CISA CYBERSECURITY ADVISORY COMMITTEE

REPORT TO THE CISA DIRECTOR

Secure By Design

October 11, 2024

Introduction:

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee (CSAC) established a Secure by Design (SBD) subcommittee (hereinafter referred to as the "subcommittee") to study the economic roadblocks that may hinder the adoption of Secure by Design principles.

The SBD subcommittee was tasked with providing recommendations for full Committee deliberation and vote to examine how CISA can encourage lasting, systemic action to reduce the nation's risk, study and maneuver the economic factors that have led to the current state of risk, and examine both the demand and supply factors that have historically limited secure software and hardware manufacturing.

The subcommittee was tasked with addressing the following questions to guide the subcommittee's work:

1. What are the incentives and economic forces that encourage or discourage software manufacturers from adopting secure by design practices, and how can CISA tilt the balance towards safer software?

2. If every enterprise and consumer made cybersecurity a top criterion for software purchases, the problem of unsafe software would start to work itself out. How can CISA work to generate a norm of "secure by demand" in the procurement process? Related, how can such a norm help customers ask for security features that increase the cost for attackers, rather than settle for security features that are merely ineffective checkbox items?

Findings:

Over the past two years, CISA has successfully raised the cybersecurity bar with its Secure by Design initiative, collaborating with over 17 domestic and international partners to publish clear guidance on the key security principles needed to defend our nation against today's ever-evolving cyber threats. Today, over 200 software manufacturers have already pledged to make measurable progress towards implementing the Secure by Design principles.

Now that CISA has successfully raised awareness of the Secure by Design principles, the next step is to encourage their widespread adoption. Over the past six months, the subcommittee has been focused on identifying a set of recommendations that would allow CISA to make measurable progress in the widespread adoption of the Secure by Design principles. The subcommittee engaged with both the public sector and private industry to gather insights and thoughts to spur adoption of the principles.

The subcommittee met with academics, subject matter experts, CISA's legal team, and CISA attestation teams to understand what motivates organizations to implement better security. The subcommittee's findings did not yield the expected results and have challenged some of its fundamental thinking in this space. Primarily, the subcommittee discovered that there is often no empirical evidence to substantiate some of its long-held security beliefs.

Fact or Myth? - Security flaws make people walk away from solutions.

There are numerous cases of companies that experienced security failures and are still around today. In general, it seems that quality failures don't always affect customer loyalty.

In 2013, the Target data breach was considered one of the biggest security breaches in history. Due to lack of network segregation, attackers were able to leverage a third-party portal to jump into Target's network and steal 40 million credit and debit card records. Eleven years later, Target is considered one of the top 10 retailers in the US.

In 2016, Samsung was forced to announce a recall of its $800+ Samsung Galaxy Note 7 devices following numerous reports of the phone catching fire. Reports at the time estimated that this "could burn a $17 billion hole in Samsung accounts" [1]. Eight years later, Samsung is still making smartphones and is considered one of the top five smartphone manufacturers worldwide.

In 2020, the SolarWinds cyberattack was called the "largest and most sophisticated attack the world has ever seen". Nearly 18,000 public and private organizations were affected by malware infected updates distributed by Microsoft. At the time of the attack discovery in December 2020, SolarWinds reported over 300,000 customers [2]. Four years later, SolarWinds continues to exist and still has over 300,000 customers [3].

Therefore, just telling organizations that not fixing security bugs will impact their business is not enough of an incentive.

After a large-scale security event occurs, the behavior of existing customers can be influenced by:

- The potential cost of switching to another brand.
- The amount of research a customer is willing to do to understand the impact of the security event.
- The effectiveness of a company's marketing messages about their response to the security event.

Customers often convince themselves that after a security breach, a company will naturally do more to make security better going forward, whether actual changes are made or not. It is unclear whether some of these same factors would influence new potential customers.

Fact or Myth? - Finding and fixing security vulnerabilities early in the development process is more cost effective.

It is a commonly held belief that fixing vulnerabilities earlier is more cost effective. "Shift left" emphasizes moving testing activities earlier in the development process, with the notion that earlier identification of issues is better and produces a higher quality product. The challenge is in quantifying how much investment needs to be made.

Numerous articles are referred to by the software industry referencing a study by the IBM Systems Science Institute that claims that fixing bugs during the design phase is 100 times cheaper than after implementation. Upon further research, there is no evidence to show that the IBM Systems Science Institute was an official research body. It appears to be an internal IBM program that has not existed since the 1980s.

There are also references to a 1988 claim by Barry Boehm that finding and fixing a software problem after delivery is often 100 times more expensive than finding it during the design phase. However, the specific cost factors used for this cost estimate are unclear and software development practices have evolved since the 1980s to be more agile.

More recently, there are reports by IBM and the Ponemon Institute on the cost of a security breach, but these reports do not include any data on the cost if security vulnerabilities are found and fixed before a security breach occurs [4].

The subcommittee observed that companies are not measuring the true cost of not being aligned to secure by design principles and that there is not an agreed upon strategy for understanding the total cost of ownership of being insecure. Despite the lack of hard numbers on the economics of early discovery of security vulnerabilities, there is general acceptance that finding them early is economically beneficial. The question is what proportion does an organization need to invest to realize that benefit?

Ideally, any software project should go through a series of automated security checks before being deployed in production. As new automated checks are added, the security bar will continue to be raised.

CISA can play a role in curating the standard security checks that should be performed. For critical infrastructure, CISA can play a role in testing these security checks and reporting on results. Many currently available security checks aim to discover instances of defects in source code but are by nature unable to find all (or even most) instances of a class of vulnerabilities. CISA could foster research and development of automated metrics of whether software conforms to Secure by Design practices and principles, such as "measuring goodness" vs "measuring badness."

The subcommittee met with the CISA legal team and the CISA assessments team and found that there are existing mechanisms that CISA can use to assess critical infrastructure and publish results. There are also a few limitations:

- CISA cannot mandate that a critical infrastructure entity undergo a cyber impact assessment.
- CISA may be able to assess a critical infrastructure entity's cyber impact, if the entity voluntarily opted in.
- CISA generally would not be able to publish assessment results without the entity's permission.

Most importantly, there are limited paths for CISA to influence budgetary decisions for entities managing critical infrastructure. CISA should be empowered to influence.

Recommendations:

- Create a study, with clear metrics, to quantify the financial impacts and customer experience impacts of companies that have survived and recovered from a large-scale security event. This should be a long-term study that captures data over a period of three to five years. It should explore:
    - The behavior of new and existing customers in response to a large-scale security event.
    - The total cost to recover from a security event over time.

- Further studies should be performed to provide empirical data to substantiate whether fixing security vulnerabilities early in the software development lifecycle is truly more cost effective. While it will likely be impossible to determine a specific dollar amount to implement secure by design principles, even providing guidance on the proportion of investment may be important to encourage organizations to start adoption.

  If it is found there is no measurable financial impact, then it may make sense to move away from using an economic rationale as a security development incentive.

- Considering CISA's aforementioned limitations, CISA should take the first steps of a multi-year effort to secure critical infrastructure.

  Design a framework and standardized "security impact study" that is lightweight, based on existing standards (such as National Institute of Standards and Technology or CISA's Secure By Design principles), and is easily consumable and executable by both technical and non-technical people. The study needs to be able to be conducted in a cost-effective manner.

  These impact studies should then be conducted on a volunteer basis, or on an opt-in basis, and offered to any organization that is part of national critical infrastructure. Results of the studies should be provided only to the organization. Aggregated/anonymized data should be published publicly by CISA on a regular basis.

Appendix 1:

The following SBD subcommittee members contributed towards this report:

- George Stathakopoulos, Chair
- Marene Allison
- Sunil Dadlani
- Brian Gragnolati
- Royal Hansen
- Matt Kehoe
- Christoph Kern
- Doug Levin
- Ciaran Martin
- Robert Scott
- Kevin Tierney
- Kiersten Todt
- Alex Tosheff
- John Viega

Appendix 2:

References:

[1] https://www.reuters.com/article/us-samsung-elec-smartphones-costs-idUSKCN12B0FX/

[2] https://www.sec.gov/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm

[3] https://investors.solarwinds.com/news/news-details/2024/SolarWinds-Celebrates-Twenty-Five-Years-of-Excellence-in-IT-Management-and-Innovation/default.aspx

[4] https://www.ibm.com/reports/data-breach