THE BUSINESS CASE FOR **SECURITY**

BACKGROUND

"Can you put a price on the value your people and assets provide to your organization?" When considering investments in organizational security, that is a key question. Leaders can build and sustain a culture of readiness within their organizations by investing in security measures to drive strategy, policy, revenue and actions. Risk resiliency improvement requires a program that considers both cyber and physical security needs.

A business case for security relies on an in-depth understanding of organizational vulnerabilities, operational priorities and return on investment. According to a 2023 poll, **73% of owners and operators of small and mid-sized businesses (SMB) experienced a data breach, a cyberattack or both in the previous 12 months even though in 2022, 70% of SMBs believed they were ready to defend against a cyberattack or data breach.**[1] Physical and cyber incidents can have catastrophic impacts on the daily operations of SMBs. **Being flexible and adapting to current and future threats will increase resilience.**

WHAT IS THE TYPICAL COST OF AN INCIDENT?

Recovery from physical or cyber incidents is often more costly than investing in preventive measures. Though the cost of remediating a physical or cyber incident is quantifiable, recovering a company's damaged infrastructure and reputation can be difficult to assess. Ultimately, **the public's trust is priceless.**

SMBs were the victim in

89%

of cyber incidents where the company's losses exceeded more than 10% of their annual revenue.[2]

Employee safety is crucial for a company's commitment to security. Workplace violence affects 2 million people each year, directly impacting the physical requirements and cost of security.[3]

Leadership within an organization **must** consider investing in the long-term well-being of their organizations to prevent future costs stemming from security incidents.

KEY CONSIDERATIONS/POTENTIAL PHYSICAL AND CYBER THREAT VECTORS

- Burglary
- Data breach
- Malware
- Hostile vehicles
- Unmanned aircraft systems
- Vandalism
- Theft
- Swatting
- Hacking
- Doxing
- Insider threat
- Fire as a weapon
- Natural disaster
- Denial of Service
- Sabotage
- Ransomware
- Terrorism
- Active assailant
- Improvised explosive device
- Social Engineering

FOLLOWING A CYBERSECURITY INCIDENT:[1]

32%
of SMBs reported a **loss in customer trust**

32%
of SMBs reported employee turnover

42%
of SMBs reported a loss in revenue

In FY23, SMBs spent
an average of $8M
to deal with the consequences of an insider incident.[4]

1. ITRC, 2023, 2023 Business Impact Report, October, idtheftcenter.org/wp-content/uploads/2023/10/ITRC_2023-Business-Impact-Report_V2.1-3.pdf.
2. Cyentia Insitute, 2022, Information Risk Insights Study, ITRC, cyentia.com/wp-content/uploads/IRIS-2022_Cyentia.pdf.
3. U.S. Department of Homeland Security. 2020. Insider Threat Mitigation Guide. Cybersecurity and Infrastructure Security Agency, 48. cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf.
4. DTEX, Ponemon Institute, 2023, Cost of Insider Risks, www2.dtexsystems.com/l/464342/2023-09-15/3w7l7n/464342/1694800570Zec90CzW/2023_Cost_of_Insider_Risks_Global_Report___Ponemon_and_DTEX__Prnt.pdf.

The Business Case for Security

Developing a business case for security adds value, driving the importance of physical and cybersecurity investments within an organization. The following steps can help assess security vulnerabilities and develop actionable mitigation steps before an incident occurs.

UNDERSTAND YOUR SECURITY POSTURE

Understand the business' security posture

- Does the company have a Chief Information Security Officer, Chief Security Officer and Chief Information Officer?
- Are existing vulnerabilities linked to physical or cyber assets?
- Do the security gaps threaten the infrastructure?

Identify business assets that need to be protected

- Physical: People, property and facilities, including access
- Cyber: Server rooms, computers and IT infrastructure, including means of information sharing, third party hosting networks and cloud-based services

Align security investments to business objectives

- Business needs, risks and compliance requirements
- Company-specific numbers quantified by business impact analysis
- The cost of investing versus the cost of an attack

Determine the right areas for investment

- Establish leadership commitment
- Risk/reward ratio
- Know and understand your threat environment
- Prioritization of quick wins and urgent gaps
- Employee training and security awareness
- Partnerships for security purposes

Implement a security plan and schedule

- Develop employee training for existing and new security measures
- Exercise the plan in coordination with local first responders
- Create a schedule for implementing the security plan

Preparation

- Focus on resource requirements for security that buys down risk
- Anticipate questions and have answers

INDUSTRY TIPS

KNOW YOUR AUDIENCE

Getting buy-in from senior executives means presenting the business case with their decision-making process in mind. Consider known resistance factors the team has already identified and craft the presentation to demonstrate the directed approach. Align an analysis and recommendations with the organization's business priorities and strategic objectives. Present a strong narrative—thoughtful storytelling engages audience members.

ESTABLISH LEADERSHIP COMMITMENT

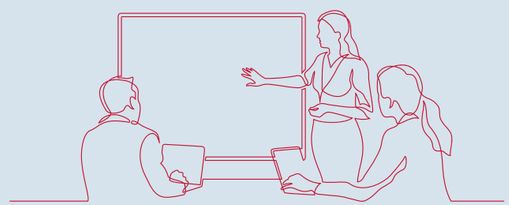
With an enterprise security approach, security investment recommendations should not come as a surprise to senior executives. Prior to writing the business case, identify senior leaders who will support, defend and advise on the project. Consult them throughout the process to ensure messaging is on point.

PARTICIPATE IN INDUSTRY ASSOCIATIONS

Industry associations are excellent resources. Participating in industry association security committees is a great way to become aware of the challenges facing your industry, identify opportunities for funding, learn industry best practices, receive trainings and identify resources through information-sharing collaborations. Designing a security strategy that is cultivated using best practices from other industry members can encourage senior leadership to have confidence in the proposal.

UNDERSTAND HOW LEADERSHIP DECISIONS ARE MADE

Security leaders need to understand how the organization makes decisions, allocates money across functional areas, prioritizes initiatives and develops strategic plans. Identify how often security measures are reviewed and consistently implemented against organizational risks and strategic priorities. These insights will inform the business case rationale and help determine the right approach for presenting this information.



For more information or to seek additional help, contact us at **Central@cisa.gov** or visit:

Cybersecurity and Physical Security Convergence Action Guide: cisa.gov/resources-tools/resources/cybersecurity-and-physical-security-convergence-action-guide

Stop Ransomware: cisa.gov/stopransomware

Free Cybersecurity Services and Tools: cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools

Critical Infrastructure Assessments: cisa.gov/critical-infrastructure-assessments

Best Practices for Making a Business Case for Security: cisa.gov/resources-tools/resources/isc-best-practices-making-business-case-security

CISA Small and Medium Businesses: cisa.gov/audiences/small-and-medium-businesses