# CYBERSECRURITY

What is cybersecurity?

Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks. In a computing context, security comprises cybersecurity and physical security -- both are used by enterprises to protect against unauthorized access to data centers and other computerized systems. Information security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cybersecurity. The most frequently adopted frameworks should come as no surprise to security practitioners:

1.PCI DSS (47%)

2.ISO 27001/27002 (35%)

3.CIS Critical Security Controls (32%)

4.NIST Framework for Improving Critical Infrastructure Security (29%)

PCI DSS

Definition

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment. The PCI DSS applies to ANY organization, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data.

The PCI Data Security Standard specifies twelve requirements for compliance, organized into six logically related groups called "control objectives". The six groups are:

1.Build and Maintain a Secure Network and Systems

2.Protect Cardholder Data

3.Maintain a Vulnerability Management Program

4.Implement Strong Access Control Measures

5.Regularly Monitor and Test Networks

6.Maintain an Information Security Policy

Risk management to protect cardholder data

Under PCI DSS’s requirement 3, merchants and financial institutions are implored to protect their clients’ sensitive data with strong cryptography. Non compliant solutions will not pass the audit. A typical risk management program can be structured in 3 steps:

1.Identify all known risks and record/describe them in a risk register. For example, hardware security modules (HSM) that are used in the cryptographic key management process could potentially introduce their own risks if compromised, whether physically or logically. HSMs create a root of trust within in the system. However, while it is unlikely, if the HSM is compromised, this could compromise the entire system.

2.Develop a risk management program is to analyze all identified risks. Included in this analysis should be a mix of qualitative and quantitative techniques to determine what risk treatment methods should be used to reduce the possibility of risks. For example, an organization might analyze the risk of using a cloud HSM versus a physical device that they use onsite.

3.Treat the risks in response to the risk analysis that was previously performed. For example, employing different treatments to protect client information stored in a cloud HSM versus ensuring security both physically and logically for an onsite HSM, which could include implementing controls or obtaining insurance to maintain an acceptable level of risk.

Continuous monitoring and review are part of the process of reducing PCI DSS cryptography risks. This includes maintenance schedules and predefined escalation and recovery routines when security weaknesses are discovered.

Pros and Cons

Pros

First, merchants typically are contractually obligated to comply with the PCI DSS. Many agreements, such as card processing agreements, expressly obligate the merchant to comply with the PCI DSS as wellas card network rules, which incorporate the PCI DSS. The individual payment brands, not the council, determine any noncompliance penalties that may be assessed. Merchants risk financial penalties for noncompliance and may even lose card network privileges.

Second, PCI DSS is the first step toward complying with rapidly changing statutory requirements surrounding data privacy. For example, the Minnesota Plastic Security Card Act implements a modified version of the PCI DSS requirement that forbids entities to store certain data after the authorization of a transaction. Nevada has enacted a law that requires any data collector doing business in the state to comply specifically with the current version of the PCI DSS if the data collector accepts card payments in connection with the sale of goods or services. In these cases, companies that are already PCI DSS compliant do not have to take further action to adhere to these new laws.

PCI DSS noncompliance is a “bad fact” for a company defending a lawsuit in the wake of a data breach. While compliance does not guarantee that a company will not be liable for losses due to a breach, noncompliance will be presented by plaintiffs and noted by courts as evidence that a company breached its duty of care. The state of Washington has even codified the defense, stating that a processor, business or vendor is not liable for a data breach if it was compliant with the PCI DSS at the time of the breach.

Likewise, PCI DSS provides specific direction and recommendations to merchants, service providers and other participants in the payments ecosystem that enable them to establish at least a base set of proven measures that help protect sensitive data. However, the PCI DSS itself considers these directives and recommendations to be minimum data protection measures, so they should not be viewed as a comprehensive set of best practices covering all circumstances.

Cons

Despite the benefits discussed above, PCI DSS compliance does not guarantee protection against data breaches, nor does it insulate a company from related expenses. In fact, several major retailers have suffered significant breaches while claiming PCI DSS compliance, and little is known about the impact of PCI DSS on data breach costs. One major limitation of the PCI DSS from a merchant perspective is that compliance does not protect a merchant from investigations and fines imposed by card networks in the event of a breach. For example, Visa requires merchants that process over six million Visa transactions per year to validate PCI DSS compliance by filing an annual report on compliance prepared by a third party qualified security assessor (QSA) (or an internal auditor in some circumstances), submitting an attestation of compliance form once per year, and conducting quarterly network scans. Despite these protocols, and even where PCI certification is in effect, it may be difficult to disprove an allegation of PCI DSS noncompliance if a breach occurs.

Card network rules, such as those promulgated by Visa, do not go so far as to say that a breach is evidence that a merchant was not compliant with the PCI DSS, but they do state that a compromised merchant “must demonstrate its ability to prevent future loss, theft or compromise of Visa account or cardholder information, as specified in the ... Payment Card Industry Data Security Standard.” The Visa rules do not discuss compliance validation in the context of a data breach, implying that the validations are not dispositive, or even impactful, once a breach occurs. PCI DSS validation confirms a merchant’s compliance at a moment in time but does not tell a card network anything about the exact circumstances contributing to a data breach. In the event of a breach, card networks may, at their discretion, require an independent forensic investigation of the compromised merchant at the merchant’s expense, even though many merchants are assessed annually by third party QSAs. The forensic investigations often identify PCI DSS shortcomings that provide the basis for card networks to penalize merchants.

References

[1] Minn. Stat. § 325E.64.

[2] Nev. Rev. Stat. § 603A.215.

[3] Wash. Rev. Code § 19.255.020.

[4] Visa Inc., Visa Core Rules and Visa Product and Service Rules (Oct. 16, 2015).

[5] Visa Inc., What to Do if Compromised (September 2013), (“At Visa’s discretion, an independent

forensic investigation must be conducted by a Payment Card Industry Forensic Investigator.”)

[6] Federal Trade Commission v. LifeLock Inc., No. CV-10-00530-PHX-JJT, 2016 WL 692048 (D. Ariz. Jan. 4, 2016).

Recommendation

For companies which desire to ensure the safety of their assets are being protected, PCI DSS is a perfect choice. Merchants typically are contractually obligated to comply with the PCI DSS. However, PCI DSS compliance does not guarantee protection against data

breaches, nor does it insulate a company from related expenses, therefore, if merchants consider more about the cost of risks, PCI DSS is not recommended.

Review of other members' report

Yumeng Pan

This report discusses the reason why we need cybersecurity frameworks. She gives the examples of the cybersecurity frameworks of Yahoo and Marriott Hotel, where users information like phone-numbers, names, date of birth, even bank accounts got breaches. Then the report introduces a dynamic network security framework.

Qianqian Guo

Firstly, the report introduce the definition, components and five main processes of cybersecurity. Then it discuss the pros and cons of four main frameworks in the market. For different purposes and targeting users, these four frameworks differ from each other. For instance, PCI DSS focuses more on safety of online and offline use of credit cards.

Hanchen Zhang

After introducing the background of cybersecurity, the report discusses a specific framework, ISO/IEC. It tells the components and some main rules of ISO/IEC. In comparison with other frameworks like NIST, the report concludes the pros and cons of the framework.