 in the older edition of the Advisen data analyzed in Romanosky (2016). The report emphasizes the heavy-tailed distribution of the loss magnitude data and explains in detail why using the arithmetic mean is misleading. While the average loss is about $19.1 million, 90% of the breaches cost less; therefore, it is not a good representation of the central tendency in the magnitude

loss data. The primary reasons are two-fold. First, the arithmetic mean is strongly impacted by the extreme values. Second, larger breaches are more likely to get disclosed and to garner media attention. Therefore, larger incidents are more likely to be included in databases that rely on scraping publicly available data. Instead, the report offers the median ($196,000) and geometric mean ($205,000) as better statistics to describe central trends in the loss magnitude data.

As expected, the median loss magnitude varies significantly by sector. The information, manufacturing, and retail sectors have the highest median losses per incident ($782,000, $604,000 and $536,000, respectively). Notably, the public sector has the lowest median per-incident cost of $132,000, which is lower than the median cost for the public sector in the older 2005–2015 Advisen dataset ($176,000). However, this should not be interpreted as a significant reduction in the per-incident cost within the public sector. It is more likely that due to more mature disclosure requirements and policies, more of the smaller incidents were disclosed in the public sector compared to the private sector over the last several years.

Along with the public sector, the lowest loss magnitude median is observed in the healthcare and financial sectors ($136,000 and $151,000, respectively). Similarly, being more tightly regulated with respect to disclosure, the healthcare and financial sectors have relatively heavier representation in this specific dataset, with smaller and less costly incidents being more frequently reported than in other less regulated sectors.

The distribution of losses by organization size also shows a significant variation in loss magnitude. However, the cross section of interest to OCE's study is the distribution of magnitude loss by organization size within the public sector, which is not a focus of the Cyentia (2020) report. To facilitate more detailed analytics for the cross sections of interest to the federal government and SLTT community and to support the analysis on an ongoing basis, CISA OCE has acquired the primary Advisen dataset.

NetDiligence (2017, 2018, 2019)

NetDiligence (2017, 2018, 2019) provides another useful source of detailed information on claim payouts and total incident costs. The *NetDiligence 2017 Cyber Claims Study* contains summary statistics for claims and losses associated with 514 incidents that occurred from 2014 to 2017. The number of the analyzed data points more than doubled in the 2018 study (i.e., 1,201 observations from 2013 to 2017). While over 500 new claims were added for incidents from 2015 to 2017, 298 observations reflect incidents that occurred in 2017. The *NetDiligence 2019 Cyber Claims Study* added almost 1,100 new data points for incidents occurring from 2016 to 2018, which increased the total sample size to 2,081 claims. Of that, 649 claims covered the events occurring in 2018.

The results of the NetDiligence studies are extremely valuable because they represent the very few primary research reports that are based on actual data for losses and resulting claims for the same set of the incidents without exogenously informed extrapolation or multiplier-based scaling. The claims cost and loss estimates are drawn from actual insurance claims data provided by the partner insurance companies that paid the claims. In addition, the report clearly explains the study methodology, underlying assumptions, and limitations.

Summary statistics for the NetDiligence (2017, 2018, 2019) total incident costs across the convenience sample of the observations from 2013 to 2018 are presented in Table 18.

Table 18: NetDiligence (2017 2018, 2019) Summary of Per-Event Costs

Study Publication Year	Number of Events	Cost per Event ($ thousands)			
		Mean	Standard Deviation	Median	Max
2017	514	$394	$1,531	$56	$16,849
2018	1,201	$604	$3,568	$61	$80,000

Sources: NetDiligence (2017, 2018, 2019)

The 2018 and 2019 NetDiligence reports break down the sample by annual revenue size, because the summary statistics differ significantly between the two subsets and there is a sufficient number of observations to support subsetting. For SMBs, the median cost of a cyber incident in 2019 dataset was approximately $48,000, with an average of $178,000 (2,003 data points comprising 96% of the sample). In the 2018 dataset, the median incident cost for SMBs was approximately $55,000, with an average of almost $226,000 (1,011 datapoints comprising 85% of the sample).

The change in median does not represent net decrease in per-incident cost from 2018 to 2019. There are multiple reasons for this change. First, both reports look at the cumulative sample of claims over a 5-year horizon (i.e., 2013–2017 and 2014–2018). Second, the size of the SMB subset nearly doubled from the 2018 to 2019 report, with not only a higher number of closed claims, but a heavier fraction of claims in the lower segment of the distribution. Similarly, the change in the average is explained by fewer SMB incidents with extreme loss totals (i.e., tail of the distribution) in the updated 2014–2018 sample.

For large organizations, the median incident cost did not change from 2018 to 2019. The median was approximately $1 million, with the average reaching $5.6 million in 2019 report (78 data points) and $5.2 million in 2018 report (82 data points). Again, this change does not represent a net increase in the per-incident cost but is rather a manifestation of several higher claims for large entities getting closed and added to the 2014–2018 dataset. The impact of higher-cost incidents— specifically extreme incidents—on the average is so severe that the average itself resides in the fourth quartile (the 75th percentile of the cost distribution for large entities is approximately $5.17 million). This again shows why the median is a more suitable statistic than the average for cyber incident cost data.

For public entities, the sample size remains limited (38 data points in the 2018 report and 66 data points in the 2019 report). The median cost of $57,000 per incident was unchanged, while the average increased slightly from $78,000 to $96,000 due to the addition of a few significantly higher cost claims to the dataset. (The maximum for this subset more than quadrupled from $328,000 to $1.4 million.)

A comparison of the total payout and the total incident cost, and a breakdown of the total incident costs by loss category from the NetDiligence (2019) study are presented in Table 19.

Table 19: NetDiligence (2019) Per-Event Cost by Cost Category, $ Thousands

Cost Category	Cases	Per-Event Cost ($ thousands)			
		Median	Mean	Max	Std. Dev
SMBs					
Total Payouts	**1,753**	**$39**	**$136**	**$10,000**	**$584**
Total Incident Costs	**2,003**	**$48**	**$178**	**$20,000**	**$852**
Total Crisis Services Costs	1,334	$33	$112	$8,209	$457
Forensics Costs	935	$26	$72	$4,900	$258
Notification Costs	350	$8	$75	$5,520	$397
Credit/ID Monitoring Costs	295	$5	$45	$2,000	$202
Legal Guidance/Breach Coach Costs	1,123	$11	$28	$1,060	$71
Other Crisis Services Costs	168	$14	$60	$1,065	$166
Legal Damages-Defense Costs	181	$14	$78	$2,500	$229
Legal Damages-Settlement Costs	97	$50	$264	$6,758	$866
Regulatory-Defense Costs	12	$41	$95	$368	$112
Regulatory Fines	9	$14	$19	$60	$18
PCI Fines	19	$68	$700	$4,235	$1,308
Lost Business Income	95	$45	$343	$10,000	$1,260
Recovery Expense	89	$14	$45	$500	$92
Large Entities					
Total Payouts	**51**	**$696**	**$3,784**	**$56,500**	**$8,655**
Total Incident Costs	**78**	**$1,000**	**$5,553**	**$80,000**	**$12,334**
Total Crisis Services Costs	46	$369	$3,843	$64,000	$10,582
Forensics Costs	30	$275	$2,036	$33,000	$6,059
Notification Costs	22	$131	$2,400	$23,000	$5,643
Credit/ID Monitoring Costs	16	$55	$1,688	$13,000	$3,901
Legal Guidance/Breach Coach Costs	33	$70	$954	$21,000	$3,643
Other Crisis Services Costs	13	$20	$218	$2,000	$543
Legal Damages-Defense Costs	8	$502	$1,380	$5,000	$1,786
Legal Damages-Settlement Costs	3*	-	-	-	-
Regulatory-Defense Costs	5	$100	$1,235	$5,791	$2,549
Regulatory Fines	1*	-	-	-	-
PCI Fines	2*	-	-	-	-
Lost Business Income	1*	-	-	-	-
Recovery Expense	1*	-	-	-	-

Note. Source: NetDiligence (2019)
* Omitting summary statistics for cost categories with fewer than five cases.

For SMBs, payout estimates ranged up to $10 million, with an average of about $136,000 and a median of about $39,000. For large entities, payout estimates ranged up to $56.5 million, with an average of about $3.8 million and a median of about $696,000.

Comparing the median payout to the median incident cost is not appropriate. Instead, the median of the ratio of the payout to the total incident cost should be estimated by first finding the ratios for the entire sample and then calculating summary statistics for the distribution of ratios. For the 2018 report, the median of the ratio between

the payout and total incident cost is approximately 83%.[23] The simple average of the ratio between total payout and total incident cost is about 74%. For 2019 report, average payout ratio for SMBs was approximately 76% with a median of 85%. For large entities, the average payout ratio was lower at approximately 68% with a median of 80%.

Claims or payout data are the types of incident cost data most readily available to insurers. However, using the claims loss data to infer total actual losses from the relevant incident types is problematic for several reasons discussed below.

First, some of the most relevant cost and loss types that can make up a significant part of the impact estimate would be omitted from claims data due to policy-specific exclusions in coverage. For example, the NetDiligence (2017, 2018, 2019) studies are focused primarily on specific incident-related expenses and do not include other impacts such as investigation and administrative expenses, customer turnover, and opportunity costs. A detailed treatment of insurance policy coverage and its associated issues is included in Romanosky et al. (2019).

Second, besides policy coverage terms and exclusions, payouts within the covered categories are restricted based on policy-specific limits and sub-limits, irrespective of the magnitude of the actual loss.

Third, insurance companies would not necessarily get data for the incidents that were settled within self-insured retention (SIR), which is a pre-specified amount of cost that the insured company has to directly pay before any insurance payout kicks in. In 2018 and 2019, SIR limits ranged up to $20 million and $15 million, respectively (NetDiligence, 2018, 2019). Any incidents with non-trivial loss magnitudes that did not exceed these SIR limits would have been omitted from the data.

Fourth, the claims data are not based on a representative random sample, but rather a convenience sample, thus lacking statistical significance to support inference. Results from the claims sample cannot be extended to support conclusions about the larger universe of the cyber incidents. The methodology section of the NetDiligence reports (2017, 2018, 2019) is both clear and concise in disclosing assumptions and limitations, which adds significant value to the reported results.

Fifth, the willingness to share even this segmented cost and loss data in the current data-sparse environment is limited, as it represents a business opportunity for insurance companies, the risk analysis industry, and cybersecurity companies establishing their own cyber insurance or risk management product lines. From that standpoint, NetDiligence's collaboration with insurance companies that are contributing the microdata and consuming the aggregate analysis, represents a significant advancement in the data-sharing space.

The difference between the payout costs and the total incident costs yet again highlights the importance of considering the reporting boundaries, underlying assumptions, and data collection methods when developing potential loss estimates. If actual total damage assessments data are not available, claims data can serve as a proxy for the lower bound of potential losses. Because fixed limits and sub-limits for each of the covered damage categories vary widely from policy to policy, using claims data as a lower bound to quantify the losses should always be caveated with the understanding that this simplification underestimates losses without any indication of how much. To overcome this challenge, as part of their cyber claim studies, NetDiligence started requesting estimates of the total incident cost, including the amounts that were excluded by the policy.

The results for the total incident cost contained in the NetDiligence (2017, 2018, 2019) reports that span from 2013 to 2018 are lower than those in the Advisen data analyzed in Romanosky (2016) or Cyentia (2020). Note that due to the relatively small convenience sample and large variability within both datasets, it is not possible to

[23] Statistics for the ratio between payout and the total breach cost are not included in the Cyber Claims study. They were provided to OCE courtesy of NetDiligence.

claim whether the difference in results is significant or not. For comparison, the NetDiligence (2017, 2018, 2019), Romanosky (2016) and Cyentia (2020) results are presented in Table 20.

Table 20: NetDiligence (2017, 2018, 2019), Romanosky (2016), and Cyentia (2020) Per-Event Costs

Study	Number of Events	Cost per Event			
		Mean	Standard Deviation	Median	Max
NetDiligence (2017)	514	$393,739	$1,530,798	$56,143	$16,849,411
NetDiligence (2018)	1,201	$603,900	$3,568,000	$61,000	$80,000,000
NetDiligence SMB (2018)	1,011	$226,000	-	$55,000	$11,750,000
NetDiligence Large (2018)	82	$5,159,000	-	$1,000,000	$80,000,000
NetDiligence SMB (2019)	2,003	$178,000	$852,000	$48,000	$20,000,000
NetDiligence Large (2019)	78	$5,553,000	$12,334,000	$1,000,000	$80,000,000
Romanosky (2016) – Full Advisen Dataset	921	$7,840,000	$47,280,000	$250,000	$750,000,000
Romanosky (2016) – Advisen Data Breach Subset	602	$5,870,000	$35,700,000	$170,000	$572,000,000
Cyentia (2020)– Full Advisen Dataset	1,900	$19,100,000	-	$196,000	>$1 billion
Cyentia (2020) – Advisen Public-Sector Subset	-	$13,000,000	-	$132,000	~$1 billion

Sources: NetDiligence (2017, 2018, 2019), Romanosky (2016), Cyentia (2020)

The difference in results could be easily explained by the difference in the reporting time intervals contained in both datasets as well as the composition of the convenience samples. Romanosky (2016) is based on Advisen data from 2005 to 2015, Cyentia (2020) summarizes a more recent Advisen dataset (i.e., from 2009 to 2019), while the NetDiligence (2018) study is based on a sample of data from insurers and underwriters on a 5-year rolling window.

The data collection methods serve as another source of differences. While Advisen data is based on the collection of published third-party estimates of incident costs, Freedom of Information Act requests, and court records, NetDiligence data come directly from the major underwriters paying the claims. Also, 85% of the NetDiligence 2018 sample and 96% of the 2019 sample consist of SMBs with less than $2 billion in annual revenues. Refer to NetDiligence (2018, 2019) and Cyentia (2020) for a detailed breakdown of the incident costs by revenue size.

An additional discrepancy in the incident cost estimates could stem from the fact that the incident types included in the NetDiligence (2018, 2019) study represent a different set of incident types and causes than the Advisen data analyzed in Romanosky (2016) and Cyentia (2020). A breakdown of the NetDiligence (2018) incident costs by incident type is presented in Table 21.

Table 21: NetDiligence (2019) Cost per Incident by Loss Category

Category	Cases	Cost[a] ($ thousands)			Rank (Median)
		Mean	Median	Max	
SMB					
Business email compromise (BEC)	164	$156	$67	$3,400	6
Hacker	285	$337	$74	$7,400	4
Legal action/Third party	112	$241	$51	$10,000	12
Lost/stolen laptop/device	95	$76	$27	$1,500	15
Malware/Virus	142	$308	$70	$9,000	5
Negligence	7	$58	$27	$135	16
Paper records	23	$69	$25	$650	17
Phishing	133	$80	$37	$1,100	14
Programming error	24	$305	$63	$3,600	8
Ransomware	478	$150	$40	$20,000	13
Rogue employee	80	$151	$60	$2,500	9
Social engineering	547	$107	$54	$3,400	11
Staff mistake	120	$78	$25	$2,500	18
System glitch	10	$1,900	$79	$17,500	3
Theft of money	9	$123	$67	$470	7
Trademark/Copyright Infringement	9	$149	$60	$468	10
Wire transfer fraud	106	$180	$105	$1,400	1
Wrongful data collection	1	$86	$86	$86	2
Large Entities					
Business email compromise (BEC)	3	$341	$77	$875	15
Hacker	20	$7,900	$2,600	$64,000	5
Legal action/Third party	11	$1,900	$1,600	$5,000	6
Lost/stolen laptop/device	4	$699	$142	$2,500	13
Malware/Virus	18	$6,900	$4,600	$33,000	3
Negligence	-	-	-	-	-
Paper records	4	$35	$18	$100	16
Phishing	1	$165	$165	$165	11
Programming error	1	$678	$678	$678	7
Ransomware	1	$15,000	$15,000	$15,000	2
Rogue employee	6	$4,300	$4,600	$11,500	4
Social engineering	9	$409	$165	$1,500	12
Staff mistake	4	$813	$325	$2,500	9
System glitch	1	$80,000	$80,000	$80,000	1
Theft of money	1	$103	$103	$103	14
Trademark/Copyright Infringement	-	-	-	-	-
Wire transfer fraud	2	$990	$505	$1,500	8
Wrongful data collection	1	$249	$249	$249	10

Note. Adapted from *NetDiligence 2019 Cyber Claims Study* by NetDiligence, 2019, pp. 28 and 30.

[a] The total cost per incident includes SIR.

For SMBs, the top five incident types with the highest median cost are wire transfer fraud ($105,000), wrongful data collection (an isolated event at $86,000), system glitch ($79,000), hacker ($75,000), and malware ($70,000). The top five incident types by the number of cases are social engineering (547), ransomware (478), hacker (285), business email compromise (BEC; 164), and malware/virus (142). Ransomware and system glitch are incident types with the highest maximum cost ($20 million and $17.5 million, respectively).

For large entities, the top five incidents by median cost are system glitch ($80 million), which is a single network outage incident that has the highest losses across the entire 2014–2018 sample, ransomware ($15 million), and malware/virus and rogue employee ($4.6 million each). By the number of cases, the top incident types are

hacker (20), malware/virus (18), and legal action/third party (11). The incidents with the highest maximum cost are system glitch ($80 million), hacker ($64 million), malware/virus ($33 million), ransomware (a single event at $15 million), followed by rogue employee ($11.5 million).

Breaking down the cost by incident type, beyond data breaches, is exceptionally useful for incidents that have to do with the loss of integrity or availability, as opposed to confidentiality. Data on the latter is more easily obtainable.

Note that the cost summaries presented in Table 21 do not attempt to break down the incident costs by year. There are four primary reasons for operating with data aggregated over the longer 2014 to 2018 time period. First, the sample is not representative enough to test the difference in incident frequency and magnitude from year to year and infer it for the rest of the population. Thus, the interpretation of the results is restricted to the actual observations. Second, the data is very sparse across both the loss categories and loss causes even within the 5-year span, let alone from year to year. Third, typically, the final tally of costs and losses is not known within the year of the incident, because losses occur and accumulate over several years after the incident, especially if litigation and class action suits are involved. Thus, a calendar year is not a meaningful basis for cost and loss comparison. Fourth, empirical research into the frequency and size of the incidents does not support conclusions regarding upward or downward trends in either of those variables.

Namely, Edwards et al. (2016) examined information on 2,253 publicized data breaches in the PRC dataset. The findings show that neither the size nor the frequency of breaches changed over time within the analyzed dataset, but rather manifested a fluctuation that is consistent with a DGP characteristic of a long-tail distribution. In other words, there are many extreme values at the high end of the distribution, which implies several large incidents may appear in any given year. While these extreme values drive the average cost for that year up, they do not represent a change in the average incident costs in the underlying distribution over a longer time horizon.

In addition to providing the payout costs and the total incident cost with detailed itemization across loss categories, incident types, and revenue sizes, the extended version of the NetDiligence (2018, 2019) reports have detail related to the summary results and itemized results for major cost categories in quantile form. This is an exceptionally valuable information, as it enables quantification for the bottom-up activity-based costing frameworks for risk analysis to capture potential loss variability, while preserving the anonymity and preventing re-identification of the individual incidents. It also allows an analyst to produce synthetic data that while statistically equivalent to the original sample, could be used to initially mask subsequently contributed data points, if cost tracking and primary data collection were to be undertaken by any individual organization or sector.

RBS (2018)

RBS collects microdata on cyber incidents and their characteristics such as incident type, number of records, year, sector, location, and annual revenue of the impacted companies. The dataset contains rich detail on over 35,200 incidents mostly from 2000 to 2018, with a handful of incidents dating back several decades.

The subset of data containing records on the cost of the incidents is the most relevant for this analysis. There are 387 data points that include records on court costs, non-court costs, or both for cyber incidents for 21 countries. U.S. incidents comprise over 65% of this subset (253 data points), with 62 data points containing cost estimates for public-sector incidents (i.e., 38 records related to Government and 24 records related to Education). Summary statistics for the U.S. segment of the RBS data that contain cost records are presented in Table 22.

Table 22: RBS (2018) Summary of Per-Event Costs (U.S.)

RBS Subset	Number of Events	Cost per Event ($ thousands)			
		Mean	Standard Deviation	Median	Max
U.S. Dataset	252	$14,253	$52,834	$609	$391,500
Public-Sector Subset (Government & Education)	62	$2,569	$11,297	$122	$86,300
Government-Only Subset	38	$3,342	$14,021	$200	$86,300

Source: RBS (2018)

The average cost of an incident in the U.S. data is $14.3 million, while the median is $609,000. For the public sector, which includes the federal government, SLTT governments, and public education institutions, the average is approximately $2.6 million, while the median is $122,000. For government-only records, the average is about $3.3 million and median is approximately $200,000. Although the caveats about the averages are also relevant here, estimates for the public-sector and government subsets are of a comparable order of magnitude to Romanosky's (2016) public-sector results (i.e., an average of $2 million and a median of $176,000).[24]

There is a large gap among the costs of the five largest incidents in the public-sector subset (i.e., $3 million, $5 million, two incidents at $20 million, and the largest one at $86 million). Removing the largest incident from the subset reduces the average to $1.2 million and the median to about $87,000, thus putting the estimates on the comparable basis with the NetDiligence (2018) results. Moreover, removing the two next highest incidents (i.e., $20 million) from the public-sector subset drops the average to approximately $560,000 and the median to $81,000, firmly leveling the estimates with NetDiligence (2018).

Similarly, removing the same largest incident from the government-only subset drops the average from $3.3 million to $1.1 million and the median from $200,000 to $185,000, thus leveling it with the Romanosky (2016) estimates. Dropping the next largest incident (i.e., $20 million), decreases the average to about $575,000, again, putting it very close to the NetDiligence (2018) estimate of $604,000.

Ponemon Institute (2013, 2014, 2015, 2016, 2017b, 2018, 2019)

Another frequently cited study on the cost of cyber incidents is the Ponemon Institute annual report series. It provides an additional set of reconciliation points to compare with the NetDiligence (2017, 2018, 2019), Romanosky (2016) and Cyentia (2020) summaries. While the Ponemon Institute publishes both a global and U.S. series of estimates, the discussion below centers on the U.S. results, as they are more relevant to the CSD mission space. Although incident cost totals are reported in Ponemon (2018, 2019), the detailed breakdown by cost category highlighting the structural assumptions is only available in 2017 report. For proper context as to the applicability of the estimates, the discussion here first introduces the high-level estimates contained in Ponemon (2017, 2018, 2019) followed by the details included in Ponemon (2017) that are not available in the subsequent versions of the report.

The 2017 Ponemon report for the United States indicates that the average cost of a breach equaled about $7.35 million. The estimate increased to $7.91 million in the 2018 study and to $8.19 million in the 2019 version. These averages vary significantly with the size of the breach and size of the organization. Arguably, the latter two factors are strongly correlated. A breakdown of the total breach costs by cost category is presented in Table 23.

Note that the cost estimates in the Ponemon Institute reports cover a larger set of cost and loss categories than the previously discussed studies. For example, abnormal customer churn is factored into the lost business cost

[24] The averages for the RBS (2018) public-sector and government subsets belong to the 90th percentile and 93rd percentile of their respective distributions (i.e., far in the tail).

estimates, as well as diminished further customer acquisition, the cost of the subsequent customer acquisition programs, loyalty programs, and other opportunity costs, reputation losses, and diminished goodwill. Those cost categories are not incorporated in the previous four studies (Romanosky, 2016; Cyentia, 2020; Net Diligence, 2017, 2018, 2019; RBS, 2018), as they are typically not allowed for inclusion in the damage assessments. This especially concerns the future unrealized opportunity costs. A more detailed breakdown of the Ponemon Institute's (2017b) costing categories is presented in Table 24.

Table 23: Ponemon Institute (2017b), U.S. Per-Event Cost by Cost Category

Cost Category	Cost per Event ($ millions)	Percentage
Average Detection & Escalation	$1.07	15%
Notification	$0.69	9%
Post Data Breach	$1.56	21%
Subtotal	**$3.32**	**45%**
Lost Business & Opportunity Cost	$4.03	55%
Total Breach (n=63)	**$7.35**	**100%**

Note. Source: Ponemon Institute (2017b). The Ponemon Institute (2018, 2019) studies do not contain a U.S.-specific breakdown. Therefore, the 2017 edition is used for the U.S.-specific results. For comparison, lost business and opportunity costs comprise 36.2% of the global cost estimate in Ponemon Institute (2019).

Table 24: Ponemon Institute (2017b) Data Breach Cost by Cost Category

Cost Category	Percentage of Total Breach Cost	Breach Cost ($ millions)
Investigations & Forensics	16%	$1.18
Audit & Consulting Services	4%	$0.29
Outbound Contact	3%	$0.22
Inbound Contact	4%	$0.29
PR	1%	$0.07
Legal - Defense	17%	$1.25
Legal - Compliance	3%	$0.22
Free or Discounted Services	1%	$0.07
Identity Protection Services	2%	$0.15
Subtotal	**51%**	**$3.75**
Lost Customer Business	41%	$3.01
Customer Acquisition	8%	$0.59
Total	**100%**	**$7.35**

Note. Adapted from *2017 Cost of Data Breach Study: United States* by Ponemon Institute, 2017b, p. 20. There appears to be a discrepancy about the percentage of data breach costs related to lost business. Using the Ponemon Institute's (2017b) costs presented in Table 23, lost business accounts for approximately 55% of total breach costs. However, the Ponemon Institute estimates that lost customer business and customer acquisition costs jointly represent 49% of the total. As presented in Table 23, the Ponemon Institute estimated that the total breach cost excluding lost business was $3.32 million, but using the percentages reported by the Ponemon Institute in Table 24, the total breach cost excluding lost business and customer acquisition costs could be as high as $3.75 million.

Regrettably, only averages are included in the report without any additional information about the ranges for each category. Relying on the averages of a very small sample has significant limitations discussed in detail in Section 3.1. Similar to the previously discussed studies, the data in the Ponemon Institute reports are

convenience samples of a small size. The basis for the 2017 Ponemon Institute U.S. study results is a convenience sample of 63 U.S. companies in 16 industry sectors. Half of the events in the sample were caused by malicious or criminal activity, with the remaining half being split almost equally between negligent employees and system glitches. Also, breaches where more than 100,000 records were compromised were not included in the 2017 study. The 2018 study was based on 65 observations for the United States across 17 sectors, with 2019 U.S. sample including 64 datapoints. To address large breaches, a separate estimate was developed in Ponemon Institute (2018, 2019). However, the reports do not include sample statistics or a detailed explanation of the methodology beyond a generic mention of the Monte-Carlo simulation or activity-based costing.[25]

The Ponemon Institute (2017b) report also compares how costs vary depending on the time to detect and contain a data breach. The 2017 U.S. report suggests it takes an average of 206 days to detect an incident and an average of 55 days to contain it, while 2019 data for the United States shows a slight reduction—196 days to identify and 49 days to contain. A summary of how the average cost varies by the average detection and containment time is presented in Table 25.

Table 25: Ponemon (2017b) Cost Estimate by Mean Detection and Containment Time

Metric	Time Interval	Average Cost per Breach ($ millions)
Mean Time to Identify	<100 days	$5.99
	≥100 days	$8.70
Mean Time to Contain	<30 days	$5.87
	≥30 days	$8.83

Source: Ponemon Institute (2017b)

It should be noted that results published in the Ponemon Institute's (2017b) annual data breach study are not direct summaries of the primary collected data. The Ponemon Institute's annual study is based on an undocumented proprietary benchmark method applied to the survey or interviews of the companies that had a data breach occur within the last 12 months. The loss results are internally derived by the Ponemon Institute from the estimates provided by the subject matter experts of the breached companies during the interviews. The methodology is not disclosed, and a discussion of validation and verification is also omitted from the documentation. In addition, the discussion of the results does not clarify which sets of results are descriptive statistics for the observations in the sample versus the secondary results derived internally (from the benchmark method or other methods).

As stated in the Limitations section of the Ponemon Institute (2017b) report, "Statistical inferences, margins of error and confidence intervals cannot be applied to these data given that our sampling methods are not scientific" (p. 25). The Ponemon Institute (2019) does not offer much additional detail regarding the methodology. Therefore, the same disclosure that the applicability and interpretability of results should be restricted only to the sample observations applies here as well. An additional disclosure in the Limitations section states, "the use of cost extrapolation methods rather than actual cost data may inadvertently introduce bias and inaccuracies" (Ponemon Institute, 2017b, p. 25). This seems to confirm that the results derived in the Ponemon Institute study are based on the internally developed cost extrapolation methods. For example, the identification of the impact that 20 various factors have on the cost of the breach presented in the report may have been derived via regression in deviation form, which leaves room for speculation regarding the quality of the model fitting 63 observations across 20 dimensions with sparse data. Therefore, besides the potential for introducing

[25] The generic explanation seems to indicate that bootstrapping of the cost elements was performed. However, there is no explanation of the actual design specification (e.g., how the random variables were constructed and over what domain they were simulated). A recognized weakness of any Monte-Carlo simulation is the results are design-specific. This significantly limits defensibility, and as a result, the usefulness of the derived estimates.

bias and inaccuracies as mentioned in the report, the black box approach significantly limits the defensibility of results and prevents comparison and reconciliation with other sources.

For the reasons mentioned in the overview of the previous studies, a comparison of the year-by-year results is omitted from this discussion. The calendar year is not a meaningful metric for reporting the costs of cyber incidents, as they can easily span several years, which would be typical for legal defense and legal compliance cost categories. This aspect is confirmed in the Ponemon Institute (2019) study showing that 67% of the costs occur in the first year, with another 22% occurring in year 2, and the remaining 11% in the subsequent years. Also, the Ponemon Institute (2019) reports a significant difference in cost accumulation over time between low and high regulatory environments. In addition, the difference from year to year could not be formally tested to support conclusions regarding its significance.

In light of those reasons (i.e., the findings in Edwards et al. (2016), the long-tail distribution of the underlying DGP, and the limited defensibility of annual averages derived on the basis of 50 to 66 observations from such a DGP as a meaningful metric), the discussion of year-to-year changes has limited value. The Ponemon Institute estimates could potentially be refined by combining the information from multiple years into a pooled sample and reporting the summary statistics of the underlying sample data, along with the quantiles for the derived results in a manner similar to NetDiligence summaries.

Baker Hostetler (2017, 2018, 2019, 2020)

Baker Hostetler's (2019, 2020) Data Security Incident Response Reports provide a valuable factual summary of incident response trends including top causes, incident response timelines, affected industries, and forensic investigation costs for network intrusions and non-network intrusions. OCE presents the average investigation costs reported in the Baker Hostetler reports from 2017 through 2020 in Table 26.

Table 26: Baker Hostetler (2017-2020) Average Per-Event Investigation Costs

Study Publication Year	Number of Incidents	Investigation Cost			
		Average for All Incidents, $	Average for Network Intrusion, $	Average for 20 Largest Investigations, $	Maximum Investigation Cost, $
2017	450	$62,290	$93,322	$257,602	> $750,000
2018	560	$84,417	$86,770	$436,938	N/A
2019	750	$63,001	$120,732	$350,576*	N/A
2020	950	$58,034	$65,227	$350,576*	N/A

Note. Source: Baker Hostetler (2017–2019).
* Average of the 20 largest network intrusions.

The costs in Table 26 are based on the data collected for 450 incidents in the 2017 report, 560 incidents in the 2018 report, 750 incidents in the 2019 report, and 950 incidents in the 2020 report. The average investigation costs across all incidents have not changed significantly from 2017 to 2019, though they have dropped slightly in 2020. There was only a temporary increase in 2018.

Network intrusions have a longer incident response timeline, and they are more costly to investigate. Namely, the average cost for a network intrusion in 2017 and 2018 ranged between $93,000 and almost $87,000, with the cost increasing to over $120,000 in 2019 and dropping to approximately $65,000 in 2020.

The average cost for the largest 20 investigations increased from around $258,000 to almost $437,000 between 2017 and 2018. In 2019, instead of providing the average cost for the largest 20 investigations, Baker Hostetler (2019) cited the average costs for the 20 largest network intrusions ($351,000), with the same number shown in 2020. Although network intrusions seem to take longer to respond and are costlier to

investigate on average (see Table 27 below), it does not necessarily mean that the average cost for the largest 20 network intrusions would be consistently higher than the average cost for the largest 20 incidents. The previous disclaimer about the heavy-tail distribution of incident costs applies here. Therefore, the increase in the average 2018 cost could simply be a result of several larger and more expensive events appearing in that year's sample.

OCE summarizes the incident response times for all incidents and network intrusions in Table 27.

Table 27: Baker Hostetler (2017-2019) Incident Response Time

Incident Response	Incident Response Time in Days					
	2017 Report		2018 Report		2019 Report	
	All Incidents	NI	All Incidents	NI	All Incidents	NI
Occurrence to Discovery	61	N/A	66	84	66	95
Discovery to Containment	8	N/A	3	5	8	10
Forensics to Completion	40	N/A	36	36	28	36
Discovery to Notification	41	N/A	38	45	56	50

Note. NI = network intrusion. The reporting changes from mean to median days in 2020 report. Therefore, only the comparable mean results from Baker Hostetler (2017–2019) are included in this table.

While the time from occurrence to discovery has not significantly changed for all incidents from 2017 to 2019 (between 61 and 66 days), for network intrusions it went up from 84 days in the 2018 report to 95 days in the 2019 report. Between 2018 and 2019, the time from discovery to containment increased for all incidents (from 3 to 8 days) and network intrusions (from 5 to 10 days). Between 2018 and 2019, the time from engaging the forensics team to completion dropped for all incidents (from 36 to 28 days), while it remained unchanged for network intrusions, with a small increase in 2020 to 34 days for all incidents and 40 days for network intrusions. Between 2018 and 2019, the overall time from discovery to notification increased (from 38 to 56 days), while the increase for the network intrusion time was smaller (from 45 to 50 days). For 2020, the mean time from discovery to notification for network intrusions increased to 56 days. Network intrusions take the longest as it involves identifying what occurred and tracking down whose information was impacted.

Table 28 summarizes the top causes of cyber incidents in the past 2 years. Phishing remains the top cause, which is consistent with the incident dynamics data from some of the reports analyzed in the OCE study (IC3 2017, 2018; DBIR 2017, 2018, 2019, 2020; Hiscox 2018, 2019). The second most frequent cause of cyber incidents in Baker Hostetler (2018, 2019, 2020) is network intrusion. Note that the breakdown of incident types or causes in Baker Hostetler does not closely align with some of the other prominent industry reports tracking incident dynamics (e.g., DBIR, IC3, and Symantec).

Table 28: Baker Hostetler (2018, 2019, 2020) Top Causes of Cyber Incidents

Cause of Cyber Incident	Percentage of Incidents Due to Cause		
	2018 Report	2019 Report	2020 Report
Phishing	34%	37%	38%
Network Intrusion	19%	30%	32%
Inadvertent Disclosure	17%	12%	12%
Stolen/Lost Device or Records	11%	13%	8%
System Misconfiguration	6%	4%	5%
Other	13%	4%	5%

Source: Baker Hostetler (2017–2020)

The prior reports also indicate that after gaining access, the most common next steps are accessing an Office 365 account (35%), roaming network to find available data (30%), dropping ransomware (12%), and obtaining a wire transfer to the attackers account (8%). However, while account takeover remained the leading next step after phishing (31%), ransomware and installation of the malware became more prevalent according to the 2020 report (24% and 13%, respectively). This information is very useful as it enables what-if analysis for various types of incidents affecting not just confidentiality, which is somewhat better quantified with breach data available in commercial datasets, but also integrity and availability.

In addition, the Baker Hostetler reports contain informative statistics on the ransomware. According to the 2019 report, in 91% of the cases involving paying ransom, victims received a decryption key. The average ransom paid was approximately $28,920. The largest ransom reached $250,000. However, the 2019 report is based predominantly on 2018 data, and in 2019, there were already three ransoms paid of at least $1 million or more. The 2020 report, which reflects 2019 data, shows a significant increase in ransomware. While an encryption key was received in 96% cases of paying ransom, the average ransom payment increased by over an order of magnitude to $302,539, and the largest ransom paid in 2019 increased over 20 times to $5.6 million. For comparison, the largest ransom demanded in 2019 was $18.8 million.

Notably, 73% of the ransom cases included a restore from backup or were managed without paying a ransom. Thus, a new emerging trend in ransomware combines stealing data before ransomware is activated and reinforcing the ransom demand with a threat to publish stolen data (6% of ransomware incidents resulted in notification to individuals about unauthorized access or acquisition of data).

Accenture and Ponemon (Richards et al., 2017; Bissell et al., 2019)

The Accenture study conducted jointly with the Ponemon Institute (Richards et al., 2017) derived an estimated average response cost based on information from 2,182 interviews with 254 companies in seven countries (i.e., Australia, France, Germany, Italy, Japan, the United Kingdom, and the United States). The number of interviewed companies increased to 355 in the 2019 study, consisting exclusively of larger organizations (i.e., those with 5,000 or more enterprise seats).[26] The U.S. data were based on responses from 61 companies.

The annualized average response cost was estimated at $11.7 million per company, with the implicit rate of 2.5 attacks per company per week on average in 2017. The companies in the United States had the highest total average annualized cost of $21 million per company in 2017, increasing to $27.4 million in the 2019 report. Malware is cited as the most prevalent and most costly type of attack.

The estimates were derived by first identifying how much respondents spent on addressing malicious cyber activity over a 4-week period, and then extrapolating the value to derive the annualized estimate. The implicit assumption is that malicious activity and expenditures persisting within the 4 sampled weeks are representative of the rest of the year. Thus, the expenditures are scaled up linearly from the sampled 4-week period to the entire year.

Note that Accenture's estimates—similar to the Ponemon Institute's U.S. report discussed above—includes abnormal customer churn, subsequent program costs to incentivize customer retention, and other opportunity costs in addition to direct costs. The Ponemon Institute's (2017b) U.S. report indicated that the lost business and opportunity costs of this nature comprised 55% of their data breach cost estimate (see Table 23). Typically, these types of losses are not allowed to be included in the damage assessments.

[26] The number of enterprise seats is a measure of company size based on the number of users connected to networks or systems as opposed to just the number of employees.

The unit of analysis here is not the total breach cost, but rather an average annualized total per organization. Organizations targeted by the study included only large companies with 5,000 or more enterprise seats. In addition, only average estimates are reported, thus all the caveats with relying on averages apply here as well. Because of these three reasons, the comparison and reconciliation of results in this report with per-incident loss estimates from other sources is not practical.

Kaspersky Lab (2016, 2017, 2018, 2019)

Starting in 2011, Kaspersky Lab conducted an annual survey in multiple countries about the impacts of cyber incidents. The 2017 survey included 5,274 interviews in 30 countries regarding the costs of the incidents experienced by the companies within the previous 12 months. The 2017 results for North America show the average total impact of a data breach equaled $1.3 million in 2017, which is a slight increase from the 2016 level of $1.2 million. For enterprises (i.e., companies with 1,000 or more employees), the largest share of the cost is from the additional staff wages, which is approximately $207,000 per breach.

Of particular interest is the subset of survey results that focuses on SMBs (i.e., companies with 50 to 999 employees). The total cost of the breach for this subset of entities equals $117,000, with the most losses caused by business loss ($21,000) and staff augmentation or additional hiring ($21,000).

The Kaspersky Lab (2018) data are based on a survey of 6,614 respondents from 29 countries. The cost estimates in the 2018 report are higher for both SMBs and enterprises. Specifically, for North America, cost of a breach for SMBs went up from $117,000 in 2017 to $149,000 in 2018 on average. For enterprises, the cost estimate increased by 23% from $1.3 million in 2017 to $1.6 million in 2018.

A breakdown of the total breach cost by category for North America is presented in Table 29.

Table 29: Kaspersky Lab (2017, 2018) Average Breach Cost by Category

Cost Category	Average Breach Cost by Business Size ($ thousands)	
	2017	2018
SMB - Total Breach Cost	**$117**	**$149**
Additional Internal Staff Wages	$16	$17
Lost Business	$21	$17
Employing External Professionals	$21	$23
Damage to Credit Rating/Insurance Premiums	$11	$18
Extra PR	$10	$15
Compensation	$8	$7
Improving Software/Infrastructure	$11	$18
Training Staff	$9	$15
Hiring New Staff	$10	$14
Penalties and Fines	-	$5
Enterprise - Total Breach Cost	**$1,336**	**$1,600**
Additional Internal Staff Wages	$207	-
Lost Business	$148	-
Employing External Professionals	$154	-
Damage to Credit Rating/Insurance Premiums	$118	-
Extra PR	$113	-
Compensation	$147	-
Improving Software/Infrastructure	$172	-
Training Staff	$153	-
Hiring New Staff	$124	-

Note. Source: Kaspersky Lab (2017, 2018 Kasperky (2018) does not include enterprise estimates for North America. Kaspersky (2019) does not provide a regional breakdown for either SMBs or enterprises. Therefore, it is not included in this table.

The cost categories here are harder to compare as they combine two different dimensions: (1) activity-based costs such as PR and training; and (2) acquisition and staff augmentation expenditures such as compensation, employing external professionals, and hiring new staff (i.e., source of expenditure). Maintaining the consistent breakdown by activity as in NetDiligence (2018, 2019) as opposed to categorizing source of expenditures for an activity would provide a more informative quantification and would enable comparison with other per-incident estimate sources and reconciliation with the estimates based on insurance claims.

Kaspersky Lab (2017) also provides a cross-section of estimates by incident type. For larger entities, the top five most expensive incidents included physical loss of device or media with data ($2.8 million); incidents affecting third-party-hosted IT infrastructure ($2.2 million); data leaks ($1.9 million); inappropriate IT resource use by employees ($1.1 million); and viruses and malware ($519,000). For SMBs, targeted attacks were the costliest at $188,000; non-computing connected devices ($152,000); physical loss of devices or media containing data ($83,000); inappropriate IT resource use by employees ($79,000); as well as viruses and malware ($68,000). The magnitudes of losses are comparable with the Romanosky (2016) and NetDiligence (2018) estimates.

Kaspersky Lab (2018) does not provide the same cross-sectional detail by region, stating that the costliest incident type for both SMBs and enterprises are incidents affecting IT infrastructure hosted by a third party ($163,000 and $1.75 million, respectively).

This study shares some of the familiar limitations. The report does not indicate if the methodology used surveys based on self-reported data of perceived losses via a poll, as opposed to an invoice-based approach to costing. The estimation methodology and assumptions are not clearly specified, and only the averages are shown. Information regarding the specific sample size for the North America report with a breakdown of the count between SMBs and enterprises would be beneficial as well. Otherwise, it is unclear how many North American firms and how many incidents are spanned by the summary estimates included in the report.

Cisco (2017, 2018a, 2018b, 2019, 2020[27])

The Cisco (2019) Chief Information Security Officer (CISO) benchmark study contains estimates of the financial impact from cyber incidents based on a survey of 2,386 responses, with North America constituting 25% of the sample. A similar question about the financial impact magnitude was included in the global Cisco 2018 Security Capabilities Benchmark Study, which surveyed 3,600 respondents across 26 countries. The Cisco (2018a) annual cybersecurity report contains a summary of the study, including the estimates of the financial impact from cyber incidents.

The question focuses specifically on the financial impact from the most impactful breach the organizations have experienced in the past year, as opposed to the average cost of a cyber incident. Impacts included financial damages, lost revenue, customers, and opportunities, as well as out-of-pocket costs. A summary of the cost estimates is presented in Table 30.

According to 2018 and 2019 data, the median cost of the most impactful incident fluctuates around $500,000. Specifically, 51% of the incidents in 2019 data were below $500,000.[28] The most prevalent attack vectors that resulted in some breach of data include malware, malicious spam, and phishing, thus, email security remains a top concern.

[27] Although the 2020 versions of CISO Benchmark Report and 2020 SMB Report were available at the time of publication, neither contain incident cost information.
[28] This figure is the sum of the percentage of attacks with the most impactful breach being less than $100,000 (31%) and those between $100,000 and $500,000 (20%). See Table 30.

Table 30: Cisco (2018a, 2019) Distribution of the Cost of the Most Impactful Breach

Financial Impact of the Most Impactful Breach in the Past Year	Percentage of Attacks by Survey Year	
	2018	2019
Less than $100,000	30%	31%
$100,000–$499,999	17%	20%
$500,000–$999,999	15%	16%
$1–$2.5 million	19%	15%
$2.5–$5 million	11%	10%
$5–$10 million	7% [a]	7%
$10 million or more	1%	1%

Note. Sources: Cisco (2018a, 2019)
[a] The 2018 version of the report grouped top two categories into 8%. OCE assumes the same ratio as in 2019.

In addition to the general annual studies, Cisco (2018b) issued a special report focusing on SMBs. It showed that 53% of the surveyed mid-market companies experienced a breach.[29] Twenty percent of the mid-market companies estimated their cost of a breach to be in the range of $1 to $2.5 million. For 29% of the mid-market companies, the breach costs were below $100,000. The results were derived from the SMB subsample of the respondents in the Cisco 2018 Security Capabilities Benchmark Study, which included 1,816 respondents from 26 countries. The estimates for the shown categories are higher than what is included in Romanosky (2016) and NetDiligence (2017); however, they align fairly closely with the RBS (2018) data for the United States and the previously discussed Kaspersky (2017, 2018) estimates, as well as the Hiscox (2017, 2018) estimates discussed below.

Hiscox (2017, 2018, 2019, 2020[30])

The Hiscox (2017) Cyber Readiness Report is the primary source of per-incident cost estimates in Symantec (2017). For completeness, the more recent numbers from Hiscox (2018, 2019) are also included in the discussion below.

The Hiscox survey is conducted by Forrester Consulting to evaluate cyber readiness and assess incident trends in the United States, United Kingdom, Germany, Spain, and the Netherlands. Over 3,000 and 4,103 respondents were surveyed in 2017 and 2018, respectively. Almost half of the respondents are from U.S. companies. In 2019 report, Belgium and France were added to the survey increasing overall number of responses to 5,400. However, the number of the U.S.-specific responses was lower (approximately 1,000) in 2019 edition. 39% of the respondents in the global sample were from small firms with fewer than 50 employees, 16% - from medium size firms (50–249 employees), 16% from large firms (250–999 employees), and 28% from enterprises (1,000 or more employees).

In the global 2018 sample, 45% of the respondents had a cyber incident occur within the last year, with 27% reporting to have two or more incidents. According to the survey results for the U.S. companies, 38% of the respondents reported an incident occurring in the preceding 12 months in Hiscox (2018), which went up to 53% in Hiscox (2019). Notably, in the 2018 sample, 53% of the U.S. government organizations experienced a cyberattack in the preceding 12 months.

[29] Cisco (2018b) defines SMBs as companies with fewer than 250 employees and midmarket companies as those with 250 to 499 employees.
[30] Although the Hiscox (2020) report was available at the time of publication, it does not contain granular incident cost information for the United States, which were included in prior versions.

The 2018 report also breaks down the incident rate by company size. Larger organizations in the United States, defined in the survey as companies with 250 or more employees, reported higher rates of cyber incident occurrence (ranging between 60% and 72% depending on the company size).

In Hiscox (2019) sample, the number of respondents experiencing a cyber incident in the 12 months prior increased to 61%. Moreover, out of the companies that experienced a cyber incident, almost a third (30%) reported four or more incidents. The Hiscox (2020) sample shows a decrease in the number of firms experiencing a cyber incident (i.e., down to 39%).

There are two types of survey-based cost estimates reported in Hiscox (2017, 2018, 2019)—total annual cost of cyber incidents to an organization and per-incident cost of an organization's largest cyberattack. The first one is a metric similar to what is reported in the Accenture and Ponemon Institute (Richards et al., 2017) study. However, the magnitude of the per-company total reported in Hiscox is significantly lower. Namely, Hiscox (2018) estimates the total annual cost for cyber incidents to be approximately $1.05 million for the largest companies (i.e., those with 1,000 or more employees), which is 20 times lower than the Accenture and Ponemon Institute (Richards et al., 2017) estimate of the average per-company total cost of $21 million. A breakdown of the company total incident cost by company size is presented in Table 31.

Table 31: Hiscox (2018, 2019) Mean U.S. Per-Company Cost of All Incidents, $

Number of Employees	Mean Total Cost per Company, $ (All Cybersecurity Incidents)	
	Hiscox (2018)	Hiscox (2019)
249 or Fewer	$34,604	~$100,000
250–999	$578,762	~$100,000
1,000 or More	$1,047,465	$213,000
Overall Range	**$350–$25,000,000**	-

Source: Hiscox (2018)

Specifically, what is reported in Accenture and the Ponemon Institute (Richards et al., 2017) for the average total cost ($21 million) is almost the same as the highest total per-company cost of $25 million in Hiscox (2018). Moreover, the total per-company annual cost in Hiscox (2018) is more than three times lower than the U.S. per-incident cost of $3.32 million in Ponemon Institute (2017).[31] Hiscox (2019) estimate for mean cost of all incidents for the U.S. enterprises (1,000+ employees) is even lower ($213,000). Mean estimate across all firm sizes is $119,000.

The second survey-based metric reported in Hiscox (2018), per-incident average cost for the largest cyber incident, varied from about $36,000 to $102,000 in the 2017 report, and $5,000 to $107,000 in the 2018 version. A breakdown of the incident cost estimates across the company sizes is presented in Table 32.

[31] To keep the Hiscox (2018) and Ponemon Institute (2017) metrics comparable, OCE excludes the opportunity cost and lost business cost from the Ponemon Institute estimate.

Table 32: Hiscox (2017, 2018) Mean Cost of Largest Incident (U.S. Companies)

Number of Employees	2017 Study	2018 Study
99 or Fewer	$35,967	N/A
100–249	$41,334	$4,883[a]
250–999	$81,322	$60,258
1,000 or More	$102,314	$106,583
Overall Range	-	**$20–$2,000,000**

Note. Source: Hiscox (2017, 2018)
[a] The 2018 Study combined the categories for companies with 99 or fewer and 100 to 249 employees. Thus, the $4,883 value is for companies with fewer than 250 employees.

The average cost of the largest cyber incident reached $102,000 in 2017 for very large U.S. companies, and only increased by 4% to $107,000 in the 2018 study, subsequently dropping to $73,000 in the 2019 report. For companies with 250 to 999 employees, the estimate for 2018 decreased by about 26%. The reduction was even more pronounced for the smaller companies defined as having fewer than 250 employees—it dropped almost 10 times.[32] However, since these are average estimates, the same caveats as discussed in the previous sections apply here as well. Therefore, this is not necessarily an indication of incidents decreasing in cost, but rather the companies sampled for 2018 might have experienced fewer costly incidents that would otherwise severely affect the average.

The Hiscox cost estimates above do not include brand damage or loss of business. In the 2017 survey, the U.S. respondents that faced a cyber incident in the last 12 months reported other non-monetary losses, namely, 15% of the organizations reported loss of customers or difficulty attracting new clients; 11% lost business partners; and 10% experienced negative publicity that adversely impacted their brand or reputation. These percentages were lower in the 2018 study: 7% lost customers, 5% had difficulty attracting new ones, 5% lost business partners, 5% experienced bad publicity that damaged the brand, and 6% of the companies had to lay off employees.

These losses are not factored into the incident cost estimates shown above. Comparing the estimates in Hiscox (2018, 2019) to the relevant Ponemon Institute (2017, 2018) metric, the average cost of an incident in the latter study is more than 30 times higher than the average of the largest incidents in both the 2017, 2018 and 2019 Hiscox reports.

Symantec (2016, 2017)

An earlier version of the Symantec (2016) report cites NetDiligence (2015) Cyber Claims results. The cited per-record costs also refer to the Ponemon Institute's (2016a) estimate of $158 per record, however, the average size of the breach considered in the Symantec report is outside of the threshold of 100,000 records for the Ponemon Institute estimate to be applicable. A detailed discussion about breach sizes relevant for this context is included in the scaling section of this study (Section 4).

Symantec (2017) also provides cost estimates for ransomware. Ransomware payouts ranged between $373 in 2014 and $294 in 2015 and increased to $1,077 in 2016. Symantec (2018) shows the average payout amount dropped by about half to $522 in 2017. According to Symantec (2017), the United States seems to be heavily targeted and most affected by ransomware among all of the analyzed regions. In 2016, a third of all infections occurred in the United States. Symantec (2017) cites the research by the Norton Cyber Security Insight team,

[32] Again, the category sizes for the smallest companies were not comparable in the 2018 study. Therefore, OCE compared the average cost for companies with 100 to 249 employees in the 2017 study to the average cost for companies with fewer than 250 employees in the 2018 study.

attributing this difference to the higher willingness to pay ransom in the United States (64% of affected individuals paid) in comparison with the rest of the regions (34%).

A particular issue with ransomware estimates arises from the fact that the payout itself constitutes only a very small portion of the significant total breach cost, while it remains to be a fairly cheap activity for the adversary to deploy. Thus, ransomware estimates, although cited here for context, are not included in the overall summary table of the per-incident cost estimates in the previous sections (see Table 1 or Table 4).

Another type of attack that has a low cost to the adversary, but a disproportionately higher cost for the targeted entities is a Distributed Denial of Service (DDoS) attack. DDoS attacks can be conducted at $5 to $20 for a medium target for under an hour, to $10 to $1,000 per day for a medium to strong target for a duration of over 24 hours. However, the Symantec (2016) report indicates the costs to an affected organization have reached $40,000 per hour, citing estimates from the Incapsula Impact Survey (Matthews, 2015).

In August 2014, Incapsula surveyed 270 North American organizations operating in software or technology, manufacturing, and banking or finance with sizes varying from 250 employees to over 10,000. Out of all the respondents, 80% had their company headquartered in the United States. Out of the 45% of respondents that experienced a DDoS attack (121), 91% (110) incurred an attack in the preceding 12 months, with 70% (85) experiencing multiple attacks within that time period. Table 33 summarizes the percentage of respondents that experienced different levels of per-hour costs due to a DDoS attack, as estimated by Incapsula based on the 2014 survey results (Matthews, 2015).

Table 33: Distribution of the Hourly Cost of a DDoS Attack

Hourly Cost	Percentage of Respondents
$4,999 or Less	15%
$5,000–$19,999	36%
$20,000–$59,999	17%
$60,000–$99,999	17%
$100,000 or More	15%

Source: Matthews (2015)

While the survey estimates cost of the DDoS attack to be about $40,000 per hour, according to the Incapsula cost interval summaries, 51% of the respondents reported hourly costs below $19,999. If $40,000 is an average response, the significant difference may be a symptom of a long-tail distribution, thus, the median would serve as a more informative statistic for the hourly cost of DDoS attacks. The business impact section of the summary lists loss of customer trust, loss of IP, and additional virus or malware infection as non-financial consequences, implying those factors were not monetized as part of the loss calculations. However, the Incapsula (Matthews, 2015) survey summary does not explicitly specify what cost categories were included in the estimates or how they were defined.

The Incapsula (Imperva, 2016) report contains an updated set of estimates for the attack duration, both for application layer and network layer attacks. Based on 2016 first-quarter data related to application layer attacks, 52% of the attacks lasted less than an hour; about 26% lasted 1 to 3 hours; and another 23% exceeded 3 hours in duration. For network layer attacks, 93% lasted less than an hour, with the remaining 7% ranging between 1 and 3 hours.

The Symantec (2016, 2017) reports also contain breach count or incident frequency estimates, as well as national and global loss estimates. Both sets of the estimates are discussed in the aggregate estimates section (Section 3.2) and scaling section (Section 4), respectively.

Biener et al. (2015)

An additional source of per-incident cyber loss data is the SAS OpRisk Global Data, which is a database that contains publicly reported operational losses. Biener et al. (2015) analyzed the cyber-relevant subset of losses reported from 1971 to 2009. While the database is focused on providing a comprehensive picture of losses for operational risk events, including both direct and indirect costs, it excludes reputational risks. In that sense, the data contained in the SAS OpRisk resource is comparable to the loss categories in NetDiligence (2017) and Romanosky (2016). Biener et al. developed a set of inclusion criteria for events in the database to qualify them as cyber risk relevant: (1) a critical asset was affected; (2) a relevant actor was involved in the cause of the cyber risk incident; and (3) the cyber-relevant outcome has to be present. Based on these criteria, 994 observations were selected to support the analysis. A detailed results table from Biener et al. is presented in Table 34.

Table 34: Biener et al. (2015) Summary of Loss Estimates by Risk Type, $ Millions

Category	Number	Mean	Standard Deviation	Min	Quantiles			VaR (95%)	TVaR (95%)	Max
					25%	50%	75%			
Cyber Versus Non-Cyber Risk										
Cyber Risk	994	40.53	443.88	0.10	0.56	1.87	7.72	89.56	676.88	13,313
Non-Cyber Risk	21,081	99.65	1,160.17	0.10	1.88	6.20	25.37	248.97	1,595.27	89,143
Cyber Risk Subcategories										
Actions of People	903	40.69	463.25	0.10	0.55	1.83	6.87	84.36	679.04	13,313
Systems & Technical Failure	37	29.07	77.33	0.10	1.10	5.03	11.65	168.95	329.04	370
Failed Internal Processes	41	47.72	205.92	0.14	0.42	2.04	9.05	158.65	743.40	1,311
External Events	13	39.40	115.73	0.28	0.56	1.03	13.77	192.88	422.71	422

Note. Adapted from "Insurability of cyber risk: An empirical analysis," by C. Biener, M. Eling, and J. H. Wirfs, 2015, *The Geneva Papers on Risk & Insurance*, *40*, p. 139. Value at Risk (VaR) represents a loss that would not be exceeded at the pre-specified probability level, α. Tail Value at Risk (TVaR) represents the expected loss, given that the loss falls in the worst part (1 - α) of the loss distribution. For a more detailed explanation see Hardy (2006).

The descriptive analysis of the sample, as well as risk metrics such as VaR and TVaR, show that for this dataset, losses for cyber-risk-relevant events are significantly lower than for other operational risks. The median per-event loss for cyber risk incidents is $1.87 million and the mean is $40.53 million. The median for operational losses from non-cyber incidents is approximately $6.2 million, with the mean being $99.65 million. The 75th percentile for cyber risk events approximated $7.72 million, which is three times lower than the 75th percentile for non-cyber risk events ($25.37 million).

In turn, these per-incident costs are considerably higher than in NetDiligence (2017) data, Advisen data analyzed in Romanosky (2016), and the Ponemon Institute (2017) estimates. Partially, this difference in magnitudes can be explained by the fact that SAS OpRisk is a global dataset with per-incident estimates varying across the regions. Estimates for North America are shown in Table 35.

While the region-specific estimates are lower than their global counterparts, the mean and median for cyber losses still remain higher than the other studies reviewed in this report. The median cyber risk losses for North America are approximately $1.68 million, with the mean approaching $20 million. Results for North America were derived based on 516 data points for cyber-related risk losses and over 14,000 data points from non-cyber risk losses.

Table 35: Biener et al. (2015) Cyber and Non-Cyber Risk Losses, $ Millions

Risk Type, North America	Number of Observations	Per-Event Losses ($ millions)	
		Mean	Median
Cyber Risk	516	$19.86	$1.68
Non-Cyber Risk	14,126	$81.11	$6.30

Source: Biener et al. (2015)

The empirical VaR defined as the 95th percentile of the underlying global sample approximated $90 million for cyber risk events, and $249 million for non-cyber risk events. Biener et al. (2015) also compare the distribution of losses for cyber and non-cyber risk events. They show that while both distributions are heavy tailed, the non-cyber losses are significantly higher, and the non-cyber loss distribution has a much heavier tail.

The implications of this finding are threefold: (1) the mean is not a good characteristic of cyber losses in this data, as it is strongly impacted by extreme values; (2) losses from cyber and non-cyber risk events come from two different DGPs, thus dictating the need to model, analyze, and manage cyber risks separately from other operational risks; and (3) prioritizing resources towards cyber risk management will remain challenging, as the empirical valuation of the limited historical data available on cyber losses shows other operational losses are a more dominant source of risk.

Deloitte (2016)

The Deloitte (2016) report offers a more detailed look at the itemization of incident costs, with emphasis on attempting to quantify the intangible losses and contrast them with the directly observable costs. The estimation and comparison are conducted for two scenarios. While the scenarios themselves are hypothetical, their characteristics and magnitude are consistent with the incident descriptions in other sources, such as the DBIR digest (Verizon, 2016b). The suggested scenarios are compatible with the overall threat and incident dynamics discussed in McAfee, Symantec, and other industry reports.

The estimated cost categories are divided into two groups. The more observable and directly measurable costs, or "above the surface" costs, include post-breach customer protection, cybersecurity improvements, customer breach notification, legal fees and litigation, regulatory fees and fines, PR, and technical investigation. The second group, referred to as "beneath the surface" costs, includes the costs and losses that often are not fully realized until 3 to 5 years after the incident. This group of costs includes the value of lost contract revenue, operational disruption, the devaluation of trade names, loss of IP, increases in insurance premiums, the increased cost of debt/financing, and the lost value of customer relationships.

The report focuses on comparing and contrasting directly observable costs and losses immediately following a cyber incident with the longer-term, less measurable indirect or intangible losses. The report emphasizes the drastic difference in magnitudes, showing how indirect losses (95% of the total) by far outweigh the directly observable ones. The strength of the comparison rests on this extreme disparity in the magnitudes. However, the magnitudes used for this illustration are an immediate function, mostly linear, of the assumptions with respect to the duration and severity of the adverse effects.

While the assumptions, rates, and scaling factors for most of the direct costs are cited, a majority of the assumptions regarding the "beneath the surface" costs are not backed up with empirical data justifying the chosen magnitudes or duration of the impact.

For example, the calculation of losses for Scenario A—a breach of 2.8 million of PHI records at a large U.S. health insurer—assumes "new members in year one (immediately after the breach) decreased by 50 percent," (Deloitte, 2016, p. 9) with subsequent recovery to the normal growth rates over a 5-year period. The associated losses are estimated at $430 million. The value of lost contract revenue, which amounts to $830 million over 5 years, is

based on an assumed 20% reduction in the annual premium increase in the first year after the breach, with subsequent recovery to the pre-incident level after 5 years. Together, these two cost categories account for over $1.26 billion, which is 75% of the total costs ($1.679 billion).

This assumed duration of impacts (5 years) contradicts the most recent research that shows the long-term effects (over a year) after a cyber breach to be negligent (Kvochko & Pant, 2015). Even considering the full magnitude of the losses for Scenario A over 5 years ($1.679 billion), it constitutes 2.8% of the annual revenue ($60 billion), and only 0.56% of the revenue for the comparable time-horizon (i.e., the 5-year loss as a fraction of 5-year revenue).

Comparing the scenario with the Anthem breach of February 2015, which was significantly larger—it affected 80 million customers—could be a useful benchmark for validating the loss assumptions. According to Yahoo Finance (2019), Anthem's enterprise value is about $64 billion, with an annual revenue of about $90.5 billion in 2017. The sales growth rate for 2018 is estimated at about 2.6%.Anthem's income statements from 2013 to 2017 are presented in Table 36 below.

The summary of revenues and profits show not only that revenue grew by 7.15% in the year of the cyber breach (2015), but that the growth rate was higher than in the preceding year (4%) and remained steady at 7% in 2016. Anthem's profit margin (i.e., net profit divided by revenue) dropped from 3.5% to 3.2% in 2015, and then to 2.9% in 2016, followed by a growth to 4.3% in 2017.

Table 36: Anthem Revenue, Net Profit, and Net Profit Margin (2013-2017)

Description	2013	2014	2015	2016	2017	Average Annual %
Revenues ($ Millions)	$71,024	$73,874	$79,157	$84,863	$90,039	6.1%
Net Profit ($ Millions)	$2,490	$2,570	$2,560	$2,470	$3,843	-
Net Profit Margin (%)	3.5%	3.5%	3.2%	2.9%	4.3%	3.5%

Source: Morningstar (2019a)

The Morningstar (2019b) data allow for a similar type of comparison for Anthem healthcare plan dynamics to validate the customer churn. Jointly, this information on revenues, profits, and healthcare plans volume suggests that the assumed drop in customers and loss of revenue for Scenario A could be extreme. Therefore, the remainder of the assumptions with respect to magnitude and severity of the "beneath the surface" costs for both scenarios would benefit from explicit empirical validation.

The Deloitte (2016) report offers a detailed description of the methods used to quantify the intangible losses. It provides exceptional value in showing how the estimates of this nature and associated assumptions need to be fully disclosed and carefully explained in order to offer value to a reader. Nevertheless, the analysis would benefit from explicitly referencing the technical basis and empirical justification for the assumptions used to parametrize 'beneath the surface' costs, as they directly drive the outcome of the analysis.

B.2 Per-Record Estimates

The disparity between Verizon DBIR (2015) and Ponemon Institute (2013, 2014) per-record estimates gave rise to a broader debate about the appropriateness of relying on the cost-per-record approach. It questioned the ability of either the Verizon or Ponemon Institute estimates to accurately predict costs of the cyber breaches, for which both the size of the breach and pre-and post-insurance payouts have been publicly disclosed. A summary of this discussion is incorporated into the Verizon DBIR (2015) report. Jacobs (2014) also provides an in-depth analysis of the main issues with these estimates, as well as the overall per-record approach to PII breach valuation.

The detailed analysis by Jacobs (2014) contains a very clear dissection of the Ponemon Institute report methodology based on their 2013 and 2014 published data. Jacobs shows that the approach used by the Ponemon Institute is overly simple and is not based on a strong model fit. Jacobs concludes that cost-per-record estimates in the Ponemon Institute reports are a poor fit to actual data. Based on R-squared, the Ponemon Institute model only describes about 13% of the variation in the data in 2013 and just over 2% of the variation in 2014.

Both Jacobs (2014) and Verizon (2015) discussions clearly explain the predicament with the per-record estimates and propose a better fitting model as part of their analysis. The proposed log-log model provides a better estimate, but even that results in a fit with R-squared of about 0.537. That means that even with a better fitting log-log model, the variability in the breach size explains only 54% of the variance in the breach cost.

Incorporating other breach characteristics into the model while still keeping the number of records in the parametrization improved the fit only slightly. Based on that, the Verizon (2015) report suggests that model improvement could be achieved by collecting more and different types of data, not necessarily by digging into more specific characteristics of the breach.

From OCE's perspective, having more and different types of data would also enable a more robust non-parametric estimation of the relationship, where categorical variables such as breach characteristics could be treated without imposing a particular functional form on the dependence.

Besides explaining why the Ponemon Institute estimates are a poor fit to the actual data, the analysis concludes that using just the number of records lost in a breach is not an accurate indication of a breach's impact. This analysis makes the assumption that the data collection method was not seriously flawed. The focus was on the Ponemon Institute's methods for analyzing the data itself.

The response from Ponemon Institute is contained in Ponemon Institute (2015a) and Goodman (2015). The Ponemon Institute defends its estimates, stating that the total cost of the breach using its method falls within the same confidence interval as Verizon (2015) DBIR results. Goodman (2015) includes a useful discussion of the challenges of using insurance data to estimate the cost of a breach. The author concludes that cyber insurance claims may not be an appropriate foundation for deriving estimates of cyber incident costs, because policies have strict limits on coverage, including sub-limits for various cost and impact categories.

For example, Target's actual cost of the breach was closer to $292 million, while the insurance threshold was only about $90 million (Target Corporation, 2017). In addition, there are various policy exclusions that would require an analyst to examine each claim to understand if any direct costs were excluded. An example of a cost that is typically excluded from the policy coverage is business interruption expenses, which is an optional coverage, typically only provided at an additional cost. There is no single standard across cyber insurance policies regarding limits, sub-limits, and exclusions, which prevent insurance claims from serving as a consistent basis for data breach cost estimation. Other examples of exclusions in insurance coverage are discussed in more detail in Romanosky et al. (2019).

The difference in methodologies between Verizon (2015) and the Ponemon Institute's estimates is further explained in Hackett (2015). To illustrate the difference, OCE uses the 2013 Target breach as an example, which resulted in the theft of 40 million payment cards and 70 million other records (Armerding, 2018a, 2018b). Applying Target's breach size numbers to the normalization steps outlined in Hackett (2015), the Ponemon Institute's estimate of $200 to $221 per record would imply over $8 billion in losses for only the payment card portion of the breached data. This estimate would be unrealistically high relative to the Target actual total breach costs of $292 million (Target Corporation, 2017). The Verizon estimate of $0.58 per record would result in $23 million for the payment card portion of the loss and $41 million for other records stolen—a total of $64 million,

which is 22% of the actual total breach cost. The actual Target loss was about $202 million after the insurance payouts of $90 million, which nets down further to approximately $140 million after the tax write-off of $62 million for breach-related costs (Target Corporation, 2017). Neither of the total cost estimates derived using the Ponemon Institute and Verizon per-records cost estimates come close to either the $292 million pre-insurance, $202 million post insurance, or $140 million net-tax loss figures.

The Ponemon Institute's per-record cost includes "soft" indirect costs and opportunity costs (almost 55% of the estimate), while the Verizon estimate does not. However, even with the downward adjustment of the Ponemon Institute's estimate to exclude the abnormal customer churn and subsequent customer retention programs, the total estimate for the Target breach would come to $3.5 billion, which is still over an order of magnitude higher than Target's actual total breach cost.

Comparing the actual costs of these breaches with the assessment offered by either Verizon or the Ponemon Institute confirms that neither one of the per-record estimates provide accurate inference for multiple reasons. Neither of them are derived based on a representative sample; the relationship between breach size and cost is not linear; and some of the dominant cost categories (e.g., identity protection and credit monitoring) do not always scale up, linearly or non-linearly.

The Verizon (2016a) DBIR disregarded the per-record estimates altogether and started to rely on the NetDiligence per-incident data instead. The Ponemon Institute seemed to continue with the same methodology. In Ponemon Institute (2017b), the estimate increased to $225 per record, where $146 is for indirect costs including abnormal customer churn and $79 is for direct costs. However, no statistical testing results are included to demonstrate the significance of the difference between the annual per-record estimates or goodness of fit to the underlying data.

The issue of cost-per-record estimates debated by the Ponemon Institute and Verizon also emphasizes the importance of separating fixed costs from the variable cleanup and recovery costs. Fixed costs do not depend on the number of systems or network segments infected or compromised. Fixed costs are also not a function of the number of victims or breached records. Fixed costs capture broad spectrum changes that are induced by the specific nature of the penetration mechanism but are not a function of its size. Examples of fixed costs may include detection, investigation, and hunting; breach anatomy analysis with subsequent documentation and reporting; change of network architecture and contact points; adjustment of access privileges; modification of communication protocols; remedial training; and changes to the control protocols. However, depending on the nature of the incident, some of these fixed cost categories may become variable. For example, an increase in the number of impacted network segments may increase the scope of hunt activities or the number of images to analyze and thereby increase the time required for an investigation. The fact that cost categories have the potential to change from fixed to variable costs makes the use of per-record averages dubious .

While fixed costs are driven by incident anatomy, system architecture, and cybersecurity processes and practices in place, variable costs are rather a function of breach size, the number of impacted machines, the number of affected system segments, and the number of breached records or victims. An example of a variable cost is removing malware from affected machines, as the time required to clean each machine is relatively constant. The number of machines in need of scrubbing determines the cost. This assumption seems to be backed by Clayton (2011), Moore (2010), and Moore and Anderson (2011), which cite Comcast partnering with McAfee for malware cleanup at $89.95 per remediation service. Moore and Anderson (2011) state that Comcast later partnered with Symantec for remediation services to be provided to its customers by a skilled technician at $100. Also, as indicated by the itemized comparison of the large and small incidents earlier in the report (see Section 3.1.1), third-party services, especially for large data breaches, are furthermore negotiated at the fixed ceiling, irrespective of the actual number of affected individuals pursuing the offered credit monitoring or identity restoration services.

There are other considerations that contribute to the challenges with cost-per-record estimates. As discussed earlier in this report, costs per year are not an accurate representation of the losses, because cost and loss accumulation from an incident may occur over several calendar years. A similar issue applies to the comparison of the per-record costs from year to year. While the correlation of the incident cost to incident size has been established in Romanosky (2016) and NetDiligence (2017), the issue of incident size and how frequencies change over time is investigated in Edwards et al. (2016). Edwards et al. analyzed the PRC cyber incident frequency and size data. The analysis showed that it is a long-tailed distribution and the power law fit, but neither size nor frequency drastically changed over the analyzed time period. This behavior is characteristic of a heavy-tailed distribution, where the upper quartile captures the occurrence of the larger, more expensive incidents. If the size or the frequency do not demonstrably change as concluded in Edwards et al., and it is a heavy-tailed distribution, to what extent it provides value-added to compare per-record estimates across calendar years—a boundary that is not meaningful from the standpoint of cost accumulation from an incident—remains an open question.

Thus, annualized normalizations done by looking at the total cost per year and dividing it by the number of records exposed in a year could be misleading. Normalization within the boundaries of a specific incident is more appropriate if the correlation between the incident size and costs supports such analysis. However, even that is problematic and has a rather limited explanatory power due to all of the issues described above. Cyentia (2020) has the most illustrative explanation of the severe variability in the cost-per-record metric in historical data and resulting pitfalls of relying on direct scaling the per-record estimates.

B.3 Aggregate Loss or Impact Estimates on the National Scale

Below, OCE summarizes aggregate national and global loss estimates available in the most widely cited published research and industry reports.

McAfee (2013, 2014, 2018)

McAfee and the Center for Strategic and International Studies issued a series of reports estimating the impact from malicious cyber activity on the global scale. Up until the 2018 update was published, McAfee (2014) and McAfee (2013) were some of the most frequently cited sources of cybercrime impact estimates on the national and global scale.

The global estimates in McAfee (2013) for cybercrime and cyber espionage range from $300 billion to $1 trillion, with U.S. malicious cyber activity being quantified between $24 billion and $120 billion, or about 0.2% to 0.80% of the U.S. GDP at the time of the publication of the report. The report indicates that the upper limit of the estimate for cybercrime and cyberespionage ranges from 0.5% to 1% of GDP, which is approximately $70 billion to $140 billion. A lower limit is specified at $20 billion to $25 billion.

The study includes a breakdown of cybercrime activity by category, but the estimate is not itemized at that level of granularity. Instead, the study provides aggregate impact estimates assessed by analogy from other types of proxy phenomena (e.g., other forms of crime and loss) at the national economy level. These estimates are based on self-reported loss assessments by affected companies with subsequent extrapolation to the national level. Also, estimates of the losses for high-income countries (e.g., the United States) are in turn used to extrapolate to the global impact number. In the absence of a more robust modeling approach and supporting macro data, these aggregate or global estimates could serve as upper bounds to illustrate the magnitude of the cybercrime problem, but they are less helpful for informing investment decisions at the micro level. Neither of the earlier McAfee reports provide an indication as to where the variability in losses may come from; how they differ based on breach size; or what patterns dominate malicious cyber activity.

The McAfee (2014) report updated the global estimate to $500 billion (0.7% of the global GDP), placing the conservative estimate at $375 billion. It also lowered the upper bound from $1 trillion to $575 billion. McAfee's (2018) estimate of the global impact from malicious cyber activity increased to $600 billion, which constitutes 0.8% of the global GDP. A summary of the estimates across the McAfee reports is presented in Table 37.

Table 37: McAfee (2013, 2014, 2018) Aggregate Estimates (U.S. and Global), $ Billions

Study Publication Year	U.S. Estimates		Global Estimates ($ billions)		
	Range ($ billions)	% of GDP	Lower	Best	Upper
2013	$24–$120	0.2%–0.80%	$300	-	$1,000
2014	~ $100	0.64%	$375	$445	$575
2018	$134–$170[a]	0.69%–0.87%	$445	-	$600

Sources: McAfee (2013, 2014, 2018).
Note. OCE scaled estimate for the U.S. McAfee's (2018) studies report North American estimates.

The McAfee (2014) report also suggests that the highest cost of cybercrime comes from IP theft. According to the U.S. Department of Commerce (as cited in McAfee, 2014), IP theft then cost U.S. companies approximately $200 to 250 billion annually. This estimate is not supported by the specific estimates or by an explanation of the actual methodology as to how IP theft is compared to other cyber breaches. The cited number is sourced to the Commerce Blog post from 2011 that is no longer available. The McAfee report does indicate that this estimate may be overstated, but states that a wealth of anecdotal evidence suggests the contrary. The evidence that supports that statement about plentiful evidence to the contrary is not cited or explained in the report. This aspect was corrected in the McAfee (2018) report with specific language explaining the approach to valuation of IP.

The McAfee (2018) report indicates that the cybercrime impact estimate used data that takes into account the loss of IP; the theft of financial assets and sensitive business information; opportunity costs; additional costs for securing networks; and the cost of recovering from cyberattacks, including reputational damage to the hacked company. However, it does not explain the methodology for enabling this valuation. Information sources include published data, interviews, and estimates from government agencies and companies around the world, but a discussion of the actual supporting data and estimation methodology is omitted. Similarly to previous editions, McAfee (2018) relies on the proxy costing of other crimes and losses (e.g., maritime piracy, pilferage, and transnational crime), further anchoring the estimate to a fraction (one-seventh) of the transnational crime costs as reported by the WEF ($1.8 trillion) and Global Financial Integrity ($1.6 to $2.2 trillion) citing May (2017).

World Economic Forum (2015, 2016, 2017, 2018, 2019)

Previously reviewed studies cite the WEF Global Risks Reports as one of the sources for the global cyber loss estimates. The WEF (2015) report states annual economic losses from cybercrime as equal to $100 billion in the United States alone. This estimate is sourced to the Gorman's (2013) *Wall Street Journal* article, which in turn cites the McAfee (2013) study conducted jointly with the Center for Strategic and International Studies , with U.S. losses estimated to range between $25 and $100 billion per year, and global losses between $100 and $500 billion each year. The U.S. estimate of $100 billion is a significant revision, as it is an order of magnitude lower than the $1 trillion annual loss initially estimated by McAfee. The WEF (2016) report cites the McAfee (2014) global cost estimate of $445 billion per year.

More recent editions of the WEF report (2017, 2018) rated cyberattacks as the third highest risk based on likelihood, and the sixth highest risk from the impact standpoint. The impact estimates cited in WEF (2018) are significantly higher in comparison to previous editions, as well as some of the other sources discussed above. Based on the Accenture and Ponemon Institute (Richards et al., 2017) study of 254 companies in seven

countries, WEF (2018) estimates the cost of responding to a cyberattack at about $11.7 million annualized per company. The global loss estimate in the WEF (2018) is based on Juniper Research (2017), which estimated that the cost of malicious cyber activity would reach about $8 trillion over the 5-year period, bringing the annual average to $1.6 trillion. This annual estimate of $1.6 trillion is about three times higher than both McAfee (2014) and McAfee (2018) numbers.

WEF (2019) reports on the changing perception of risks with over 80% of respondents expecting cyber risks from theft of data/money (82%) and disruptions of operations and infrastructure (80%) to increase. These two risks are rated as fourth and fifth in the WEF (2019) short-term risk outlook.

Symantec (2016, 2017, 2018)

The Symantec (2016) Internet Security report cites an estimate of global cybercrime costing up to $575 billion annually. The source of the estimate is the BAML (2015) Global Research report and Thematic Investing Primer, who in turn cited the McAfee (2014) report's global loss estimate of $575 billion. BAML (2015) also cites the Ponemon Institute's (2014) estimate for the average annual cost of cybercrimes for U.S. companies in 2014, which was approximately $12.7 million per company. The BAML (2015) report also considers a potential worst-case 2020 'Cybergeddon' scenario, under which cybercrime could lead to losses reaching $3 trillion. BAML (2015) cites this $3-trillion estimate from the WEF (2014) study done in collaboration with McKinsey that was originally based on Chinn et al. (2014). However, Chinn et al.'s estimate does not seem to represent direct costs and losses, or impacts to national economies modeled in a conventional way for this context (e.g., CGE, Implan, or REMI), but rather losses of unrealized technological innovation gains assuming current cyber threat trends would persist.

Symantec (2017) mentions that one of the major sources of loss is BEC, which is essentially phishing. The cited estimates indicate that it costed more than $3 billion from 2013 to 2016, with a victim count of approximately 22,000. Symantec's estimated BEC victim count and losses align with the FBI (2016) Cincinnati announcement published in December 2016.

A subsequent FBI (2017) announcement in May 2017 includes statistics between October 2013 and December 2016, while the FBI IC3 (2018) public service announcement (PSA) on BEC fraud from July 2018 includes cumulative statistics from October 2013 through May 2018. OCE took the difference between the two PSA versions to estimate the exposed dollar loss due to BEC for January 2017 through May 2018. The Original FBI PSA statistics and the OCE-derived exposed dollar losses for BEC are presented in Table 38.

Table 38: Total BEC/EAC Victim Count and Exposed Dollar Losses (BEC/EAC Statistics Reported to the IC3 and Derived from Multiple Sources)

	Oct 2013–May 2018	Oct 2013–Dec 2016	Net: Jan 2017–May 2018
Domestic & international incidents	78,617	40,203	38,414
Domestic & international dollar loss ($ billions)	$12.5	$5.3	$7.2

Sources: FBI (2017, 2018)

A global estimate of victims and exposed losses presented in Table 38 is based on BEC statistics derived by IC3 from multiple sources, including IC3-reported complaints, international law enforcement complaint data, and filings from financial partner institutions. This global estimate brings the incident count for domestic and international BEC victims to approximately 40,203 by December 2016 and 78,617 by May 2018. Exposed losses

due to BEC accumulate to $5.3 billion by December 2016, and increase to $12.5 billion by May 2018.[33] This implies that BEC-exposed losses for January 2017 through May 2018 are approximately $7.2 billion, which is nearly 36% more than in the previous 3 years combined. Because each of the sources contributing to the PSA statistics track their BEC incidents differently, the term 'exposed' was adopted to cover actual, attempted, and linked loss amounts. The goal of this estimate is to capture the best 'global footprint' of BEC available.

Table 39 presents the BEC victim counts and exposed dollar losses for the subset of victim complaints reported to IC3, where the country was identified. The statistics are pulled from the "victim" module containing self-reported loss data and self-reported geo-location, which allows IC3 to determine the U.S. portion of BEC losses.

Table 39: BEC Victim Count and Exposed Dollar Losses (BEC/EAC Statistics Reported in Victim Complaints Where a Country was Identified)

	Oct 2013–May 2018	Oct 2013–Dec 2016	Net: Jan 2017–May 2018
Victims			
U.S.	41,058	22,292	18,766
Non-U.S.	2,565	2,053	512
Total	**43,623**	**24,345**	**19,278**
Exposed Dollar Loss ($ billions)			
U.S.	$2.94	$1.59	$1.34
Non-U.S.	$0.67	$0.63	$0.04
Total	**$3.61**	**$2.22**	**$1.39**

Sources: FBI (2017, 2018)

Between October 2013 and December 2016, the total exposed losses for the United States were about $1.6 billion. By May 2018, 17 months later, BEC losses for the United States nearly doubled to almost $3 billion. Thus, BEC is not only the primary source of losses in the U.S. complaints, but it is also showing rapid growth from 2017 to 2018.

To refine the statistics further, it is worth comparing FBI (2018) PSA exposed losses, which include actual, attempted, and linked losses, with the IC3 (2017) annual report adjusted losses. IC3 (2017, 2019, 2020) are based only the IC3 complaint data and reflect adjusted or actual losses through December 2017, 2018, and 2019, respectively.

The total actual losses reported by IC3 constituted approximately $4.12 billion by December 2016 and reached $5.52 billion by December 2017. That is, losses in excess of $1.4 billion were reported to IC3 in just 2017 (for global data across all complaint types). In IC3 (2019), the reported losses nearly doubled to $2.706 billion in 2018, increasing further to $3.5 billion in 2019 (IC3, 2020). This brings the 5-year adjusted rolling total (2015–2019) to $10.2 billion in losses (IC3, 2020).

According to the annual statistics presented in the IC3 (2017) report, out of the $1.4 billion in losses reported in 2017 complaints, $676 million dealt specifically with the BEC or email account compromise (EAC), thus accounting for 48% of the overall annual adjusted losses.

2018 BEC and EAC losses reached approximately $1.3 billion, which is a 92% increase from the previous year. In 2019, BEC and EAC losses increased by over 30% reaching $1.7 billion (IC3, 2020). The share of BEC in the total losses filed with IC3 in 2018 and 2019 remained unchanged (48%–49%).

[33] Exposed losses include both actual and attempted loss amounts.

Note that IC3 accounts for claims on a wide variety of conventional Internet crimes beyond "pure" cybercrimes such as BEC or EAC. IC3 also tracks complaints and losses due to conventional crimes conducted over the Internet, such as non-payment or non-delivery, re-shipping, confidence or romance fraud, technical support fraud, sextortion, impersonation schemes, and advanced fees. Therefore, the aggregate loss statistics from IC3 cited in Symantec (2017) are not necessarily directly comparable to other sources that have a narrower definition of cyber events, incidents, and breaches. The subtotal for the IC3 categories that are more cyber relevant is closer to $980 million in 2017 and $1.89 billion in 2018 (approximately 70% of total reported losses in each year). This brings the share of 2017 and 2018 reported BEC losses ($676 million and $1.3 billion, respectively) closer to 69% of the 2017 and 2018 annual cyber losses ($980 million and $1.89 billion respectively).

Symantec (2018) indicates that spear phishing remains the top delivery tactic, with 71% of organized groups choosing to rely on it in 2017. The second most used attack vector is watering holes (24%). Updated statistics in the IC3 (2020) report indicate that phishing/vishing/smishing/pharming remained the top incident type by the number of victims, while BEC and EAC remained the leading incident type by total loss magnitude in 2019.

Symantec also adds value to this discussion by publishing an annual summary of the underground marketplace prices for anything from payment card details to the PayPal accounts. One of the potential ways of using this information—if sufficient time series data are available at a more granular level—is assessing changes in the price of tools, services, and data for sale as an indication of effective defensive interventions or mitigations.

Cybersecurity Ventures (2016, 2017, 2018, 2019)

The Cybersecurity Ventures reports include a projection of future global losses from adversary cyber activity. The 2017 Cybercrime Report states that annual global losses from cybercrime will reach $6 trillion by 2021. Although abundant in references—albeit predominantly circular—the report and cited articles referencing other estimates by Cybersecurity Ventures and the Herjavec Group, co-author and sponsor of the report, do not contain any specific details about the assumptions or methodology behind that projection.

The magnitude of the Cybersecurity Ventures assessment is challenging to reconcile with other aggregate estimates reviewed by OCE. The projected annual loss of $6 trillion in 2021 is six times higher than the retracted McAfee (2013) projection of $1 trillion, which in turn was significantly revised down in a subsequent version. It is an order of magnitude higher than McAfee's (2018) upper-bound annual loss estimate of $600 billion, and it is three orders of magnitude higher than the $5.52 billion in cumulative actual losses reported to IC3 (2017) over the 5-year period from 2013 to 2017 or $7.45 billion in total losses reported from 2014 to 2018.

It can be argued that the difference in boundaries of the loss estimates between these sources may potentially explain some of the variability in the magnitudes. Cybersecurity Ventures' loss estimate includes the following factors: damage and destruction of data, stolen money, lost productivity, theft of IP, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

With the exception of a few cost categories (e.g., reputational harm and valuation of IP loss), the factors listed above are mostly consistent with the cost categories reflected in the estimates and sources discussed throughout the rest of this study, and shown in Appendices B and C. Moreover, some of the lower previously cited estimates include legal and PR fees, costs of ongoing investigations and data forensics, and interruptions to digital business transactions. These are explicitly excluded from the Cybersecurity Ventures estimate. In addition, other factors that are not accounted for in the Cybersecurity Ventures (2016) assessment are unreported cybercrimes, declines in stock and public company valuations directly and indirectly related to security breaches, negative impacts on post-hack ability to raise capital for start-ups, interruptions to e-commerce and other digital

business transactions, loss of competitive advantage, departure of staff, and recruiting replacement employees in connection with cyberattacks and resulting losses.[34]

Thus, even accounting for differences in the estimate boundary does not provide a sufficient explanation of how in 3 years, annual losses from adversarial cyber activity can scale up to a level that represented a third of U.S. GDP and almost 8% of the global GDP in the year of report publication (2016).[35]

Norton (2015, 2016, 2017, 2018)

Norton's (2017) Cyber Security Insights report states that global losses across 20 countries constituted $172 billion and affected 978 million consumers in 2017. About 11% of the losses ($19.4 billion) occurred in the United States and impacted 143 million consumers, bringing the average loss per victim to about $135. The report indicates that each victim spent an average of 19.8 hours (2.5 workdays) dealing with the consequences.

OCE presents the combined results from 2015, 2016, and 2017 editions of the Norton Cyber Security Insights report in Table 40 below.

Table 40: Norton Reports (2015-2017) Summary of Aggregate Loss Estimates

Year	Number of Victims (millions)		Total Losses ($ billions)		Average Hours to Resolve	
	U.S.	Global	U.S.	Global	U.S.	Global
2015	-	-	$28.9	$150.0	17.0	21.0
2016	106.6	689.4	$20.3	$125.9	12.8	19.7
2017	143.0	978.0	$19.4	$172.0	19.8	23.6

Note. Sources: Norton (2015, 2016, 2017). The number of countries covered in the global results: 17 in 2015, 21 in 2016, and 20 in 2017.

Norton's 2017 estimates are based on the self-reported data in an online survey of 21,500 respondents across 20 countries collected in October 2017. Estimates for the 2016 report are based on a sample of 20,000 respondents across 21 countries, with the online survey administered from September to October 2016. The U.S. subsample included approximately 1,000 respondents.

Besides typical cyber incidents such as credit card fraud, account password compromise, and involvement in a data breach or ransomware attack, the definition of cybercrime in the context of the Norton reports also includes traditional crimes now conducted online such as identity theft, online bullying, online purchases that turned out to be a scam, and technical support scams.

The difference in assumptions, definitions, data collection methods, and reliance on self-reported loss estimates could partially explain why the estimated losses for the United States from the Norton report are an order of magnitude higher than the annual total damages reported by Symantec (2017), which is based on IC3 estimates for the same year (i.e., $1.4 billion in annual losses and $5.5 billion in total losses between 2013 and 2017).

Norton (2018) version of the report is focused on the privacy concerns, PII data protection and ID theft. Report summarizes results of the online survey conducted by the Harris Poll in October of 2018 globally and U.S.-

[34] The CEA (2018) report discussed later in this study looks specifically at the declines in stock and public company valuations and attempts to account for underreporting. The resulting estimate assesses the upper boundary of annual losses for the United States at approximately $109 billion. This is still about an order of magnitude lower than the Cybersecurity Ventures projection of $6 trillion.

[35] According to the World Bank (2019), U.S. GDP was $18.7 trillion and global GDP was $76.1 trillion in 2016. Retrieved in April 2019. Source: https://databank.worldbank.org/data/reports.aspx?source=2&series=NY.GDP.MKTP.CD&country=

specific survey with 5000 respondents conducted by the Harris Poll in the U.S. in January of 2019. U.S. results show that on average it took consumers 3.1 hours to resolve the issues associated with the cyber crime, with median of 2 hours. If $20 per hour rate from July 22, 2019 Equifax ruling by FTC can be applied here to monetize the consumer time loss, the median cost per U.S. consumer is $40 with the average being $62. The number of victims in the U.S. was 105.4–151.9 million. Multiplying hourly loss rate by the number of affected consumers results in the aggregate costs and losses to consumers on the order of $6.5 billion to $9.4 billion based on average loss (3.1 hours per person) and $4.2 billion to $6.1 billion based on the median number of hours (2 hours spent per person).

RAND Corporation (Dreyer et al., 2018)

RAND developed a detailed set of macro estimates of the impact from cyber incidents in its "Estimating the Global Cost of Cyber Risk" study (Dreyer et al., 2018). RAND's objective was to quantify global estimates, which they calculated by aggregating individual country results. The U.S. results can be used as an example to illustrate the methodology.

The 2005 to 2015 Advisen dataset subsample containing total incident cost and company revenue information by sector serves as the basis for the U.S. estimation. The sector-specific data were bootstrapped[36] to calculate an annual total for incident costs based on first drawing a number of incidents from the set of incidents per year per sector, then drawing cost and cost-to-revenue ratios for that incident from that sector's incident data. Cost data are summed across all sampled incidents for the year to form an annual total cost. Bootstrapping for 100,000 iterations formed the desired distribution of direct costs and distribution of cost-to-revenue ratios for each sector. Quartiles for the distribution of the cost-to-revenue ratios from the RAND study (Dreyer et al., 2018) are presented in Table 41.

Table 41: RAND Cost-to-Revenue Ratios by Sector (Bootstrapped Distribution)

Sector	Percentile			
	25th	50th	75th	95th
Banking	0.01%	0.04%	0.06%	0.26%
Business & Professional Services	1.31%	10.66%	31.55%	214.89%
Consumer Goods	0.07%	1.29%	5.52%	192.78%
Healthcare & Insurance	0.09%	0.43%	0.77%	10.27%
Public	0.02%	0.09%	0.17%	1.47%
Telecom	0.02%	0.08%	0.26%	25.00%
Transportation	0.01%	2.09%	5.83%	142.88%
Wholesale & Retail	0.01%	0.11%	0.33%	3.02%
Oil, Gas, & Chemicals	0.17%	1.54%	2.97%	67.69%
Utilities	0.17%	1.54%	2.97%	67.69%
Other	0.17%	1.54%	2.97%	67.69%

Source: Adapted from *Estimating the global cost of cyber risk: Methodology and examples,* by P. Dreyer, T. Jones, K. Klima, J. Oberholtzer, A. Strong, J. W., Welburn, and Z. Winkelman, 2018, p. 22.

Since Table 41 is derived from per-incident microdata at the firm level, cost-to-revenue ratios in excess of 100% are possible, as they indicate that incident costs exceed annual revenue for the company. RAND calculates GDP at risk by applying the cost-to-revenue ratio to the corresponding sector's annual GDP and summing across the sectors. The results of this scaling are presented in Table 42 below.

[36] For more information on bootstrapping please see https://towardsdatascience.com/an-introduction-to-the-bootstrap-method-58bcb51b4d60?gi=f08ac2500824

Table 42: RAND GDP at Risk by Percentile

	Percentile			
	25th	50th	75th	95th
Direct cost (% of GDP)	0.2%	1.7%	4.8%	55.4%
Total direct cost	$ 27.8 billion	$241.9 billion	$665 billion	$7.71 trillion

Source: Adapted from *Estimating the global cost of cyber risk: Methodology and examples,* by P. Dreyer, T. Jones, K. Klima, J. Oberholtzer, A. Strong, J. W., Welburn, and Z. Winkelman, 2018, p. 23.

RAND's results suggest that the median exposure from cyber incidents is approximately $242 billion nationally (Dreyer et al., 2018). This number is fundamentally different than the results calculated via linear scaling in Romanosky (2016). Considering that both sets of the estimates are based on the Advisen data, it is instrumental to understand the model design and scaling steps in the RAND study.

First, applying the firm-level cost-to-revenue ratios to sector-specific GDP means that all entities within that sector are exposed at that rate. For example, if the median incident cost-to-revenue ratio for business and professional services is about 11%, applying it to that sector's annual GDP to obtain the median exposure level implies all firms within that sector are exposed at 11% of their revenue, irrespective of the number of entities or the incident rate in this sector. So if the exposure is at 11% for the companies that did get breached, but the incident rate is only 1.5% (i.e., only an average of 1.5% of entities got breached per year), further scaling would produce a value that denotes losses instead of exposure, following the nomenclature in this study.

Second, the implication is that values in excess of 100% at the firm level, when scaled to the annual GDP level, essentially eliminate that industry's total output for more than a year if a breakdown by sector is shown. When summed across the sectors and presented as a percentage of overall GPD, the implication of having values above 100% in the sum product is essentially spilling over and eliminating output in other industries in the aggregate sum. Thus, the result that denotes direct cost as a percentage of GDP may need a different characterization that does not rely on an annual metric as a comparison benchmark, or the derived results may need to be heavily caveated with these considerations.

A computational result that could be comparable to other aggregate loss studies is the intermediate bootstrapping output, where the number of incidents is first drawn from the set of incidents per year per sector, then cost is drawn for that incident from that sector's incident data. Cost data is subsequently summed across all sampled incidents for the year to form annual total loss.

CEA (2018)

The White House CEA (2018) issued The Cost of Malicious Cyber Activity to the U.S. Economy report, where scarcity of data is identified as one of the major challenges associated with developing a national loss estimate. To address this challenge, the CEA report estimated the cost of malicious cyber activity to the U.S. economy by evaluating changes in stock prices following the disclosure of a data breach. The resulting estimate of national losses ranged between $57 billion and $109 billion in 2016, representing between 0.31% and 0.58% of the 2016 GDP. CEA's estimate is higher than the loss values estimated in Romanosky (2016), Biener et al. (2015), and NetDiligence (2017), but is lower than the McAfee (2018) estimates. The difference between the estimates can be explained by examining the CEA report's assumptions and methodology.

The CEA report uses the change in stock prices of breached companies within a 7-day window of the breach disclosure (as recorded in Thomson Reuters between January 2000 and January 2017) as the per-event loss estimate. The dataset contains news of 290 adverse cyber events committed against 186 unique firms. Based on the 7-day difference between stock price return and the market return, the average loss was estimated at

0.8% of the market value. For the 159 events between 2014 and January 2017, the 7-day stock price changes equaled 1.01%.

Given the capitalization level of the studied companies, this approximated to $498 million in average losses per adverse cyber event, with a median loss of about $15 million per event. The average losses per cyber event decreased to $338 million if the 1% tail (i.e., the most expensive incidents) was removed. CEA per-event estimates exceed average per-event estimates in Romanosky (2016), NetDiligence (2017), and Ponemon Institute (2017) by two orders of magnitude.

CEA applied the 7-day stock price reaction of 1.01% to the market value of all publicly traded companies ($26.6 trillion). Then based on the annualized Ponemon Institute (2017) survey breach rate, CEA applied a breach frequency of 13.85% to derive the $37.2 billion loss estimate. It should be noted that the Ponemon Institute survey results are not based on a statistically representative sample to support such inference.

To account for additional impacts (such as spillover effects, the closely held and government entities segment not accounted for in the market capitalization data, as well as the cost incurred by private individuals) the initial CEA estimate of $37.2 billion is further scaled up to $57.1 billion based on CEA's additional bridging assumptions.

By relying on stock prices changes, the CEA methodology is able to include breaches that are both observed and disclosed, but not those that are (1) unobserved and undisclosed, and (2) those that are observed and undisclosed. To address this challenge, the CEA (2018) report assumes that 3% of observed breaches are observed and disclosed, that 97% remain either unobserved or undisclosed, and that the impacts to the sample of firms with observed and disclosed breaches is representative of those that are unobserved and undisclosed. The upper-bound estimate of $109 billion is developed by scaling 34 incidents in Thomson Reuters for 2016 up by 97% to represent 1,156 breaches for 2016. This, in turn, comprises 26.78% of all publicly traded firms. Using this value instead of the Ponemon Institute's (2017) breach frequency (13.85%), while holding the rest of the assumptions fixed, nearly doubles the loss estimate from $57 billion to $109 billion.

Typically, unrealized losses, such as differences in market performance (especially short-term stock price fluctuations), are not allowed to be included in damage assessments, as shown in Romanosky et al. (2019). Further, several studies that looked into the recent data breaches found no statistically significant market reaction in either the short or long term after the breaches occurred. Alternatively, a slight stock price decrease was followed by a quick recovery. This aspect is discussed in more detail in Section 3.3. The canonical approach to event studies includes the normalization of market performance of the impacted companies by comparing it against a control group represented by market indices. That is, analysts attempt cyber incident's impact on market fluctuations from the dominant market trends driving the overall stock performance. Yet details of the cyber incident become known as the investigation proceeds, with varying degrees of information known or announced at the time of incident disclosure. Therefore, full details of the event are rarely known to the market within the 7-day time period chosen for analysis.

The CEA (2018) results hold to the extent one is willing to accept CEA calculation steps as a defensible approach for extrapolating per-event losses to the national level on an annual scale, namely:

(1) The 7-day stock market performance scaled up;
(2) By either the Ponemon Institute's breach frequency of 13.85%, or, alternatively;
(3) By an assumed underreporting rate of 97%; and
(4) Applied to a small sample of disclosed breaches in 2016 (34 incidents).

The bridging assumptions, such as the Ponemon Institute's incident rates, are not based on the statistically representative sample to support the inference. However, most of the data sources providing the incident rate or

incident frequency estimates share the same predicament. Also, strong underreporting assumptions may carry adverse implications for the effectiveness of the breach disclosure guidelines.

B.4 Individual Case Studies of Sets of Hypothetical Scenarios

Below, OCE summarizes cost estimates developed for hypothetical scenarios intended to demonstrate the possible breadth, depth, and rate of propagation of the negative consequences of cyber incidents and resulting extreme magnitudes of associated losses.

Lloyd's (2015)

Lloyd's (2015) explores the impacts of several severity and duration scenarios for a single power outage blackout event. The scenarios are intentionally extreme to demonstrate the potential extent of cyber risks and resulting consequences. The emphasis is not on the probability of the scenarios, but on the technical possibility of extreme events of these magnitudes.

The Lloyd's (2015) hypothetical scenario assumes a blackout across 15 states with 93 million people losing power. The factors that drive the severity of the consequences are a decline in trade, a disruption of water supply, a collapse of infrastructure with subsequent disruption of the transportation systems, and increased mortality rates due to disruptions and failures of health and safety systems.

The aggregate impact at the national level is approximately $243 billion, rising to more than $1 trillion for the most extreme set of assumptions. The report intentionally postulates a scenario where a wide range of claims could be triggered by one event. Note that the lower-bound estimate for this scenario ($243 billion) is very close to the median exposure due to malicious cyber activity in the RAND study (Dreyer et al., 2018), which was approximately $242 billion.

Lloyd's (2017)

Lloyd's (2017) is focused on a more clean-cut cyber scenario without triggering physical consequences. The 2017 report considers cloud service provider interruption scenarios and operating system (OS) vulnerability. Again, the factors and scenario assumptions are intentionally structured to accommodate depth, breadth, and a rate of propagation that could result in a minimum of 55 hours in downtime, thus driving the startlingly high magnitude of impacts.

The losses range from $4.6 to $53.05 billion for cloud service disruption and $9.68 to $28.72 billion for an OS mass vulnerability scenario. These magnitudes could be significantly exacerbated due to loss aggregation. For example, in the cloud disruption scenario, the upper-bound estimate can jump from $4.6 billion to $53.05 billion to over $121.41 billion from just this single postulated event.

Lloyd's (2018)

The Lloyd's (2018) study is done in collaboration with AIR estimates impacts from a set of scenarios involving extended cloud outages by leading cloud service providers (i.e., the top 15 providers in the United States, which accounted for 70% of the market share). Three outage duration scenarios are considered in the analysis: 0.5 to 1 days; 3 to 6 days; and 5.5 to 11 days. However, losses persist longer than the outage duration.

Instead of using market share allocations for the impacts, this study considers relationships between specific cloud service providers and their customers, and then incorporates customer characteristics to estimate exposure. This allowed Lloyd's to establish patterns of association between otherwise seemingly uncorrelated losses. A bottom-up aggregation of the losses per scenario is then performed to assess overall impact.

In this cloud outage study, the losses were calculated on a per-provider basis. The total losses for an incident that would take one of the top three largest cloud providers offline range from $2.8 billion to $5.9 billion for a 0.5- to 1-day outage (Scenario 1), $6.9 billion to $14.7 billion for a 3- to 6-day outage (Scenario 2); and $11.2 billion to $23.8 billion for a 5.5- to 11-day outage (Scenario 3).

For an outage involving a small cloud provider, one that has the 10th to 15th largest market share in the United States, the impacts are significantly lower. For Scenario 1, the loss is approximately $0.4 to $0.9 billion; for Scenario 2, the loss is about $1.1 billion to $2.1 billion; and losses reach $1.7 billion to $3.4 billion for Scenario 3.

Losses for a single large provider outage in this study are approximately half the loss estimates in Lloyd's (2017) cloud service disruption analysis.

Lloyd's (2019)

Lloyd's (2019) explores potential losses for a global malware attack by considering three scenarios with various durations and severities. Scenario 1 assumes a 43.1% global infection rate of devices with one particular operating system. Scenario 2 assumes two operating systems are impacted, which results in 97.3% of devices being infected globally. Scenario 3 assumes the same infection rate as Scenario 2, however, the negative consequences are exacerbated by a backup wiper (i.e., malware that deletes the backups and shadow copies, and destroys data and systems). The impacts for the three scenarios were estimated at $85 billion, $159 billion, and $193 billion, respectively.

Similar to other impact estimates based on the hypothetical extreme scenarios, this study emphasizes the insurance gap resulting from a severe correlated loss. The insurance gap is a shortage between the total collected premiums and the total payouts that would have to occur on underwritten policies under the assumed scenario. Specifically, the 2019 estimated global cyber insurance premium is approximately $6.4 billion, while the losses from the considered scenarios exceed the premium by 1.2 to 3.4 times. This means that insurance companies can experience significant financial losses because of the systemic correlated cyber risk presented by malware.

This scenario-based analysis is not performed with intent of assessing direct economic losses in the traditional sense of consequence quantification, but rather relies on the stochastic probable maximum loss modeling to assess extreme exposure accumulation from a cyber insurance standpoint. In that sense, the losses from a single scenario in Lloyd's (2015) and Lloyd's (2019) studies are comparable with RAND's (Dreyer et al., 2018) sector and aggregate national estimates.

Although this range of impacts from a single event has not materialized in the past, the recent cyberattacks on the Ukrainian grid and the scale of the WannaCry and NotPetya infections clearly demonstrated the viability of scenarios with significantly amplified breadth, depth, and rate of propagation to potentially trigger the Lloyd's (2015, 2019) estimated level of losses. These estimated level of losses, in turn, are significantly higher than Lloyd's (2017, 2018) extreme scenarios.

However, even the highest of these hypothetical scenario-based estimates are still only a fraction of the BAML (2015) estimate that considers a potential worst-case 2020 "Cybergeddon" scenario, which stated that cybercrime could put at risk up to $3 trillion of global economic value. In turn, the BAML "Cybergeddon" estimate is only half of the $6 trillion annual loss projected for 2021 by Cybersecurity Ventures (2017)—another example of an assessment that is challenging to cross-validate and reconcile.

To summarize, the objective of these intentionally severe scenarios is to explore extreme losses and risk accumulation. They are constructed with hypothetically high rates of depth, breadth, and propagation to illustrate

a severe but plausible magnitude of consequences. Since the resulting impacts are extreme by design, they do not constitute a defensible benchmark or baseline level of losses to serve as a standalone basis for ROI or cost-benefit analysis. Instead, they are intended as stress tests to understand extreme tail risk, how it can scale, and the resulting potential gap between the total coverage and total premiums in cyber insurance (Coburn et al., 2018). Essentially, they are meant to support cyber insurance portfolio allocation decisions and risk accumulation management in the cyber insurance industry at the aggregate level. Therefore, it is not appropriate to use loss estimates from these studies to motivate increased investment in specific tools, technologies, or processes at an individual company or agency level.

APPENDIX C – ITEMIZED COST OF LARGE INCIDENTS

In this appendix, OCE describes the itemized costs for the 12 largest incidents discussed in Section 3.1.1. Table 43, below, summarizes the itemized costs for each incident and presents the primary source OCE used to develop the costs described below.

Table 43: Costs, Cost-to-Revenue Ratios, and People Affected (Large Incident Sample)

Company Affected	Year of Incident	Total Cost ($ million)	Cost-to-Revenue Ratio	Number of People/Records Affected (millions)	Primary Source
Equifax*	2017	700	4.88%	145.5	Prior, R. (2019)
Anthem	2015	375.5	0.48%	78.8	Anthem (2015)
Yahoo	2014	350	7.58%	500	Armerding (2018a)
Merck	2017	310	0.78%	-	Gunderman (2017)
Target	2013	292	0.41%	70	Armerding (2018a)
Home Depot	2014	252	0.30%	56	Armerding (2018b)
Sony PlayStation	2011	171	0.20%	101.6	*Sony Agrees* (2014)
Equifax	2017	164	4.88%	145.5	Equifax (2018)
Sony Pictures	2014	43	0.06%	0.047	Armerding (2018b)
Experian	2015	20	0.42%	15	Experian (2016)
Yahoo	2013	16	0.34%	1,000	Jay (2017)
Ashley Madison	2015	12.8	11.74%	37	Stempel (2017)
LinkedIn	2012	4	0.41%	6.5	Lennon (2017)

Note. The primary source column presents the primary source used to construct the total cost estimate.

Anthem – 2015 Breach

In 2015, the United States' largest healthcare insurance provider, Anthem, experienced a data breach that affected 78.8 million people and leaked PII and financial information (Freeman, 2017; Pierson, 2017). The total reported cost of the Anthem breach was $375.5 million (OCE). $115 million went toward a settlement for those affected by the breach (Freeman, 2017). $31 million was spent on notification and $112 million was spent on credit monitoring (McGee, 2017). The remaining $117.5 million was used to contract third party security experts ($2.5 million) and implement security improvements ($115 million) (McGee, 2017). Anthem's operating revenue was $78.4 billion for 2015 (Anthem, 2015) with the cost of this breach 0.48% (OCE) of operating revenue.

Yahoo – 2014 Breach

In 2014, Yahoo announced a major breach of about 500 million user accounts during which names, email addresses, telephone numbers, birth dates, encrypted passwords, and security questions were released (Perlroth, 2016, Armerding, 2018b). At the time, Verizon was in the process of acquiring Yahoo for $4.8 billion, but later revised the deal due to the data breach for a sale price of $4.48 billion—a $350 million reduction in price due to the data breach (Armerding, 2018b; Goel, 2017). This breach's cost was 7.58% (OCE) of Yahoo's 2014 revenue ($4.62 billion) (Yahoo, 2014).

Merck – 2017 Incident

The NotPetya ransomware campaign impacted FedEx, Maersk, and Merck. Specifically for Merck, the 2017 Quarter 3 losses equaled $135 million from lost sales and approximately $175 million in costs, spread across the cost of goods sold and the operating expense lines (Gunderman, 2017). Quarter 4 losses were anticipated to reach the same mark. Merck experienced a production shutdown that resulted in a drop in sales of nearly $240

million (Davis, 2017). While the loss is significant in absolute terms, Merck is one of the largest pharmaceutical company in the United States with over $40 billion in sales (Merck, 2017). Merck's research and development budget in 2016 alone was approximately $9 billion. Cost-to-revenue ratio for this breach was 0.78% (OCE).

Target – 2013 Breach

Target announced a breach of its point-of-sales systems in 2013 that released 40 million payment cards and 70 million other records containing PII (Armerding, 2018b). According to Target's 2016 Annual Report, the total cost of the breach was $292 million (Target, 2017). Of this total cost, $67 million was paid out as a settlement to Visa (Garcia, 2015); $10 million was paid to settle a class action lawsuit for impacted customers (Garcia, 2015); and $39 million was paid in a settlement for affected banks (Rashid, 2017; Lynch, 2017). Target's insurance covered $90 million and Target was able to deduct an additional $52 million in taxes for breach-related costs (Target, 2017). Target's total revenue in 2013 was $71.3 billion (Target, 2017) with the breach costing 0.41% (OCE) of total revenue.

Home Depot – 2014 Breach

In 2014, Home Depot experienced a breach of its payment card systems that resulted in the loss of credit and debit card information and the email information of 56 million customers (Armerding, 2018b). The total reported cost for the breach was $252 million (Allison, 2015). The majority of this cost ($134.5 million) was paid to Visa, MasterCard, and various banks in compensation for the breach (Cost of a retail data breach, 2017). An additional settlement with banks cost Home Depot $25 million (Cost of a retail data breach, 2017, Roberts, 2017). $19.5 million was paid in a settlement to impacted customers (Armerding, 2018b). Home Depot's insurance covered $100 million of these costs (Allison, 2015). The company's 2014 revenue was $83.2 billion (Home Depot, 2014) and the total cost of the breach was 0.30% of this total revenue.

Sony PlayStation Network – 2011 Breach

A hack of the Sony PlayStation Network, namely Computer Entertainment America LLC, Sony Online Entertainment LLC (SOE), and Sony Network Entertainment International LLC, resulted in the breach of 101.6 million Sony accounts (including PII and Payment Card Industry information) and a 23-day closure of the network. Sony reports that it spent $171 million (Martinez, 2011) on total breach costs including: a $19 million settlement for a class action lawsuit; a $1 million settlement to reimburse identity theft charges (Asbury, 2014); $14 million to make subscribers whole again; $2.75 million in attorney fees (Asbury, 2014); as well as $1.25 million in notice costs and administrative costs, credit monitoring costs, and other related costs (Asbury, 2014). Sony's reported revenue for 2011 was $83.8 billion (Sony Corporation, 2013). Therefore, this breach cost 0.2% of Sony's 2011 revenue.

Equifax – 2017 Breach

In 2017, Equifax went through a data breach that leaked 146 million customers' PII including social security numbers and driver's license numbers. Equifax 2017 annual report shows that it incurred $164 million in total pre-tax costs (Equifax, 2018). The expenses included $55.5 million in credit monitoring, $17.1 million in external consulting, and $14.9 million in customer support (Dignan, 2017). Using Equifax's total revenue for 2017 of $3.36 billion (Equifax, 2018), the cost of the breach was estimated to be 4.88% of revenue. Insurance payout of $50.0 million brings net expenses down to $114.0 million (Equifax, 2018), which is 3.39% of the revenue. Note, the total cost of the incident is not fully known yet as litigation and fines were still in the early stages against Equifax, when the OCE analysis was conducted. However, as of May 2019, Moody's downgraded Equifax's rating to negative specifically naming cyber as a factor in rating change, with $690 million 2019Q1 expenses for the breach as contributing to the downgrade. This is the company's future cost estimate for settling ongoing class action cases, as well as potential federal and state regulatory fines. Then on July 22, 2019, FTC ruled to impose

a fine of $700 million in individual compensation and civil penalties.[37]

Sony Pictures – 2014 Breach

Sony Pictures experienced an intrusion in 2014 that resulted in the leaking of celebrity PII, five Sony films, and private employee PII, and financial information. The breach affected 47,000 people. To resolve a class action lawsuit, Sony agreed to settle with employees whose data was breached with a payout of $8 million to cover damages and legal costs (Raymond, 2015). Sony reported a cost of $15 million for cleanup and investigation into the incident during the last quarter of 2014 (Frizell, 2015; Lemos, 2015), and the chief financial officer reported the total cost to be $35 million (Lemos, 2015). The National Association of Theater Owners estimates that Sony lost about $30 million of sales due to the leak of their unreleased movie "The Interview." (McClintock, 2015). Sony Pictures' 2014 revenue was $8.3 billion and the total cost of the breach was $43 million (Sony Corporation, 2014). Thus, the breach cost 0.52% of Sony Picture's revenue. Sony's total reported revenue for 2014 was $77.6 billion (Sony Corporation, 2014). Therefore, this breach cost 0.06% of Sony's total 2014 revenue.

Experian – 2015 Breach

In 2015, Experian suffered an intrusion into its systems that resulted in 15 million records of customer information from T-Mobile being breached. Experian reported a cost of $20 million in one-time costs to respond to the incident (*Update 1-Experian*, 2015). Experian's revenue for 2015 was $4.81 billion (Experian, 2016), with the costs of this breach equaling 0.42% of revenue.

Yahoo – 2013 Breach

A breach of Yahoo in 2013 leaked approximately 1 billion user accounts. A reported $5 million was spent on forensics and $11 million on legal actions (Jay, 2017). This cost is not representative of the total cost of the breach, since some costs got wrapped up into the 2014 breach. Yahoo's revenue for 2013 was $4.68 billion (Statista, 2018) making this breach 0.34% of its total revenue.

Ashley Madison – 2015 Breach

In 2015, Ashley Madison experienced a data breach that released the PII of 37 million members. The breach initiated difficulties for the company, causing it to rebrand. Ashley Madison agreed to an $11.2 million settlement for victims of the breach and a $1.6 settlement with the Federal Trade Commission for lax security practices (Stempel, 2017). Ashley Madison's revenue was $109 million in 2015, and the total direct costs as a percentage of this revenue were 11.74%.

LinkedIn – 2012 Breach

LinkedIn suffered a breach in 2012 that leaked 6.5 million email and encrypted passwords combinations. LinkedIn spent $1 million on investigation and forensics of the incident, and another $3 million on repairing and upgrading security measures and systems (Lennon, 2012; Fontana, 2012). LinkedIn's total revenue for 2012 was $972.3 million (LinkedIn Corporation, 2013). Therefore, this incident cost 0.41% of LinkedIn's total revenue.

[37] https://www.cnn.com/2019/07/25/us/equifax-700-million-settlement-data-breach-trnd/index.html

Table 44: Summary of Itemized Costs for Large Incidents, $ Millions

Affected Entity	Yahoo - 2014	Target	Sony Pictures	The Home Depot	Sony PlayStation Network
Primary Source	Armerding (2018a,b)	Armerding (2018a,b)	Armerding (2018a,b)	Armerding (2018a,b)	*Sony Agrees* (2014)
Info Type	PII	PII, PCI	PII, PCI	PII, PCI	PII, PCI
Number of Records Affected (millions)	3,000	110	47	56	102
Total Cost ($ millions)	$350	$292	$43	$252	$171
Incident Investigation & Forensic Analysis	-	-	-	-	-
Incident Response & Containment (Direct Response, Cleanup, & Recovery Costs):	-	-	$15.0	-	-
Patching & Updates	-	-	-	-	-
Cleanup & Removal of Artifacts	-	-	-	-	-
Network Countermeasures & Reconfiguration	-	-	-	-	-
Network Mitigation	-	-	-	-	-
Installation of Additional Authentication & Security Solutions	-	-	-	-	-
Other IT & Cyber Services to Clean up the Incident	-	-	-	-	-
Data Management to Upgrade Privacy Policy Changes	-	-	-	-	-
Data Restoration from Backup	-	-	-	-	-
Documentation & Reporting	-	-	-	-	-
Other Contracted Third-Party Services for Incident Response & Recovery Including Staff Augmentation	-	-	-	-	-
Hardware Upgrade or Replacement	-	-	-	-	-
Software Upgrade or Replacement	-	-	-	-	-
Incident-Induced Staff Hiring	-	-	-	-	-
Incident-Induced Additional Training (Staff Time & Acquisitions for Development & Implementation)	-	-	-	-	-
Management, General Council, Public Affairs, etc.	-	-	-	-	-
Cost of PR Campaign or Crisis Management Services	-	-	-	-	-
Lost Revenue or Productivity:	-	-	-	-	-
Business Interruption or Downtime	-	-	-	-	-
Lost Transactions, Sales, or Revenue	$350.0	-	-	-	-
Other Mission Disruptions _____	-	-	-	-	-
Theft, Fraud, & Direct Financial Losses:	-	-	-	-	-
Financial Theft & Fraud	-	$67.0	-	-	-
Extortion Demands & Costs	-	-	-	-	-
Credit Card & Account Losses	-	-	-	-	-
Other _____	-	-	-	-	-
Legal Fees & Regulatory Fines:	-	-	$8.0	-	-

Affected Entity	Yahoo - 2014	Target	Sony Pictures	The Home Depot	Sony PlayStation Network
Legal Fees/Individual Litigation/Class Action	-	$49.0	-	-	$19.0
Attorney Fees	-	-	-	-	$2.8
Liability Claims/Restitution	-	-	-	-	-
Regulatory Fines, Fees, & Assessments	-	-	-	-	$1.3
Additional Reserve Requirements	-	-	-	-	-
Other Fees & Fines _____	-	-	-	-	-
Victim Notification & Protection Services:	-	-	-	-	$14.0
Victim Notification	-	-	-	-	-
Credit Monitoring & Identity Theft Protection/Repair	-	-	-	-	$1.0
Other Third-Party Services	-	-	-	-	-
Reserve Fund Requirement	-	-	-	-	-
Other Losses:	-	-	-	-	-
Loss of IP	-	-	-	-	-
Loss of System Functionality	-	-	-	-	-
Loss of PII, PHI, etc.	-	-	-	-	-
Physical Asset Damage	-	-	-	-	-
Bodily Injury	-	-	-	-	-
Loss of Life	-	-	-	-	-
Environmental Damage	-	-	-	-	-
Other _____	-	-	-	-	-

Note. IT = information technology; PR = public relations; IP = intellectual property; PII = personally identifiable information; PHI = personal health information.

Affected Entity	Equifax	LinkedIn	Yahoo - 2013	Experian	Ashley Madison	Anthem
Primary Source	Lennon (2017)	Lennon (2017)	Jay (2017)	Experian (2016)	Stempel (2017)	Anthem (2015)
Info Type	PII	PII	PII	PII	PII	PII & Financial
Number of Records (millions)	-	7	1,000	15	37	79
Total Cost ($ millions)	$87.5	$4.0	$16.0	$20.0	$12.8	$375.5
Incident Investigation & Forensic Analysis	-	$1.0	$5.0	-	-	-
Incident Response & Containment (Direct Response, Cleanup, and Recovery Costs):	-	$3.0	-	-	-	$117.5
Patching & Updates	-	-	-	-	-	-
Cleanup/Removal of Artifacts	-	-	-	-	-	-
Network Countermeasures & Reconfiguration	-	-	-	-	-	-
Network Mitigation	-	-	-	-	-	-
Installation of Additional Authentication & Security Solutions	-	-	-	-	-	-
Other IT & Cyber Services to Clean Up the Incident	-	-	-	-	-	-
Data Management to Upgrade Privacy Policy Changes	-	-	-	-	-	-
Data Restoration from Backup	-	-	-	-	-	-
Documentation & Reporting	-	-	-	-	-	-
Other Contracted Third-Party Services for Incident Response & Recovery Including Staff Augmentation	-	-	-	-	-	$2.5
Hardware Upgrade or Replacement	-	-	-	-	-	-
Software Upgrade or Replacement	-	-	-	-	-	-
Incident-Induced Staff Hiring	-	-	-	-	-	-
Incident-Induced Additional Training (Staff Time & Acquisitions for Development & Implementation)	-	-	-	-	-	-
Management, General Council, Public Affairs, etc.	-	-	-	-	-	-
Cost of PR Campaign or Crisis Management Services	-	-	-	-	-	-
Lost Revenue or Productivity:	-	-	-	-	-	-
Business Interruption/Downtime	-	-	-	-	-	-
Lost Transactions/Sales/Revenue	$55.5	-	-	-	-	-
Other Mission Disruptions _____	-	-	-	-	-	-
Theft/Fraud/Direct Financial Loss:	-	-	-	-	-	-
Financial Theft & Fraud	-	-	-	-	-	-
Extortion Demands & Costs	-	-	-	-	-	-
Credit Card & Account Losses	-	-	-	-	-	-
Other _____	-	-	-	-	-	-
Legal Fees & Regulatory Fines:	-	-	$11.0	-	-	-

Affected Entity	Equifax	LinkedIn	Yahoo - 2013	Experian	Ashley Madison	Anthem
Legal Fees/Individual Litigation/Class Action	-	-	-	-	$11.2	$115.0
Attorney Fees	-	-	-	-	-	-
Liability Claims/Restitution	-	-	-	-	-	-
Regulatory Fines, Fees, & Assessments	-	-	-	-	$1.6	-
Additional Reserve Requirements	-	-	-	-	-	-
Other Fees & Fines _____	$17.1	-	-	-	-	-
Victim Notification & Protection Services:	-	-	-	-	-	-
Victim Notification	-	-	-	-	-	-
Credit Monitoring & Identity Theft Protection/Repair	-	-	-	-	-	$112.0
Other Third-Party Services	$14.9	-	-	-	-	-
Reserve Fund Requirement	-	-	-	-	-	-
Other Losses:	-	-	-	-	-	-
Loss of IP	-	-	-	-	-	-
Loss of System Functionality	-	-	-	-	-	-
Loss of PII, PHI, etc.	-	-	-	-	-	-
Physical Asset Damage	-	-	-	-	-	-
Bodily Injury	-	-	-	-	-	-
Loss of Life	-	-	-	-	-	-
Environmental Damage	-	-	-	-	-	-
Other _____	$87.5	-	-	-	-	-

Note. IT = information technology; PR = public relations; IP = intellectual property; PII = personally identifiable information; PHI = personal health information.

APPENDIX D – ITEMIZED COST, SMALLER INCIDENTS

In this appendix, OCE describes the itemized costs for the smaller incidents discussed in Section 3.1.1. Table 45, below, summarizes the itemized costs for each incident and presents the primary source OCE used to develop the costs described below.

Table 45: Costs, Cost-to-Revenue Ratios, and People Affected (Smaller Incident Sample)

Entity	Total Cost ($ millions)	Cost-to-Budget Ratio[a]	Number of People/Records Affected[b] (millions)	Primary Source[c]
Internal Revenue Service (IRS)	$30.00	0.23%	0.10	Rubin & Belkin (2017)
Maricopa County Colleges	$26.02	3.64%	2.00	Faller (2014)
South Carolina's Department of Revenue	$12.13	0.05%	0.40	Shain (2015)
Michigan State University	$9.40	0.22%	0.40	Weidmayer (2016)
State of Utah, Medicaid Server	$9.00	0.08%	0.78	Insurance Journal (Associated Press, 2013)
NationWide Insurance	$5.50	0.03%	1.27	Gallagher (2017)
Ohio State University	$4.00	0.08%	0.76	Book, Jurich, & Marotti (2010)
Bank of New York Mellon	$3.63	0.03%	0.641	State of Connecticut Department Of Banking (2009)
Rosen Hotels & Resorts	$2.34	N/A	Unknown	Brinkmann (2017)
Ingham County, MI	$1.46	0.63%	Unknown	Lacy (2017)
Georgia, State voters' data	$1.20	0.06%	6.00	Torres (2015)
Wisconsin Department of Revenue	$1.00	0.02%	0.17	Levin (2012)
Allentown, PA	$1.00	0.92%	Unknown	Blake (2018)
Orange County Transportation Authority	$0.66	0.01%	N/A	Gerda (2016)
City of Fort Lauderdale	$0.43	0.08%	N/A	Barszewski (2015)
Ferris State University	$0.38	0.13%	0.06	McVicar (2013)
Madison County, Indiana	$0.24	0.83%	N/A	Ragan (2016)
Cuesta College, San Luis Obispo	$0.16	0.34%	N/A	Lambert (2015)
University of California, Berkeley	$0.15	0.01%	0.002	Schaffhauser (2014)
University of Central Florida	$0.11	0.01%	0.06	Russon (2016)
Anderson County, TN	$0.10	0.38%	0.002	Huotari (2016)

[a] This is calculated as the cost of an incident as a percentage of the annual operating budget.
[b] "Unknown" means a metric other than number of records specified, and "N/A" means no records were breached, but an incident that required cleanup still occurred.

Internal Revenue Service (IRS) – 2017 Breach – Rubin (2017)

In 2017, the IRS's financial tool was breached, exposing 100,000 records that resulted in 8,000 fraudulent reports being filed. This breach cost the IRS a total of $30 million (Rubin and Belkin, 2017). The IRS's operating budget for 2017 was $13.24 billion (IRS, 2016), making the cost of this breach 0.23% of the 2017 budget.

Maricopa County Colleges – 2013 Breach – Faller (2014)

In 2013, Maricopa County Colleges experienced a breach of 2 million records of PII, including social security numbers and banking information. The total cost of the breach was $26 million with $7.5 million spent on third-party incident response, $9.3 million spent on legal costs, $7 million spent on notification and credit monitoring, and $2.2 million spent on records management and PR (Faller, 2014). The operating revenue for Maricopa County Colleges for FY2013 and FY 2014 were $683 and $715 million respectively (Maricopa County Community College District, 2013, 2014), making the cost of this breach 3.64% of their budget.

South Carolina's Department of Revenue – 2012 Breach – Shain (2012)

In 2012, South Carolina's Department of Revenue suffered a data breach of 400,000 records. The breach cost $12.125 million, with $125,000 for consulting with the security company, Mandiant, and $12 million for credit monitoring and identity theft protection (Shain, 2012). South Carolina's total operating budget for 2012 was $23.11 billion (State of South Carolina, 2012), making this breach 0.05% of the budget.

Michigan State University – 2016 Breach – Weidmayer (2016)

Michigan State University suffered a breach of 400,000 records and consequently paid out $2.9 million for credit monitoring (Weidmayer, 2016). Total Michigan State University revenue for 2016-2017 (general fund) equaled $1.3 billion (Michigan State University, 2017). The cost of the breach is 0.22% of the operating budget.

The State of Utah – 2012 Breach – Insurance Journal (2013)

In 2012, the State of Utah suffered a breach of 780,000 Utah residents' health records from an unsecured state Medicaid server. The State of Utah reported a direct loss due to the breach of $9 million, including costs of $467,000 for hotline and community meetings, $1.9 million for credit monitoring, $1.2 million on a security review of state servers, and $4.4 million for security fixes and upgrades (Associated Press, 2013). Utah's total fiscal year 2012 operating budget was $12 billion (Utah State Legislature, 2012). This breach cost 0.075% of the 2012 budget.

Nationwide Mutual Insurance Company – 2012 Breach – Gallagher (2017)

The Nationwide Mutual Insurance Company suffered a data breach in 2012 of 1,270,000 records, resulting in a $5.5 million multistate settlement (Gallagher, 2017). Nationwide Mutual Insurance collected $16.3 billion in premiums in 2012 (Nationwide Mutual Insurance Company, 2012). This breach cost is approximately 0.03% of the total premiums earned.

Ohio State University – 2010 Breach – Book (2010)

In 2010, Ohio State University suffered a breach of 760,000 records and spent $4 million for consulting, notification, credit monitoring, and a call center (Book, Jurich & Marotti, 2010). The breach cost 0.083% of the university's 2010-2011 operating budget of $4.8 billion (The Ohio State University, 2010).

Bank of New York Mellon – 2008 Breach – Connecticut Department of Banking (2009)

A breach of the Bank of New York Mellon leaked 640,994 records in 2008, resulting in $3.48 million spent on credit monitoring and $50,000 paid in fines to the State of Connecticut for a total cost of $3.63 million (State of Connecticut Department of Banking, 2009). The Bank of New York Mellon's 2008 operating budget was $13.7 billion, making this leak 0.03% of the 2008 revenue (The Bank of New York Mellon Corporation, 2008).

Rosen Hotels & Resorts – 2016 Breach – Brinkmann (2017)

A 2016 breach of Rosen Hotels & Resorts resulted in an unknown number of records being disclosed, and a total cost of $2.34 million, including $150,000 on digital forensics, $50,000 in attorney fees, $2 million in fines from

Visa and MasterCard ($1 million each), a $128,830 fine from American express, and $15,000 in crisis management consulting (Brinkmann, 2017). Information on the 2016 annual revenue was not available.

Ingham County, Michigan – 2017 Incident – Lacy (2017)

Ingham County (of Michigan) suffered an incident that affected 1,600 workstations, costing a total of $1.46 million, including $41,044 for 1,460 regular employee hours, $25,451 for 559 hours of overtime, $17,000 for consulting, $3,000 for government help, $1,800 for additional security licenses, $1.25 million for a redesign of its network, and $125,000 for a new security position (Lacy, 2017). Ingham County's 2017 budget was $234 million, with the total incident cost making up 0.626% of the budget (Ingham County Controller's Office, 2016).

Georgia – 2015 Breach – Torres (2015)

A Georgia data leak of 6 million voter information records resulted in $1.2 million spent on credit monitoring and identity theft protection (Torres, 2015). Georgia's general fund in 2015 was $19.73 billion (State of Georgia, 2014). This brings cost of the incident to 0.006% of the total revenue.

Wisconsin Department of Revenue – 2012 Breach - Levin (2012)

In 2012 Wisconsin Department of Revenue accidentally made public 110,795 Social Security numbers and tax ID numbers of Wisconsin residents, which were mistakenly embedded in a real estate report and posted to the department's website for almost 3 months before being removed. The state was estimated to spend at least $1 million on credit monitoring for victims (Levin, 2012). The FY 2012–13 state budget was approximately $66 billion, with the breach costing less than 0.002% of the annual budget (*Wisconsin State Budget*, 2013).

Allentown, Pennsylvania – 2018 Breach - Blake (2018)

In 2018, Allentown, Pennsylvania suffered a breach of an unknown number of records, resulting in $1 million in total costs (Blake, 2018). Allentown's 2018 operating budget was $108.4 million, making the cost of this breach 0.92% of the 2018 budget (Althouse, 2017; City of Allentown, 2017).

Orange County Transportation Authority - 2016 Incident - Gerda (2016)

A 2016 ransomware attack on the Orange County Transportation Authority systems affected 88 servers, but no records were breached. The total cost of the attack was $660,000, including $330,000 for labor and $218,000 for emergency contracts with Microsoft and CISO Share (Gerda, 2016). Orange County's 2016–2017 operating budget was $6.07 billion, making this total attack cost less than 0.01% of the budget (County of Orange, 2016).

City of Fort Lauderdale, Florida – 2014 Incident - Barszewski (2015)

The City of Fort Lauderdale, Florida suffered a cyberattack by the group Anonymous that resulted in $430,294 in total costs. Of which, $366,989 was spent on security consulting, $45,398 was spent on software licenses to manage computer activities, and $17,907 was spent for new hardware (Barszewski, 2015). No records were breached. Fort Lauderdale's 2014 adopted budget was approximately $550 million, and the total incident cost was 0.08% of this budget (City of Fort Lauderdale, 2013).

Ferris State University – 2013 Breach - McVicar (2013)

A data breach occurred at Ferris State University that disclosed 62,000 records. The university spent $380,925 on forensics, legal fees, notifications, a call center, consulting, and credit monitoring (McVicar, 2013). All but $21,398 of the total cost was covered by insurance (McVicar, 2013). The university's operating budget was $283 million (Eisler, 2013), making the breach cost 0.13% of the total budget.

Madison County of Indiana – 2016 Incident - Ragan (2016)

In 2016, Madison County of Indiana experienced an incident affecting 600 computers and 75 servers in a ransomware attack. The total cost to recover from the attack was $236,680 with $17,500 spent on incident response, $198,180 spent on third-party contracts, and $21,000 paid in ransom (Ragan, 2016). The 2016 operating budget for Madison County was $28.4 million (de la Bastide, 2015), making the cost of this incident 0.83% of the budget.

Cuesta College – 2015 Breach - Lambert (2015)

Cuesta College suffered a breach of an undisclosed number of records, resulting in $156,000 spent on identity protection (Lambert, 2015). Cuesta College's operating budget for 2015 was $46.6 million (San Luis Obispo County Community College District, 2013). The identity protection cost is 0.34% of the annual budget.

University of California, Berkeley – 2014 Breach - Schaffhauser (2014)

The University of California, Berkeley breach of 1,600 records resulted in $150,000 spent on credit monitoring and consulting (Schaffhauser, 2014). The university's 2014 operating budget was $2.35 billion (UC Berkeley, 2013), making this breach 0.006% of the budget.

University of Central Florida – 2016 Breach - Russon (2016)

A 2016 data breach of 63,000 records at the University of Central Florida resulted in a total cost of $109,364, including $64,388 to run a call center ($550 for call center set up), $28,335 in postage, $15,246 in printing services, $345 to find changes of address across the county, and $325-per-hour Verizon consulting to clean up the breach (Russon, 2016). The total breach cost was covered by insurance (Russon, 2016). The breach cost was 0.007% of the university's 2016 operating budget of $1.56 billion (University of Central Florida, 2015).

Anderson County, Tennessee – 2016 Breach - Huotari (2016)

1,800 people were impacted by a breach of Anderson County's (of Tennessee's) systems. The total cost of the breach was $100,000, including $28,000 on information technology services, $48,000 on hardware upgrades, and $7,000 on an emergency incident response contract (Huotari, 2016). The total general fund (operating budget) for Anderson County in 2016 was $26.3 million (Anderson County Government, 2018). This cost of this breach was 0.38% of the operating budget.

Table 46: Summary of Itemized Costs for Smaller Government Incidents, $ Thousands

Affected Entity	1	2	3	4	5	6
Source	Rubin & Belkin (2017)	Faller (2014)	Shain (2012)	Associated Press (2013)	Book et al. (2010)	Brinkmann (2017)
Info Type	Tax Returns	PII, Financial	PII, PCI	PII	PII	PCI
Number of Records (thousands)	100	2,000	3,600	780	760	N/A
Total Cost ($ thousands)	$30,000	$26,019.436	$14,125	$9,000	$4,000	$2,383.830
Incident Investigation & Forensic Analysis	-	-	-	-	-	-
Incident Response, & Containment (direct response, cleanup, and recovery costs):	-	-	-	-	-	-
Patching & Updates	-	-	-	-	-	-
Cleanup/Removal of Artifacts	-	-	-	-	-	-
Network Countermeasures & Reconfiguration	-	-	-	-	-	-
Network Mitigation	-	-	-	-	-	-
Installation of Additional Authentication & Security Solutions	-	-	-	-	-	-
Other IT & Cyber Services to Clean Up the Incident	-	-	-	-	-	-
Data Management to Upgrade Privacy Policy Changes	-	-	-	-	-	-
Data Restoration from Backup	-	-	-	-	-	-
Documentation & Reporting	-	-	-	-	-	-
Other Contracted Third-Party Services for Incident Response & Recovery Including Staff Augmentation	-	$7,500	$125	-	-	-
Hardware Upgrade or Replacement	-	-		$4,400	-	-
Software Upgrade or Replacement	-	-	-	-	-	-
Incident-Induced Staff Hiring	-	-	-	-	-	-
Incident-Induced Additional Training (staff time & acquisitions for development and implementation)	-	-	-	-	-	-
Management, General Council, Public Affairs, etc.	-	$2,200	-	-	-	$15
Cost of PR Campaign or Crisis Management Services	-	-	-	$467	-	-
Lost Revenue or Productivity:	-	-	-	-	-	-
Business Interruption/ Downtime	-	-	-	-	-	-
Lost Transactions/Sales/ Revenue	-	-	-	-	-	-
Other Mission Disruptions _____	-	-	-	-	-	-

Source	Rubin & Belkin (2017)	Faller (2014)	Shain (2012)	Associated Press (2013)	Book et al. (2010)	Brinkmann (2017)
Theft/Fraud/Direct Financial Loss:	-	-	-	-	-	-
Financial Theft & Fraud	$30,000	-	-	-	-	-
Extortion Demands & Costs	-	-	-	-	-	-
Credit Card & Account Losses	-	-	-	-	-	-
Other _____	-	-	-	-	-	-
Legal Fees & Regulatory Fines:	-	$9,300	-	-	-	-
Legal Fees/Individual Litigation/Class Action	-	-	-	-	-	-
Attorney Fees	-	-	-	-	-	$50
Liability Claims/Restitution	-	-	-	-	-	$2,128.830
Regulatory Fines, Fees, & Assessments	-	-	-	-	-	-
Additional Reserve Requirements	-	-	-	-	-	-
Other Fees & Fines	-	-	-	-	-	-
Victim Notification & Protection Services:	-	$7,000	-	-	-	$40
Victim Notification	-	-	-	-	-	-
Credit Monitoring & Identity Theft Protection/Repair	-	$3,000	$12,000	$1,900	-	-
Other Third-Party Services	-	-	$2,000	-	-	-
Reserve Fund Requirement	-	-	-	-	-	-
Other Losses:	-	-	-	-	-	-
Loss of IP	-	-	-	-	-	-
Loss of System Functionality	-	-	-	-	-	-
Loss of PII, PHI, etc.	-	-	-	-	-	-
Physical Asset Damage	-	-	-	-	-	-
Bodily Injury	-	-	-	-	-	-
Loss of Life	-	-	-	-	-	-
Environmental Damage	-	-	-	-	-	-
Other _____	-	-	-	-	-	

Note. IT = information technology; PR = public relations; IP = intellectual property; PII = personally identifiable information; PHI = personal health information.

Affected Entity (Cont'd)	7	8	9	10	11	12
Source	Lacy (2017)	Blake (2018)	Gerda (2016)	Barszewski (2015)	McVicar (2013)	Ragan (2016)
Info Type	County Systems	PII	PII, Financial	N/A	PII	County Systems
Number of Records Breached (thousands)	1.6 computers	N/A	0.088 servers	N/A	62	
Total Cost ($ thousands)	$1,463.295	$1,000	$660	$430.294	$380.925	$236.68
Incident Investigation & Forensic Analysis	-	-	-	-	-	-
Incident Response & Containment (direct response, cleanup, & recovery costs):	-	-	-	-	-	$198.18
Patching & Updates	-	-	-	-	-	-
Cleanup/Removal of Artifacts		-	-	-	-	-
Network Countermeasures & Reconfiguration	$1,250	-	-	-	-	-
Network Mitigation	-	-	-	-	-	-
Installation of Additional Authentication & Security Solutions	-	-	-	-	-	-
Other IT & Cyber Services to Clean Up the Incident	$66.495	-	$330	-	-	-
Data Management to Upgrade Privacy Policy	-	-	-	-	-	-
Data Restoration from Backup	-	-	-	-	-	-
Documentation & Reporting	-	-	-	-	-	-
Other Contracted Third-Party Services for Incident Response & Recovery Including Staff Augmentation	$20	-	$218	$366.989	-	$17.5
Hardware Upgrade or Replacement	-	-	-	$17.907	-	-
Software Upgrade or Replacement	$1.8	-	-	$45.398	-	-
Incident-Induced Staff Hiring	$125	-	-	-	-	-
Incident-Induced Additional Training (staff time and acquisitions for development and implementation)	-	-	-	-	-	-
Management, General Council, Public Affairs, etc.	-	-	-	-	-	-
Cost of PR campaign or Crisis Management	-	-	-	-	-	-
Lost Revenue or Productivity:	-	-	-	-	-	-
Business Interruption/Downtime	-	-	-	-	-	-
Lost Transactions/Sales/Revenue	-	-	-	-	-	-
Other Mission Disruptions _____	-	-	-	-	-	-
Theft/Fraud/Direct Financial Loss:	-	-	-	-	-	-
Financial Theft & Fraud	-	-	-	-	-	-
Extortion Demands & Costs	-	-	-	-	-	$21
Credit Card & Account Losses	-	-	-	-	-	-

Source	Lacy (2017)	Blake (2018)	Gerda (2016)	Barszewski (2015)	McVicar (2013)	Ragan (2016)
Other _____	-	-	-	-	-	-
Legal Fees and Regulatory Fines:	-	-	-	-	-	-
Legal Fees/Individual Litigation/Class Action	-	-	-	-	-	-
Attorney Fees	-	-	-	-	-	-
Liability Claims/Restitution	-	-	-	-	-	-
Regulatory Fines, Fees, & Assessments	-	-	-	-	-	-
Additional Reserve Requirements	-	-	-	-	-	-
Other Fees & Fines _____	-	-	-	-	-	-
Victim Notification & Protection Services:	-	-	-	-	-	-
Victim Notification	-	-	-	-	-	-
Credit Monitoring & Identity Theft Protection/Repair	-	-	-	-	-	-
Other Third-Party Services	-	-	-	-	-	-
Reserve Fund Requirement	-	-	-	-	-	-
Other Losses:	-	-	-	-	-	-
Loss of IP	-	-	-	-	-	-
Loss of System Functionality	-	-	-	-	-	-
Loss of PII, PHI, etc.	-	-	-	-	-	-
Physical Asset Damage	-	-	-	-	-	-
Bodily Injury	-	-	-	-	-	-
Loss of Life	-	-	-	-	-	-
Environmental Damage	-	-	-	-	-	-
Other _____	-	-	-	-	-	-

Note. IT = information technology; PR = public relations; IP = intellectual property; PII = personally identifiable information; PHI = personal health information.

Affected Entity (Cont'd)	13	14	15	16	17	18
Source	Schaffhauser (2014)	Russon (2016)	Huotari (2016)	Weidmayer (2016)	Lambert (2015)	Torres (2015)
Info Type	PII, PCI	PII	PII, PHI, Banking	PII	PII	PII
Number of Records (thousands)	1.6	63	1.8	400	N/A	6,000
Total Cost ($ thousands)	$150	$109.364	$100	$9,400	$156	$1,200
Incident Investigation & Forensic Analysis	-	-	-	-	-	-
Incident Response & Containment (direct response, cleanup, & recovery costs):	-	-	-	-	-	-
Patching & Updates	-	-	-	-	-	-
Cleanup/Removal of Artifacts	-	-	-	-	-	-
Network Countermeasures & Reconfiguration	-	-	-	-	-	-
Network Mitigation	-	-	-	-	-	-
Installation of Additional Authentication & Security Solutions	-	-	-	-	-	-
Other IT & Cyber Services to Clean Up the Incident	-	-	$28	-	-	-
Data Management to Upgrade Privacy Policy Changes	-	-	-	-	-	-
Data Restoration from Backup	-	-	-	-	-	-
Documentation and Reporting	-	-	-	-	-	-
Other Contracted Third-Party Services for Incident Response & Recovery Including Staff Augmentation	-	-	$7	-	-	-
Hardware Upgrade or Replacement	-	-	$48	-	-	-
Software Upgrade or Replacement	-	-	-	-	-	-
Incident-Induced Staff Hiring	-	-	-	-	-	-
Incident-Induced Additional Training (staff time and acquisitions for development & implementation)	-	-	-	-	-	-
Management, General Council, Public Affairs, etc.	-	-	-	-	-	-
Cost of PR campaign or Crisis Management Services	-	-	-	-	-	-
Lost Revenue or Productivity:	-	-	-	-	-	-
Business Interruption/Downtime	-	-	-	-	-	-
Lost Transactions/Sales/Revenue	-	-	-	-	-	-
Other Mission Disruptions _____	-	-	-	-	-	-
Theft/Fraud/Direct Financial Loss:	-	-	-	-	-	-
Financial Theft & Fraud	-	-	-	-	-	-
Extortion Demands and Costs	-	-	-	-	-	-

Source	Schaffhauser (2014)	Russon (2016)	Huotari (2016)	Weidmayer (2016)	Lambert (2015)	Torres (2015)
Credit Card and Account Losses	-	-	-	-	-	-
Other _____	-	-	-	-	-	-
Legal Fees and Regulatory Fines:	-	-	-	-	-	-
Legal Fees/Individual Litigation/Class Action	-	-	-	-	-	-
Attorney Fees	-	-	-	-	-	-
Liability Claims/Restitution	-	-	-	-	-	-
Regulatory Fines, Fees, & Assessments	-	-	-	-	-	-
Additional Reserve Requirements	-	-	-	-	-	-
Other Fees & Fines _____	-	-	-	-	-	-
Victim Notification & Protection Services:	-	-	-	-	-	-
Victim Notification	-	$44.426	-	-	-	-
Credit Monitoring & Identity Theft Protection/Repair	-	-	-	$2,900	$156	$1,200
Other Third-Party Services	-	$64.938	-	-	-	-
Reserve Fund Requirement	-	-	-	$6,500	-	-
Other Losses:	-	-	-	-	-	-
Loss of IP	-	-	-	-	-	-
Loss of System Functionality	-	-	-	-	-	-
Loss of PII, PHI, etc.	-	-	-	-	-	-
Physical Asset Damage	-	-	-	-	-	-
Bodily Injury	-	-	-	-	-	-
Loss of Life	-	-	-	-	-	-
Environmental Damage	-	-	-	-	-	-
Other _____	-	-	-	-	-	-

Note. IT = information technology; PR = public relations; IP = intellectual property; PII = personally identifiable information; PHI = personal health information.

Affected Entity (Cont'd)	19	20	21
Source	CT Department of Banking (2009)	Gallagher (2017)	Levin (2012)
Info Type	PII	PII	PII
Number of Records (thousands)	640.994	1,270	171
Total Cost ($ thousands)	$3,630	$5,500	$1,000
Incident Investigation & Forensic Analysis	-	-	
Incident Response & Containment (direct response, cleanup, & recovery costs):	-	-	-
Patching & Updates	-	-	-
Cleanup/Removal of Artifacts	-	-	-
Network Countermeasures & Reconfiguration	-	-	-
Network Mitigation	-	-	-
Installation of Additional Authentication & Security Solutions	-	-	-
Other IT & Cyber Services to Clean Up the Incident	-	-	-
Data Management to Upgrade Privacy Policy Changes	-	-	-
Data Restoration from Backup	-	-	-
Documentation and Reporting	-	-	-
Other Contracted Third-Party Services for Incident Response & Recovery Including Staff Augmentation	-	-	-
Hardware Upgrade or Replacement	-	-	-
Software Upgrade or Replacement	-	-	-
Incident-induced Staff Hiring	-	-	-
Incident-induced Additional Training (staff time and acquisitions for development & implementation)	-	-	-
Management, General Council, Public Affairs, etc.	-	-	-
Cost of PR campaign or Crisis Management Services	-	-	-
Lost Revenue or Productivity:	-	-	-
Business Interruption/Downtime	-	-	-
Lost Transactions/Sales/Revenue	-	-	-
Other Mission Disruptions _____	-	-	-
Theft/Fraud/Direct Financial Loss:	-	-	-

Source	CT Department of Banking (2009)	Gallagher (2017)	Levin (2012)
Financial Theft & Fraud	-	-	-
Extortion Demands & Costs	-	-	-
Credit Card & Account Losses	-	-	-
Other _____	-	-	-
Legal Fees & Regulatory Fines:	-	-	-
Legal Fees/Individual Litigation/Class Action	-	$5,500	-
Attorney Fees	-	-	-
Liability Claims/Restitution	-	-	-
Regulatory Fines, Fees, & Assessments	-	-	-
Additional Reserve Requirements	-	-	-
Other Fees & Fines _____	$150	-	-
Victim Notification & Protection Services:	-	-	-
Victim Notification	-	-	-
Credit Monitoring & Identity Theft Protection/Repair	$3,480	-	-
Other Third-Party Services	-	-	$1,000
Reserve Fund Requirement	-	-	-
Other Losses:	-	-	-
Loss of IP	-	-	-
Loss of System Functionality	-	-	-
Loss of PII, PHI, etc.	-	-	-
Physical Asset Damage	-	-	-
Bodily Injury	-	-	-
Loss of Life	-	-	-
Environmental Damage	-	-	-
Other _____	-	-	-
			-

Note. IT = information technology; PR = public relations; IP = intellectual property; PII = personally identifiable information; PHI = personal health information.

REFERENCES

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 1563–1580. https://aisel.aisnet.org/icis2006/94/

Advisen. (2015). *Cyber risk data methodology for insurance & risk analysis*. https://in.advisenltd.com/cyber-risk-data-methodology/

AFP. (2017, November 10). *Massive data breach has cost Equifax nearly $90 million*. DailyMail.com. http://www.dailymail.co.uk/wires/afp/article-5071923/Massive-data-breach-cost-Equifax-nearly-90-million.html

Allison, D. (2015, December 3). Home Depot reaches settlement over data breach. *Dayton Business Journal.* https://www.bizjournals.com/dayton/blog/morning_call/2015/12/home-depot-reaches-settlement-data-breach.html

Althouse, S. (2017, November 3). *First Allentown budget meeting of 2018 a quiet affair*. WFMZ. http://www.wfmz.com/news/lehigh-valley/2018-general-budget-meeting-generally-irrelevant-in-allentown/651187128

A.M. Best (2018, October). Special report focuses on cyber insurance. *Best's Review*, *10*, 76–77. http://news.ambest.com/articlecontent.aspx?pc=1009&AltSrc=108&refnum=278309

Anderson, R. (2001). Why information security is hard - an economic perspective. *Proceedings: 17th Annual Computer Security Applications Conference*. 358–365. https://doi.org/10.1109/ACSAC.2001.991552

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2012, June 25–26). *Measuring the cost of cybercrime* [Paper presentation]. 11th Annual Workshop on the Economics of Information Security, Berlin, Germany. https://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf

Anderson, R., Barton, C., Böhme, R., Clayton, R., Gañán, C., Grasso, T., Levi, M., Moore, T., & Vasek, M. (2019, June 3–4). *Measuring the changing cost of cybercrime* [Paper presentation]. The 2019 Workshop on the Economics of Information Security, Boston, MA, United States. https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_25.pdf

Anderson, R., & Moore, T. (2006, October). The economics of information security. *Science*, *314* (5799). 610–613. https://science.sciencemag.org/content/sci/314/5799/610.full.pdf

Anderson County Government. (2018). *Anderson County Government FY 2018/2019: Annual Budget Document*. http://www.anderson-county.com/wp-content/uploads/2018/07/Annual-Budget-Document-FY-2018-2019.pdf

Andriotis, A. (2017, November 10). Equifax apologizes for security breach as it reports earnings drop; CEO discusses efforts to keep clients from taking business elsewhere. *Wall Street Journal (Online).* https://search.proquest.com/docview/1962320214?accountid=31567

Anthem, Inc. (2016, January 27). *Anthem reports fourth quarter and full year 2015 results* [Press release]. Business Wire. https://www.businesswire.com/news/home/20160127005299/en/Anthem-Reports-Fourth-Quarter-Full-Year-2015

Anthem, Inc. (2016). *2015 Annual Report*. https://ir.antheminc.com/static-files/c5f53cca-6940-46e2-bcae-8cff5b7b70c7

Armerding, T. (2017, May 25). *Cybersecurity ROI: Still a tough sell*. CSO Online. https://www.csoonline.com/article/3198458/cyber-attacks-espionage/cybersecurity-roi-still-a-tough-sell.html

Armerding, T. (2018a, January). *The 17 biggest data breaches of the 21st century*. CSO Online. Retrieved July, 2019, from https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

Armerding, T. (2018b, December). *The 18 biggest data breaches of the 21st century*. CSO Online. Retrieved July, 2019, from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Asbury, K. (2014, July 23). *Sony agrees to $15M settlement in data breach class action; $2.75M for attorneys*. Washington Examiner. https://www.washingtonexaminer.com/sony-agrees-to-15m-settlement-in-data-breach-class-action-275m-for-attorneys

Associated Press. (2013, May 1). *Study: Utah health breach could approach $406M*. Insurance Journal. https://www.insurancejournal.com/news/west/2013/05/01/290357.htm

Baker Hostetler. (2017). *Data Security Incident Response Report*. https://www.databreaches.net/bakerhostetler-2017-data-security-incident-response-report-based-on-450-incidents/

Baker Hostetler. (2018). *Data Security Incident Response Report*. https://www.dataprivacymonitor.com/data-security-incident-response/fourth-annual-data-security-incident-response-report-released-building-cyber-resilience/

Baker Hostetler. (2019). *Data Security Incident Response Report*. https://f.datasrvr.com/fr1/019/33725/2019_BakerHostetler_DSIR_Final.pdf

Baker Hostetler. (2020). *Data Security Incident Response Report*. https://f.datasrvr.com/fr1/620/24943/2020_DSIR_Report_(003).pdf

Bank of America Merrill Lynch. (2015, September 3). *Thematic investing: You've been hacked! - Global cybersecurity primer*. https://www.longfinance.net/media/documents/BAML_2015_Youve_been_hacked_-_Global_Cybersecurity_Primer.pdf

The Bank of New York Mellon Corporation. (2008). *2008 Annual Report*. https://www.bnymellon.com/_global-assets/pdf/investor-relations/annual-report-2008.pdf

Barszewski, L. (2015, January 19). Lauderdale spends $430,000 on computer security after Anonymous attack. *Sun Sentinel.* http://www.sun-sentinel.com/local/broward/fort-lauderdale/fl-lauderdale-anonymous-threat-cost-20150119-story.html

Beek, C., Bulygin, Y., Frosst, D., Greve, P., Jarvis, J., Peterson, E., Rosenquist, M., Ruiz, F., Schmugar, C., Simon, R., Snell, B., Sommer, D., Sun, B., & Wosotowsky, A. (2016, November). *McAfee Labs 2017 Threats Predictions*. McAfee Labs. https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf

Bermuda:Re+ILS. (2018, December 7). *Cyber: Still small for its age*. Bermuda Insurance Magazine. https://www.bermudareinsurancemagazine.com/contributed-article/cyber-still-small-for-its-age

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk & Insurance, 40*(1): 131–158. https://doi.org/10.1057/gpp.2014.19

Bisogni, F., Asghari, H., & Van Eeten, M. J. G. (2017, June 26–27). *Estimating the size of the iceberg from its tip: An investigation into unreported data breach notifications* [Paper presentation]. 16th Annual Workshop on the Economics of Information Security, La Jolla, CA, United States. https://weis2017.econinfosec.org/wp-content/uploads/sites/3/2017/05/WEIS_2017_paper_54.pdf

Bisogni, F., Cavallini, S., & di Trocchio, S. (2011). Cybersecurity at European level: The role of information availability. *Communications & Strategies*, (81), 105–124. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2021825

Bissell, K., LaSalle, R., & Cin, P. D. (2019). *The cost of cybercrime. Ninth annual Cost of Cybercrime Study: Unlocking the value of improved cybersecurity protection.* Independently conducted by Ponemon Institute LLC and jointly developed by Accenture. https://www.accenture.com/t20190305T185301Z__w__/us-en/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

Blake, A. (2015, August 25). Ashley Madison hack could cost dating site more than $1 billion as lawsuits mount. *The Washington Times*. https://www.washingtontimes.com/news/2015/aug/25/ashley-madison-hack-could-cost-dating-site-more-1-/

Blake, A. (2018, February 21). Malware infection poised to cost $1 million to Allentown, Pa.: Mayor. *The Washington Times*. https://www.washingtontimes.com/news/2018/feb/21/malware-infection-posed-cost-1-million-allentown-p/

Blatnik, J. (2017, May 25). *The impact of WannaCry on the ransomware conversation*. SecurityWeek. https://www.securityweek.com/impact-wannacry-ransomware-conversation

Bloomberg News. (2017, September 9). Equifax's insurance said likely to be inadequate against breach costs. *The Denver Post.* https://www.denverpost.com/2017/09/09/equifaxs-insurance-said-likely-to-be-inadequate-against-breach/

Blosfield, E. (2020, August 12). *Cyber lessons for the insurance industry continue three years after NotPetya*. Insurance Journal. https://www.insurancejournal.com/news/national/2020/08/12/578788.htm

Book, R., Jurich, J., & Marotti, A. (2010, December 14). *Hacked: Data breach costly for Ohio State, victims of compromised info*. The Lantern. https://www.thelantern.com/2010/12/hacked-data-breach-costly-for-ohio-state-victims-of-compromised-info/

Brinkmann, P. (2017, March 29). American Express, Mastercard, Visa fine Rosen Hotels in data breach, lawsuit says. *Orlando Sentinel.* http://www.orlandosentinel.com/business/brinkmann-on-business/os-rosen-hotels-data-breach-20170329-story.html

Bureau of Economic Analysis. (2020). National Income and Product Accounts. Table 1.1.5. Gross Domestic Product. Retrieved July 10, 2020, from https://apps.bea.gov/iTable/iTable.cfm?reqid=19&step=3&isuri=1&select_all_years=0&nipa_table_list=5&series=a&first_year=2017&scale=-9&last_year=2019&categories=survey&thetable=x

Cambridge Centre for Risk Studies. (2016, January). *Cyber Insurance Exposure Data Schema v1.0*. Cyber Policy Magazine. https://cyberpolicymagazine.com/images/pdf-downloads/rms_cyber_exposure_data_schema_jan2016.pdf

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431–448. https://doi.org/10.3233/JCS-2003-11308

Chinn, D., Kaplan, J., & Weinberg, A. (2014, January). *Risk and responsibility in a hyperconnected world*. World Economic Forum in collaboration with McKinsey & Company. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/risk%20and%20responsibility%20in%20a%20hyperconnected%20world%20implications%20for%20enterprises/risk%20and%20responsibility%20in%20a%20hyperconnected%20world.ashx

Cisco. (2017). *Cisco 2017 Annual Cybersecurity Report*. https://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf

Cisco. (2018a). *Cisco 2018 Annual Cybersecurity Report*. https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

Cisco. (2018b). *Small and mighty: How small and midmarket businesses can fortify their defenses against today's threats* [Cisco Cybersecurity Special Report]. https://www.cisco.com/c/dam/global/en_hk/products/security/security-reports/Cisco_2018_SMB_Final.pdf?oid=wprsc013702

Cisco. (2019). *Anticipating the unknowns: Chief information security officer (CISO) benchmark study*. https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/1963786/2019CISOBenchmarkReportCiscoCybersecuritySeries.pdf?ccid=cc000160&dtid=oemzzz000233&ecid=14396&oid=wprsc015512

Cisco. (2020a). *Securing what's now and what's next: 20 cybersecurity considerations for 2020*. https://ebooks.cisco.com/story/2020-ciso-benchmark/

Cisco. (2020b). *Big security in a small business world: 10 myth busters for SMB cybersecurity.* https://www.cisco.com/c/en/us/products/security/smb-report-2020.html

City of Allentown. (2017). *2018 Final City Budget*. https://www.allentownpa.gov/Government/City-Budget

City of Fort Lauderdale. (2013). *FY 2014 Adopted Budget*. http://www.fortlauderdale.gov/home/showdocument?id=4555

Clayton, R. (2011). Might governments clean-up malware? *Communications & Strategies*, (81), 87–104. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2020273

Coburn, A., Leverett, E., & Woo, G. (2018). *Solving cyber risk: Protecting your company and society*. John Wiley & Sons, Incorporated.

Colón, M. (2012a, August 3). *Data breach costs LinkedIn up to $1 million*. SC Magazine. https://www.scmagazine.com/data-breach-costs-linkedin-up-to-1-million/article/543380/

Colón, M. (2012b, August 6). *Data breach costs LinkedIn up to $1 million*. iTnews. https://www.itnews.com.au/news/data-breach-costs-linkedin-up-to-1-million-310976

Cost of a retail data breach: $179 million for Home Depot. (2017, March 14). *WebTitan*. https://www.webtitan.com/blog/cost-retail-data-breach-179-million-home-depot/

The Council of Economic Advisors. (2018, February). *The cost of malicious cyber activity to the U.S. economy*. https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

County of Orange (2016). *FY 2016-2017 Annual Budget*. http://bos.ocgov.com/finance/2017FN/charts_frm.htm

Crecente, B. (2014, July 24). *Sony: We settled PSN hack suit to avoid trial costs, but 'continue to deny the allegations.'* Polygon. https://www.polygon.com/2014/7/24/5933569/sony-we-settled-psn-hack-suit-to-avoid-trial-costs-but-continue-to

Cybersecurity Ventures. (2016). *Cybersecurity Ventures 2016 Cybercrime Report – Hackerpocalypse: A cybercrime revelation*. Cyber Defense Magazine. http://www.cyberdefensemagazine.com/cybersecurity-ventures-2016-cybercrime-report-hackerpocalypse-a-cybercrime-revelation/

Cybersecurity Ventures. (2017). *2017 Cybercrime Report*. https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Cybersecurity Ventures. (2018). *2018 Cybersecurity Market Report*. https://cybersecurityventures.com/cybersecurity-market-report/

Cybersecurity Ventures. (2019). *2019 Official Annual Cybercrime Report*. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Cyentia Institute. (2020). *2020 Information Risk Insights Study*. https://www.cyentia.com/wp-content/uploads/IRIS2020_cyentia.pdf

Davis, J. (2017, October 27). *Petya cyberattack cost Merck $135 million in revenue*. Healthcare Finance. https://www.healthcarefinancenews.com/news/petya-cyberattack-cost-merck-135-million-revenue

Dean, B. (2015, March 4). *Why companies have little incentive to invest in cybersecurity*. The Conversation. http://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570

de la Bastide, K. (2015, October 13). Madison County Council adopts 2016 budget. *10.1093/cybsec/tyw003*. http://www.heraldbulletin.com/news/madison-county-council-adopts-budget/article_e77f111c-7208-11e5-a41b-831d6d35cbda.html

Deloitte. (2016). *Beneath the surface of a cyberattack. A deeper look at business impacts*. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf

Dignan, L. (2017, November 9). *Equifax spends $87.5 million on data breach, more expenses on deck*. ZDNet. http://www.zdnet.com/article/equifax-spends-87-5-million-on-data-breach-more-expenses-on-deck/

Donaldson, S. (2017, May 19). WannaCry ransomware: Who it affected and why it matters. *Red Hat Developer*. https://developers.redhat.com/blog/2017/05/19/wannacry-ransomware-who-it-affected-and-why-it-matters/

Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J. W., & Winkelman, Z. (2018). *Estimating the global cost of cyber risk: Methodology and examples*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR2299.html

Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity, 2*(1), 3–14. https://doi.org/10.1093/cybsec/tyw003

Eilifsen, A., & Messier, W. F., Jr. (2015). Materiality guidance of the major public accounting firms. *Auditing: A Journal of Practice & Theory*, *34*(2), 3–26. http://doi.org/10.2308/ajpt-50882

Eisler, D. L. (2013, October). *Fall Budget Forum: 2013 fiscal results, 2014 budget, performance funding, enrollment, and future prospects*. https://ferris.edu/HTMLS/administration/president/budget-pres/forums/docs/Fall_Budget_Forum_2013_with_comments.pdf

Equifax. (2018). *Equifax 2017 Annual Report*. https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual%20Reports/2017-annual-report.pdf

Ernst & Young. (2014, November 19). *Cyber-economic risk insights. Executive summary*. Defense One Summit 2014: Defining the U.S. Military's purpose in the new global security architecture. https://www.defenseone.com/feature/defense-one-summit/

Experian. (2016, May 11). *Preliminary results for the year ended 31 March 2016* [News release]. https://www.experianplc.com/media/2715/experian-full-year-results-fy16.pdf

Experian Data Breach Resolution. (2017). *Fourth annual 2017 Data Breach Industry Forecast*. Experian. https://www.experian.com/assets/data-breach/white-papers/2017-experian-data-breach-industry-forecast.pdf

Ezell, B. C., Bennett, S. P., von Winterfeldt, D., Sokolowski, J., & Collins, A. J. (2010). Probabilistic risk analysis and terrorism risk. *Risk Analysis*, *30*(4), 575–589. https://doi.org/10.1111/j.1539-6924.2010.01401.x

Faller, M. B. (2014, December 17). Maricopa County colleges computer hack cost tops $26M. *The Republic.* https://www.azcentral.com/story/news/local/phoenix/2014/12/17/costs-repair-massive-mcccd-computer-hack-top-million/20539491/

Fanelli, B., Pessanha, R., Gwiazdowski, A., Chng-Castor, A., & Auger, G. (2017). *2017 state of cybersecurity among small businesses in North America*. Council of Better Business Bureaus. https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf

Fanelli, B., Pessanha, R., Gwiazdowski, A., & Scott, T. (2016). *The state of cybersecurity among small businesses in North America*. Council of Better Business Bureaus. https://www.bbb.org/globalassets/local-bbbs/fort-wayne-in-52/media/documents/state-of-cybersecurity-among-small-businesses.pdf

Farrow, S., & Szanton, J. (2016). Cybersecurity investment guidance: Extensions of the Gordon and Loeb Model. *Journal of Information Security, 7*(2), 15–28. https://doi.org/10.4236/jis.2016.72002

Fazzini, K. (2019, May 22). *Equifax just became the first company to have its outlook downgraded for a cyber attack*. CNBC. https://www.cnbc.com/2019/05/22/moodys-downgrades-equifax-outlook-to-negative-cites-cybersecurity.html

Federal Bureau of Investigation. (2016, December 15). *Business e-mail compromise scheme fraud alert*. FBI Cincinnati Division. https://www.fbi.gov/contact-us/field-offices/cincinnati/news/press-releases/business-e-mail-compromise-scheme-fraud-alert

Federal Bureau of Investigation. (2017, May 4). *Business e-mail compromise: E-mail account compromise: The 5 billion dollar scam* (Alert Number I-050417-PSA). https://www.ic3.gov/media/2017/170504.aspx

Federal Bureau of Investigation. (2018, July 12). *Business e-mail compromise the 12 billion dollar scam* (Alert Number I-071218-PSA). https://www.ic3.gov/media/2018/180712.aspx

Federal Energy Regulatory Commission. (2017, December 21). *FERC proposes to require expanded cyber security incident reporting* [News release]. https://www.ferc.gov/media/news-releases/2017/2017-4/12-21-17-E-1.asp#.XK5Hmjbsakz

Financial Accounting Standards Board. (1980, May). *Statement of Financial Accounting Concepts No. 2: Qualitative Characteristics of Accounting Information*. https://www.fasb.org/jsp/FASB/Document_C/DocumentPage?cid=1218220132599&acceptedDisclaimer=true

Fleming, M., Jr. (2014, November 25). *Sony hacker paralysis reaches day two – Update*. Deadline Hollywood. https://deadline.com/2014/11/sony-computers-hacked-skull-message-1201295288/

Fontana, J. (2012, August 3). *Breach clean-up cost LinkedIn nearly $1 million, another $2-3 million in upgrades*. ZDNet. http://www.zdnet.com/article/breach-clean-up-cost-linkedin-nearly-1-million-another-2-3-million-in-upgrades/

Franceschi-Bicchierai, L. (2016, December 25). *The worst hacks of 2016*. VICE Motherboard. https://motherboard.vice.com/en_us/article/wnxkz9/the-worst-hacks-of-2016

Frater, P. (2016, April 27). *Sony returns to profit as motion pictures drops 34 percent*. Variety. http://variety.com/2016/biz/asia/sony-returns-to-profit-as-motion-pictures-drops-1201762488/

Freeman, L. (2017, June 27). *Anthem reaches settlement in massive 2015 security breach*. The News Press. https://search.proquest.com/docview/1913586726?accountid=31567

Freund, J. (2020, August 25–27). *Engineering economic externalities: Methods for determining material cyber security fines*. [Video]. SIRAcon 2020. https://www.societyinforisk.org/Blog-Posts/8654352

Friedman, A. A. (2013, September). *Cyber theft of competitive data: Asking the right questions*. Center for Technology Innovation at Brookings. https://www.brookings.edu/wp-content/uploads/2016/07/BrookingsCyberTech92513.pdf

Friedman, A. A., Mack-Crane, A., & Hammond, R. A. (2013, December). *Cyber-enabled competitive data theft: A framework for modeling long-run cybersecurity consequences*. Center for Technology Innovation at Brookings. https://www.brookings.edu/wp-content/uploads/2016/06/Cyberenabled-Theft-of-Competitive-Data_revised.pdf

Frizell, S. (2015, February 4). Sony is spending $15 million to deal with the big hack. *Time.* http://time.com/3695118/sony-hack-the-interview-costs/

Gallagher, O. (2017, August 14). *Nationwide Insurance pays Mass. $100,000 as part of multistate data-breach settlement*. Agency Checklists: Massachusetts Insurance News. http://agencychecklists.com/2017/08/14/nationwide-insurance-pays-mass-100000-as-part-of-multistate-data-breach-settlement-19525/

Gara, T. (2014, February 18). What did the Target hack really cost? The numbers trickle in. *The Wall Street Journal*. https://blogs.wsj.com/corporate-intelligence/2014/02/18/what-did-the-target-hack-really-cost-the-numbers-trickle-in/

Garcia, A. (2015, December 2). *Target settles for $39 million over data breach*. CNNMoney. http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/index.html

Gerda, N. (2016, August 2). *Transportation Authority kept secret cyber attack that cost $600,000*. Voice of OC. https://voiceofoc.org/2016/08/transportation-authority-kept-secret-cyber-attack-that-cost-600000/

Goel, V. (2017, February 21). Verizon will pay $350 million less for Yahoo. *The New York Times.* https://search.proquest.com/docview/1870461372/fulltext/47F6EBE37DDF4F92PQ/12?accountid=31567

Goodin, D. (2011, May 24). *PlayStation Network breach will cost Sony $171m*. The Register. https://www.theregister.co.uk/2011/05/24/sony_playstation_breach_costs/

Goodman, B. (2015, April 19). A few challenges in calculating total cost of a data breach using insurance claims payment data. *Ponemon Institute*. https://www.ponemon.org/blog/a-few-challenges-in-calculating-total-cost-of-a-data-breach-using-insurance-claims-payment-data

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb Model. *Journal of Information Security, 6*(1), 24–30. https://doi.org/10.4236/jis.2015.61003

Gorman, S. (2013, July 22). Annual U.S. cybercrime costs estimated at $100 billion. *The Wall Street Journal.* https://www.wsj.com/articles/SB10001424127887324328904578621880966242990

Gorman, S., Cole, A., & Dreazen, Y. (2009, April 21). Computer spies breach fighter-jet project. *The Wall Street Journal.* https://www.wsj.com/articles/SB124027491029837401

Greenberg, A. (2018, August 22). *The untold story of NotPetya, the most devastating cyberattack in history*. WIRED. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Greenemeier, L. (2009, April 21). Unknown hackers steal details on U.S. Joint Strike Fighter project. *Scientific American*. https://blogs.scientificamerican.com/news-blog/unknown-hackers-steal-details-on-us-2009-04-21/

Griffin, R., Chiglinsky, K., & Voreacos, D. (2019, December 3). *Was it an act of war? That's Merck cyber attack's $1.3 billion insurance question*. Insurance Journal. https://www.insurancejournal.com/news/national/2019/12/03/550039.htm

Grotto, A. J., & Makridis, C. (2018, July 11). Publicly reported data breaches: A measure of our ignorance? *Lawfare*. https://www.lawfareblog.com/publicly-reported-data-breaches-measure-our-ignorance

Gunderman, D. (2017, October 31). *NotPetya costs Merck, FedEx, Maersk $800M*. Cyber Security Hub. https://www.cshub.com/attacks/news/notpetya-costs-merck-fedex-maersk-800m

Hachman, M. (2011, May 23). *PlayStation hack to cost Sony $171M; Quake costs far higher*. PC Magazine. https://www.pcmag.com/article2/0,2817,2385790,00.asp

Hackett, R. (2015, March 27). *How much do data breaches cost big companies? Shockingly little*. Fortune. http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/

Hardy, M. R. (2006). *An introduction to risk measures for actuarial applications*. Casualty Actuarial Society. https://www.casact.org/library/studynotes/hardy4.pdf

Hawkins, B. (2015). *Case study: The Home Depot data breach*. SANS Institute. https://www.sans.org/reading-room/whitepapers/breaches/case-study-home-depot-data-breach-36367

Hilary, G., Segal, B., & Zhang, M. H. (2016). *Cyber-risk disclosure: Who cares?* (Georgetown McDonough School of Business Research Paper No. 2852519). https://doi.org/10.2139/ssrn.2852519

Hill, M. (2016, July 4). *Majority of orgs still don't know value of critical data*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/majority-of-orgs-dont-know-value/

Hiscox. (2017). *The Hiscox Cyber Readiness Report 2017*. https://www.hiscox.com/documents/brokers/cyber-readiness-report.pdf

Hiscox. (2018). *2018 Hiscox Cyber Readiness Report*. https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf

Hiscox. (2019). *Hiscox Cyber Readiness Report 2019*. https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf

Hiscox. (2020). *Hiscox Cyber Readiness Report 2020*. https://www.hiscoxgroup.com/sites/group/files/documents/2020-06/Hiscox-Cyber-Readiness-Report-2020.pdf

Holder, W. W., Schermann, K. R., & Whittington, R. (2003). Materiality considerations. *Journal of Accountancy*, *196*(5), 61–66. https://www.journalofaccountancy.com/issues/2003/nov/materialityconsiderations.html

Home Depot. (2014). *2014 Annual Report*. http://www.homedepotar.com/2014/financial.html

Huotari, J. (2016, August 16). *County agrees to spend up to $100,000 to fix computer security breach*. Oak Ridge Today. http://oakridgetoday.com/2016/08/16/county-agrees-to-spend-up-to-100000-to-fix-computer-security-breach/

Imperva. (2016). *DDoS Threat Landscape Report 2015 - 2016*. Retrieved July 2019, from https://lp.incapsula.com/rs/804-TEY-921/images/2015-16%20DDoS%20Threat%20Landscape%20Report.pdf

Ingham County Controller's Office (2016). *2017 Ingham County Budget*. https://co.ingham.org/departments_and_officials/controller/2017_adopted_budget.php

Internal Revenue Service. (2016). *FY 2017 President's Budget*. https://www.treasury.gov/about/budget-performance/CJ17/02-06.%20IRS%20FY%202017%20CJ%201%2022%2016%20v2%20FINAL%20CLEAN.PDF

Internet Crime Complaint Center. (2017). *2017 Internet Crime Report*. Federal Bureau of Investigation. https://pdf.ic3.gov/2017_IC3Report.pdf

Internet Crime Complaint Center. (2019). *2018 Internet Crime Report*. Federal Bureau of Investigation. https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf

Internet Crime Complaint Center. (2020). *2019 Internet Crime Report*. Federal Bureau of Investigation. https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf

The Interview: A guide to the cyber attack on Hollywood. (2014, December 29). BBC News. http://www.bbc.com/news/entertainment-arts-30512032

Isaac, M., Benner, K., & Frenkel, S. (2017, November 21). Uber hid 2016 breach, paying hackers to delete stolen data. *The New York Times.* https://www.nytimes.com/2017/11/21/technology/uber-hack.html

Jacobs, J. (2014, December 11). Analyzing Ponemon cost of data breach. *Data Driven Security*. https://datadrivensecurity.info/blog/posts/2014/Dec/ponemon/

Jay, J. (2017, May 10). *Yahoo coughed up $16m in legal costs following 2013 data breach*. TEISS. https://teiss.co.uk/information-security/yahoo-16m-legal-costs-data-breach/

Johnson, T. (2015, October 20). *Sony cyber attack settlement includes ID theft protection, $4.5 mil reimbursement funds*. Variety. https://variety.com/2015/film/news/sony-hack-class-action-settlement-id-theft-protection-1201621993/

Johnson, V. R. (2005). Cybersecurity, identity theft, and the limits of tort liability. *South Carolina Law Review*, *57*(2), 255–312. https://law.bepress.com/cgi/viewcontent.cgi?referer=&httpsredir=1&article=3530&context=expresso

Juniper Research. (2017, May 30). *Cybercrime to cost global business over $8 trillion in the next 5 years* [Press release]. https://www.juniperresearch.com/press/press-releases/cybercrime-to-cost-global-business-over-$8-trn

Kambic, D., Moore, A., Tobar, D., & Tucker, B. (in press). *Loss Magnitude Estimation in Support of Business Impact Analysis*. Carnegie Mellon University, Software Engineering Institute, CERT Division. Pending public release.

Kaspersky Lab. (n.d.). *Damage control: The cost of security breaches: IT Security Risks Special Report Series*. https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

Kaspersky Lab. (2016a). *KSN report: Ransomware in 2014-2016*. https://securelist.com/files/2016/06/KSN_Report_Ransomware_2014-2016_final_ENG.pdf

Kaspersky Lab. (2016b). *Measuring financial impact of IT security on businesses: IT Security Risks Report 2016*. https://media.kaspersky.com/en/business-security/kaspersky-it-security-risks-report-2016.pdf

Kaspersky Lab. (2017). *IT security: Cost center or strategic investment?* https://go.kaspersky.com/rs/802-IJN-240/images/IT%20Security%20Econmics%20Report%209.18.17.pdf?aliId=488652022

Kaspersky Lab. (2018). *On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives.* https://go.kaspersky.com/rs/802-IJN-240/images/2205_kaspersky_%20IT%20Security%20economy%20Report_final_2305.compressed_NA.PDF

Kaspersky Lab. (2019). *IT security economics in 2019: how businesses are losing money and saving costs amid cyberattacks*. https://media.kasperskydaily.com/wp-content/uploads/sites/92/2019/10/01041217/Kaspersky_Report-IT-Security-Economics_report_2019_NA.pdf

Katz, E. (2019, February 12). *OPM awards $416M contract for protection services to hack victims*. Government Executive. https://www.govexec.com/pay-benefits/2019/02/opm-awards-416m-contract-protection-services-hack-victims/154814/

Krebs, B. (2012, October 15). The scrap value of a hacked PC, revisited. *Krebs on Security*. https://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

Krebs, B. (2016, July 14). The value of a hacked company. *Krebs on Security*. https://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/

Kuchler, H. (2016, December 14). Ashley Madison agrees $1.6m fine for data breach. *Financial Times.* https://www.ft.com/content/db7a5c42-c21a-11e6-9bca-2b93a6856354

Kvochko, E., & Pant, R. (2015, March 31). Why data breaches don't hurt stock prices. *Harvard Business Review.* https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices

Lacy, E. (2017, May 19). Cyberattack a $2M 'wake-up call' to Ingham County. *Lansing State Journal.* https://www.lansingstatejournal.com/story/news/local/2017/05/19/cyberattack-2-m-wake-up-call-ingham-county/333542001/

Lambert, C. (2015, October 16). Cuesta College to offer free ID theft protection after data breach. *The Tribune News*. http://www.sanluisobispo.com/news/local/article39055911.html#!

Lee, R. M., Assante, M. J., & Conway, T. (2016, March 18). *Analysis of the cyber attack on the Ukrainian power grid: Defense use case.* SANS Institute, Electricity Information Sharing and Analysis Center. http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

Lemos, R. (2015, February 4). *Sony pegs initial cyber-attack losses at $35 million*. eWeek. http://www.eweek.com/security/sony-pegs-initial-cyber-attack-losses-at-35-million

Lemos, R. (2016, September 24). *RAND insurance payout study hints at smaller average data breaches*. eWeek. http://www.eweek.com/security/rand-insurance-payout-study-hints-at-smaller-average-data-breaches

Lennon, M. (2012, August 3). *LinkedIn: Breach cost up to $1M, says $2-3 million in security upgrades coming*. SecurityWeek. https://www.securityweek.com/linkedin-breach-cost-1m-says-2-3-million-security-upgrades-coming

Lennon, M. (2017, November 9). *Equifax: Hack related expenses cost company $87.5 million in Q3*. SecurityWeek. http://www.securityweek.com/equifax-hack-related-expenses-cost-company-875-million-q3

Levin, A. (2012, October 1). *The Wisconsin Department of Revenue: A bargain for the identity theft collective*. Huffington Post. https://www.huffingtonpost.com/adam-levin/wisconsin-leaks-taxpayer-id-numbers_b_1729239.html

Lewis, D. (2015, May 31). *Heartland Payment Systems suffers data breach*. Forbes. https://www.forbes.com/sites/davelewis/2015/05/31/heartland-payment-systems-suffers-data-breach/#71d04d21744a

LinkedIn Corporation. (2013, February 7). *LinkedIn announces fourth quarter and full year 2012 financial results*. https://news.linkedin.com/2013/02/linkedin-announces-fourth-quarter-and-full-year-2012-financial-results

Lipkin, M., Sistrunk, J., Shrestha, B., & Bowen, E. (2014, June 13). *Sony strikes $15M deal to exit data-breach MDL*. Law360. https://www.law360.com/articles/548191/sony-strikes-15m-deal-to-exit-data-breach-mdl

Liptak, A. (2017, July 16). *Ashley Madison's parent company has proposed a settlement with users exposed in data breach*. The Verge. https://www.theverge.com/2017/7/16/15979222/ashley-madison-ruby-corp-settlement-data-breach-cybersecurity

Lloyd's. (2015). *Business blackout: The insurance implications of a cyber attack on the US power grid*. Prepared in collaboration with and based on original research by the Centre for Risk Studies, University of Cambridge. www.lloyds.com/businessblackout

Lloyd's. (2017). *Counting the cost: Cyber exposure decoded*. Prepared in collaboration with Cyence. https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/countingthecost

Lloyd's. (2018). *Cloud down: Impacts on the US economy*. Prepared in collaboration with AIR. https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/cloud-down

Lloyd's. (2019). *Bashe attack: Global infection by contagious malware*. Prepared in collaboration with and based on original research by the Centre for Risk Studies, University of Cambridge. https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/bashe-attack

Lunden, I. (2015, February 25). *Target says credit card data breach cost it $162M in 2013-14*. TechCrunch. https://techcrunch.com/2015/02/25/target-says-credit-card-data-breach-cost-it-162m-in-2013-14/

Lynch, V. (2017, May 26). Cost of 2013 Target data breach nears $300 million. *The SSL Store*. https://www.thesslstore.com/blog/2013-target-data-breach-settled/

MarketWatch. (2018a). *Home Depot Inc*. https://www.marketwatch.com/investing/stock/hd/financials

MarketWatch. (2018b). *Target Corp*. https://www.marketwatch.com/investing/stock/tgt/financials

Maricopa County Community College District. (2013). *Comprehensive Annual Financial Report: Fiscal year ended June 30, 2013*. https://www.azauditor.gov/sites/default/files/Maricopa_CCCD_6_30_13_CAFR.pdf

Maricopa County Community College District. (2014). *Budget Analysis Report*. https://district.maricopa.edu/sites/g/files/vmcrws416/files/documents/Jun-14%20Final.pdf

Martinez, E. (2011, May 24). *PlayStation Network breach has cost Sony $171 million*. CBS News. https://www.cbsnews.com/news/playstation-network-breach-has-cost-sony-171-million/

Matthews, T. (2015). *Incapsula Survey: What DDoS attacks really cost businesses.* Incapsula. https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf

May, C. (2017, March). *Transnational crime and the developing world*. Global Financial Integrity. https://www.gfintegrity.org/wp-content/uploads/2017/03/Transnational_Crime-final.pdf

Maynard, T., & Ng, G. (2017). *Emerging Risks Report 2017: Counting the cost: Cyber exposure decoded*. Cyence and Lloyd's. https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2017/cyence/emerging-risk-report-2017---counting-the-cost.pdf

McAfee. (2013). *The economic impact of cybercrime and cyber espionage*. Center for Strategic and International Studies. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf

McAfee. (2014). *Net losses: Estimating the global cost of cybercrime. Economic impact of cybercrime II*. Center for Strategic and International Studies. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

McAfee. (2018, February). *Economic impact of cybercrime—No slowing down*. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email

McClintock, P. (2015, January 16). *'The Interview' lost Sony $30 million, says theater group*. The Hollywood Reporter. https://www.hollywoodreporter.com/news/interview-lost-sony-30-million-764366

McGee, M. K. (2014, September 2). *Hospital chain breach: How expensive?* DataBreachToday. https://www.databreachtoday.com/hospital-chain-breach-how-expensive-a-7252

McGee, M. K. (2017, January 10). *A new in-depth analysis of Anthem breach*. BankInfoSecurity. https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

McGrath, M. (2014, February 26). *Target profit falls 46% on credit card breach and the hits could keep on coming*. Forbes. https://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/#69b8c7db7326

McVicar, B. (2013, October 22). *$380k spent investigating, cleaning up after Ferris State's online security breach*. MLive Media Group. http://www.mlive.com/news/grand-rapids/index.ssf/2013/10/ferris_state_spent_380000_inve.html

Mead, D. (2014, January 29). The latest cost of the Target hack: $153 million worth of new credit cards. *VICE Motherboard*. https://motherboard.vice.com/en_us/article/gvybey/the-latest-cost-of-the-target-hack-153-million-worth-of-new-credit-cards

Merck. (2017). *2017 Annual Report*. http://www.annualreports.com/HostedData/AnnualReports/PDF/NYSE_MRK_2017.pdf

Michigan State University. (2017). *Michigan State University 2017-2018 budgets*. https://msu.edu/_assets/documents/transparency-reporting/2017-18Budgets.pdf

Moore, T. (2010). Introducing the economics of cybersecurity: Principles and policy options. In, *Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for U.S. policy* (pp. 3–24). The National Academies Press. https://doi.org/10.17226/12997

Moore, T., & Anderson, R. (2011). *Economics and internet security: A survey of recent analytical, empirical and behavioral research*. (Harvard Computer Science Group Technical Report TR-03-11). https://www.researchgate.net/publication/216757810_Economics_and_Internet_Security_a_Survey_of_Recent_Analytical_Empirical_and_Behavioral_Research

Morgan, S. (2016, August 17). Hackerpocalypse: A cybercrime revelation. *Herjavec Group*. https://www.herjavecgroup.com/hackerpocalypse-cybercrime-report/

Morningstar. (2019a, February). *Anthem Inc: ATNM*. Retrieved on March 15, 2019, from http://quote.morningstar.ca/Quicktakes/Financials/is.aspx?t=ANTM&region=USA&culture=en-CA&ops=clear

Morningstar. (2019b, February). *Anthem Inc: ATNM*. Retrieved on March 15, 2019, from http://quote.morningstar.ca/Quicktakes/stock/perf.aspx?t=ANTM&region=USA&culture=en-CA&ops=clear

National Institute of Standards and Technology. (2012). *Computer security incident handling guide* (Special Publication 800-61r2). U.S. Department of Commerce. http://dx.doi.org/10.6028/NIST.SP.800-61r2

National Retail Federation. (2018). *2018 National Retail Security Survey*. In Partnership with Appriss Retail and University of Florida. https://cdn.nrf.com/sites/default/files/2018-10/NRF-NRSS-Industry-Research-Survey-2018.pdf

Nationwide Mutual Insurance Company. (2012). *Combined Annual Statement of the Nationwide Mutual Insurance Company*. http://static.nationwide.com/static/2012-Combined-Statement.pdf?r=40

NetDiligence. (2015). *2015 Cyber Claims Study*. https://netdiligence.com/wp-content/uploads/2017/03/NetDiligence_2015_Cyber_Claims_Study_093015.pdf

NetDiligence. (2017). *NetDiligence 2017 Cyber Claims Study* (Version 1.3). https://netdiligence.com/wp-content/uploads/2017/10/2017-NetDiligence-Claims-Study_Public-Edition-1.3.pdf

NetDiligence. (2018). *NetDiligence 2018 Cyber Claims Study* (Version 1.0). https://netdiligence.com/wp-content/uploads/2018/11/2018-NetDiligence-Claims-Study_Version-1.0.pdf

NetDiligence. (2019). *NetDiligence Cyber Claims Study: 2019 report*. https://netdiligence.com/cyber-claims-study-2019-report/

Norton. (2015). *Norton Cybersecurity Insights Report.* https://us.norton.com/norton-cybersecurity-insights-report-global?inid=hho_norton.com_cybersecurityinsights_hero_seeglobalrpt

Norton. (2016). *2016 Norton Cyber Security Insights Report*. http://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/2016-Norton-Cyber-Security-Insights-Report.pdf

Norton. (2017). *2017 Norton Cyber Security Insights Report: Global results*. http://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-US.pdf

Norton. (2018). *Cyber Safety Insights Report: Global results*. https://now.symassets.com/content/dam/norton/campaign/NortonReport/2019/2018_Norton_LifeLock_Cyber_Safety_Insights_Report_Global_Media_Deck.pdf

Office of Management and Budget. (2003, September 17). *Circular A-4*. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A4/a-4.pdf

Office of Management and Budget. (2017). *Federal Information Security Modernization Act of 2014: Annual report to Congress*. https://www.whitehouse.gov/wp-content/uploads/2017/11/FY2017FISMAReportCongress.pdf

Office of Management and Budget. (2019). *Federal Information Security Modernization Act of 2014: Annual Report to Congress: Fiscal Year 2019*. https://www.whitehouse.gov/wp-content/uploads/2020/05/2019-FISMARMAs.pdf

The Ohio State University. (2010). *2010 - 2011 Current Funds Budget*. Prepared by the Office of Resource Planning. http://www.rpia.ohio-state.edu/cfb/docs/cfb-2011.pdf

Perez, C. (2015, August 24). Ashley Madison facing massive lawsuit 'on behalf of all Canadians.' *New York Post.* https://nypost.com/2015/08/24/ashley-madison-facing-578m-class-action-lawsuit/

Perlroth, N. (with de la Merced, M. J.). (2016, September 22). Yahoo says hackers stole data on 500 million users in 2014. *The New York Times.* https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html

Pierson, B. (2017, June 23). *Anthem to pay record $115 million to settle U.S. lawsuits over data breach*. Reuters. https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML

Ponemon, L. (2015, April 16). Why Ponemon Institute's Cost of Data Breach methodology is sound and endures. *Ponemon Institute*. https://www.ponemon.org/blog/why-ponemon-institute-s-cost-of-data-breach-methodology-is-sound-and-endures

Ponemon Institute. (2012, June). *2012 Consumer Study on Data Breach Notification*. Experian Data Breach Resolution. http://www.experian.com/assets/data-breach/brochures/ponemon-notification-study-2012.pdf

Ponemon Institute. (2013). *2013 Cost of Data Breach Study: Global analysis*. Benchmark research sponsored by Symantec. https://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf

Ponemon Institute. (2014). *Is your company ready for a big data breach? The second annual study on data breach preparedness.* Sponsored by Experian Data Breach Resolution. https://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf

Ponemon Institute. (2015, October). *2015 Cost of Cyber Crime Study: Global*. Sponsored by Hewlett Packard Enterprise. http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf

Ponemon Institute. (2016a, July). *2016 Cost of Data Breach Study: Global analysis*. IBM Security. https://www.bankinfosecurity.com/whitepapers/2016-cost-data-breach-study-global-analysis-w-2647

Ponemon Institute. (2016b, October). *2016 Cost of Cyber Crime Study & the Risk of Business Innovation*. Sponsored by Hewlett Packard Enterprise. https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

Ponemon Institute. (2017a, June). *2017 Cost of Data Breach Study: Global overview*. Benchmark research sponsored by IBM Security. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

Ponemon Institute. (2017b, June). *2017 Cost of Data Breach Study: United States*. Sponsored by IBM Security. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130USEN&

Ponemon Institute. (2018, July). *2018 Cost of Data Breach Study: Global overview*. Security Intelligence. https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

Ponemon Institute. (2019). *2019 Cost of Data Breach Report*. Security Intelligence. https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

Prior, R. (2019, July 26). *Equifax will pay up to $700 million over its data breach: Here's how to claim your money*. CNN Business. https://www.cnn.com/2019/07/25/us/equifax-700-million-settlement-data-breach-trnd/index.html

Privacy Rights Clearinghouse. (2018). *Data breaches*. https://www.privacyrights.org/data-breaches?title=playstation

PwC. (2018). *Are insurers adequately balancing risk & opportunity? Findings from PwC's global cyber insurance survey*. https://www.pwc.com/us/en/industry/assets/pwc-cyber-insurance-survey.pdf

Radichel, T. (2014). *Case study: Critical controls that could have prevented Target breach*. SANS Institute. https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412

Ragan, S. (2016, December 8). *After attack, Indiana county will spend $220,000 on Ransomware recovery*. CSO Online. https://www.csoonline.com/article/3148274/security/after-attack-indiana-county-will-spend-220000-on-ransomware-recovery.html

Rashid, F. Y. (2017, May 31). *The Target data breach settlement sets a low bar for industry security standards*. CSO Online. https://www.csoonline.com/article/3199064/the-target-data-breach-settlement-sets-a-low-bar-for-industry-security-standards.html

Raymond, N. (2015, October 20). *Sony to pay up to $8 million in 'Interview' hacking lawsuit*. Reuters. https://www.reuters.com/article/us-sony-cyberattack-lawsuit/sony-to-pay-up-to-8-million-in-interview-hacking-lawsuit-idUSKCN0SE2JI20151020

Reuters. (2017, July 15). *Ashley Madison parent in $11.2 million settlement over data breach*. CNBC. https://www.cnbc.com/2017/07/15/ashley-madison-parent-in-11-point-2-million-settlement-over-data-breach.html

Richards, K., LaSalle, R. & van den Dool, F. (2017). *2017 Cost of Cyber Crime Study: Insights on the security investments that make a difference*. Independently conducted by Ponemon Institute LLC and jointly developed by Accenture. https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017

Risk Based Security. (2018). *Cyber risk analytics* [Data file]. https://www.cyberriskanalytics.com/#about

Risk Management Solutions, Inc. (2016). *Managing cyber insurance accumulation risk*. Prepared in collaboration with and based on original research by the Centre for Risk Studies, University of Cambridge. https://forms2.rms.com/rs/729-DJX-565/images/RMS-Managing-Cyber-Insurance-Accumulation-Risk-05142016.pdf

Roberts, J. J. (2017, March 9). *Home Depot to pay banks $25 million in data breach settlement*. Fortune. http://fortune.com/2017/03/09/home-depot-data-breach-banks/

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cyber Security*, *5*(1), 1–19. https://doi.org/10.1093/cybsec/tyz002

Rubin, R., & Belkin, D. (2017, April 6). *IRS data on up to 100,000 taxpayers compromised in breach of college financial-aid tool*. FOX Business. http://www.foxbusiness.com/politics/2017/04/06/irs-data-on-up-to-100000-taxpayers-compromised-in-breach-college-financial-aid-tool.html

Ruby Life Inc. (2017, July 14). *Ruby Corp and plaintiffs reach proposed settlement of class action lawsuit regarding Ashley Madison data breach*. PR Newswire. https://www.prnewswire.com/news-releases/ruby-corp-and-plaintiffs-reach-proposed-settlement-of-class-action-lawsuit-regarding-ashley-madison-data-breach-634551783.html

Russon, G. (2016, March 28). The cost of UCF computer hack: $109K spent to notify victims. *Orlando Sentinel*. http://www.orlandosentinel.com/features/education/school-zone/os-ucf-lawsuit-dismissed-hack-story.html

San Luis Obispo County Community College District. (2013). *Final Budget 2014-2015*. https://www.cuesta.edu/about/documents/fiscal-docs/Adopted_Budget_2014-2015.pdf

SAS. (2015). *SAS® OpRisk global data.* https://www.sas.com/content/dam/SAS/en_us/doc/productbrief/sas-oprisk-global-data-101187.pdf

Schaffhauser, D. (2014, December 16). *Berkeley breach hits 1,600, costs $150,000 so far*. Campus Technology. https://campustechnology.com/articles/2014/12/16/berkeley-breach-hits-1600-costs-150000-so-far.aspx

Schreier, J. (2011, May 23). *Sony estimates $171 million loss from PSN hack*. WIRED. https://www.wired.com/2011/05/sony-psn-hack-losses/

Securities and Exchange Commission. (2018). *17 CFR Parts 229 and 249:Commission statement and guidance on public company cybersecurity disclosures.* https://www.sec.gov/rules/interp/2018/33-10459.pdf

Shain, A. (2012, October 30). *SC hack victims to get lifetime ID theft resolution aid*. The State. http://www.thestate.com/news/politics-government/article14413562.html

Silver-Greenberg, J., Goldstein, M., & Perlroth, N. (2014, October 2). JPMorgan Chase hacking affects 76 million households. *The New York Times.* https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/

Siwicki, B. (2016, May 23). *Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money*. Healthcare IT News. http://www.healthcareitnews.com/news/kansas-hospital-hit-ransomware-pays-then-attackers-demand-second-ransom

Solomon, H. (2020, May 21). *Attackers still exploiting old vulnerabilities, says NTT report*. IT World Canada. https://www.itworldcanada.com/article/attackers-still-exploiting-old-vulnerabilities-says-ntt-report/430994

Sony agrees to reimburse ID theft charges, offer user benefits to settle breach lawsuit. (2014, June 23). Bloomberg. https://www.bna.com/sony-agrees-reimburse-n17179891495/

Sony Corporation. (2013). *2013 Sony Corporation, SEC Form 20-F*. https://www.sec.gov/Archives/edgar/data/313838/000119312513273660/d519176d20f.htm

Sony Corporation. (2014). *2014 Sony Corporation, SEC Form 20-F*. https://www.sec.gov/Archives/edgar/data/313838/000119312515231346/d895998d20f.htm

Sony Corporation. (2015). *FY2014 consolidated financial results: (Fiscal year ended March 31, 2015)*. https://www.sony.net/SonyInfo/IR/library/fr/14q4_sonypre.pdf

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, *58,* 216–229. https://doi.org/10.1016/j.cose.2015.12.006

State of Connecticut Department of Banking. (2009, February 3). *Department of Consumer Protection and Department of Banking announce settlement with Bank of New York Mellon for 2008 data breach*. http://www.ct.gov/dob/cwp/view.asp?a=2245&q=433242

State of Georgia. (2014). *The Governor's Budget Report: Fiscal Year 2015*. https://opb.georgia.gov/sites/opb.georgia.gov/files/related_files/document/FY2015GovernorsReport.pdf

State of South Carolina. (2012). *Executive Budget Fiscal Year 2011-2012*. https://www.scstatehouse.gov/sess119_2011-2012/appropriations2011/xbud1112.pdf

Statista. (2018). *Revenue of Yahoo from 2004 to 2016 (in million U.S. dollars)*. https://www.statista.com/statistics/266253/yahoos-annual-gaap-revenue/

Stempel, J. (2017, July 14). *Ashley Madison parent in $11.2 million settlement over data breach*. Reuters. https://www.reuters.com/article/us-ashleymadison-settlement/ashley-madison-parent-in-11-2-million-settlement-over-data-breach-idUSKBN19Z2F0

Stewart, K. (2013, April 29). Report: Utah's health data breach was a costly mistake. *The Salt Lake Tribune.* http://archive.sltrib.com/article.php?id=56210404&itype=CMSID

Symantec. (2014). *ISTR: Internet Security Threat Report: 2014* (Volume 19). https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Symantec. (2015). *ISTR 20: Internet Security Threat Report* (Volume 20). https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf

Symantec. (2016, April). *ISTR: Internet Security Threat Report* (Volume 21). https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Symantec. (2017, April). *ISTR: Internet Security Threat Report* (Volume 22). https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Symantec. (2018). *ISTR: Internet Security Threat Report* (Volume 23). https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

Symantec. (2019, February). *ISTR: Internet Security Threat Report* (Volume 24). https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

Target Corporation. (2015, February 25). *Target reports fourth quarter and full-year 2014 earnings*. http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=2019880

Target Corporation. (2017). *2016 Annual Report*. https://corporate.target.com/_media/TargetCorp/annualreports/2016/pdfs/Target-2016-Annual-Report.pdf

Tofan, D., Nikolakopoulos, T., & Darra, E. (2016, August). *The cost of incidents affecting CIIs: Systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII)*. European Union Agency for Network and Information Security. https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis

Torres, K. (2015, December 16). Sign-up now for credit monitoring after Georgia data breach. *The Atlanta Journal-Constitution.* https://www.ajc.com/news/state--regional-govt--politics/sign-now-for-credit-monitoring-after-georgia-data-breach/gAz6DskpC7WbThe9XljRWO/

Turner, N. (2014, November 6). *Insurance covers $27M of Home Depot's breach recovery costs*. Bloomberg. Insurance Journal. https://www.insurancejournal.com/news/national/2014/11/06/346189.htm

University of California, Berkeley. (2013). *2013-2014 UC Berkeley Budget Plan*. https://cfo.berkeley.edu/sites/default/files/2013-14%20UC%20Berkeley%20Budget%20Plan%20-%20Final%20%289-5-13%29.pdf

University of Central Florida. (2015). *UCF Facts 2015-2016 Archive.* https://www.ucf.edu/ucf-facts-2015-2016/#budget

UPDATE 1-Experian says receives class actions on T-Mobile breach. (2015, November 10). Thompson Reuters. https://uk.reuters.com/article/experian-cybercrime-t-mobile-us-idUKL3N1352S620151110

U.S. Census Bureau. (2013). *2012 Census of Governments: Organization component estimates*. https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?src=bkmk

Utah State Legislature. (2012). *Utah State Budget Summary*. https://le.utah.gov/lfa/reports/cobi2012/COBI2012.htm

Utermohlen, K. (2017, July 17). *Ashley Madison data breach victims may receive up to $3,500*. InvestorPlace. https://investorplace.com/2017/07/ashley-madison-data-breach/

Verizon. (2014). *2014 Data Breach Investigations Report*. https://webfiles.dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf

Verizon. (2015). *2015 Data Breach Investigations Report*. https://www.verizon.com/about/news/2015-data-breach-report-info

Verizon. (2016a). *2016 Data Breach Investigations Report*. http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Verizon. (2016b). *Data Breach Digest*. http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf

Verizon. (2017). *2017 Data Breach Investigations Report: 10th edition*. https://enterprise.verizon.com/resources/reports/2017_dbir.pdf

Verizon. (2018). *2018 Data Breach Investigations Report: 11th edition.* https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

Verizon. (2019). *2019 Data Breach Investigations Report*. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Verizon. (2020). *2020 Data Breach Investigations Report*. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Vijayan, J. (2010, June 4). *Insurer says it's not liable for University of Utah's $3.3M data breach*. Computerworld. https://www.computerworld.com/article/2518592/data-security/insurer-says-it-s-not-liable-for-university-of-utah-s--3-3m-data-breach.html

Vorhies, J. B. (2005). The new importance of materiality. *Journal of Accountancy, 199*(5), 53–59. https://www.journalofaccountancy.com/issues/2005/may/thenewimportanceofmateriality.html

Wassel, B. (2018, August 27). *2017 shrink cost U.S. retailers $42.49 billion, 1.85% of sales*. Retail TouchPoints. https://www.retailtouchpoints.com/topics/security-pci-compliance/2017-shrink-cost-u-s-retailers-42-49-billion-1-85-of-sales

Weidmayer, M. (2016, December 2). *MSU to spend $2.9 million in wake of data breach*. The State News. http://statenews.com/article/2016/12/msu-to-spend-nearly-3-million-after-data-breach

Willis, H. H., LaTourrette, T., Kelly, T. K., Hickey, S., & Neill, S. (2007). *Terrorism risk modeling for intelligence analysis and infrastructure protection*. RAND Center for Terrorism Risk Management Policy. https://www.rand.org/content/dam/rand/pubs/technical_reports/2007/RAND_TR386.pdf

Wisconsin state budget (2012-2013). (2013). Ballotpedia. https://ballotpedia.org/Wisconsin_state_budget_(2012-2013)

The World Bank (2017). *Listed domestic companies, total: World Federation of Exchanges database*. https://data.worldbank.org/indicator/CM.MKT.LDOM.NO?locations=US

The World Bank. (2019). *GDP (current US$)*. https://databank.worldbank.org/data/reports.aspx?source=2&series=NY.GDP.MKTP.CD&country=

World Economic Forum. (2014, January). *Risk and responsibility in a hyperconnected world*. In collaboration with McKinsey & Company. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/the%20rising%20strategic%20risks%20of%20cyberattacks/risk%20and%20responsibility%20in%20a%20hyperconnected%20world.ashx

World Economic Forum. (2015). *Global Risks 2015: 10th edition*. http://reports.weforum.org/global-risks-2015/

World Economic Forum. (2016). *The Global Risks Report 2016: 11th edition*. http://wef.ch/risks2016

World Economic Forum. (2017). *The Global Risks Report 2017: 12th edition*. http://wef.ch/risks2017

World Economic Forum. (2018). *The Global Risks Report 2018: 13th edition*. http://wef.ch/risks2018

World Economic Forum. (2019). *The Global Risks Report 2019: 14th edition*. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

XE. (2015). *XE currency table: JPY - Japanese Yen*. http://www.xe.com/currencytables/?from=JPY&date=2015-01-01

Yahoo. (2014). *2014 Annual Report*. http://www.annualreports.com/HostedData/AnnualReportArchive/y/NASDAQ_YHOO_2014.pdf

Yahoo Finance. (2019). *Anthem, Inc. (ANTM).* https://finance.yahoo.com/quote/ANTM/key-statistics/