Cybersecurity Frameworks

Kesha Williams

Old Dominion University

When dealing with any organization in this digital age, one has to understand that the use of cybersecurity is paramount if one wants to ensure the security of the data and systems that lie within. While it may seem that mainly large businesses face the majority of cyber-attacks, this is not the case. According to USA Today, two thirds of all cyber-attacks are directed at small businesses. This is even more unfortunate because 90% of these businesses don’t use data protection and as a result, 60% of them go out of business within 6 months of an attack. In order to combat this, there are cybersecurity frameworks that are established to ensure that these businesses, either large or small, are protected from these crippling attacks. A framework is essentially a guide that covers five function areas: Identify, Protect, Detect, Respond, and Recover. Depending on the type of business, most would choose the framework that is the most compatible and improves their cyber resilience. While there are many that are available, PCI DSS and CIS Critical Security Controls are two of the top utilized frameworks. Through knowing this, I can agree that these are excellent resources to use when having a business pertaining to retail such as Walmart or Target, however, we must weigh the pros and cons to ensure that these would be the most compatible.

As many know, a retail business conducts the sales of goods and services to consumers in small quantities for use or consumption. This can happen through multiple channels of distribution such as in store or online sales and for both channels, there needs to be some form of payment method to complete the sale. There are methods such as cash, credit, and check but depending on where you go, it can determine if a particular one is available for use or not. These days, many people use credit and this is where the PCI DSS framework comes in. This is the Payment Card Industry Data Security Standard and it handles the standards of the card payment industry to ensure the security and safety of cardholder data. These can be utilized by businesses varying in size, vendors, banks or other financial institutions, and developers of hardware and software for payment processing. The development of these standards are derived from the PCI SSC or Security Standards Council that was founded in 2006 by American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. While many would think so, the PCI SSC does not have jurisdiction over the compliance or enforcement of the framework. This would be in the hands of the payment brand or bank that is being used which is a common reason why many merchants comply with the PCI DSS because they are contractually obligated to. Through knowing this, it is easy to see that this framework has numerous benefits due to many card companies and banks making it a requirement when running a business with card transactions.

Looking at the retail industry, there are plenty of establishments that are doing well for themselves and this is most likely made possible due to the PCI DSS. This is beneficial because it give customers more opportunities to make purchases at your establishment due to not everyone has cash on them at the time. This essentially increases the amount of profit and enables you to grow the business while updating the technology and other security measures that keep transactions and other data secure. Next, this provides recommendations at a minimum level of protection. Though this can be seen as con since it doesn’t provide high level safety measures for all situations or circumstances, however, I see it as being a beneficial guide. By having a base level of protection, any business like Walmart or other retail business, can tailor their methods to fit their needs that can depend on many varying factors. On the opposite side of the spectrum, there are a few downsides to using this framework. If a business has compliance with PCI DSS, it doesn’t guarantee protection against attacks or compromise. A good example of this would be the breach that Target suffered back in September 2013 despite being compliant with this standard. Sometime after they passed the PCI compliance audit, many of the point of sale or POS systems weren’t protected from malware and they were storing 3 digit CVV codes in the system. This would probably be some of the reasoning behind the attack, but at the time, they were still somehow certified as being compliant. Nonetheless, I would still keep this as a main framework if I were to have an establishment in retail because the pros outweigh the cons.

Another important framework would be the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Security. As a result of an executive order by President Barack Obama, this was first established in 2014 by the NIST and provides guidelines and standards to manage a cybersecurity risk while having a cost effective approach of protecting critical infrastructure. It is composed of five components such as Identify, Protect, Detect, Respond, and Recover, with each function providing a means of establishing an effective form of cybersecurity management. The Identify function enables you to understand the environment that you’re in and the various risks, assets, roles and responsibilities that’s within the business. Next would be the protect tier and involves the implementation of safeguards and proper training of employees to further ensure security. Respond would consist of the plan of action in the event of a breach or attack and Recover deals with the aftermath of the attack. When in recovery, the business needs to initiate a plan in a timely fashion that reflects off the previous incident in order to avoid it happening in the future and to retain any assets that were under siege.

Similarly to the previous framework, I also feel that this would be a beneficial guide for many businesses in the retail industry. Cybersecurity risks are prevalent regardless where you are and what type of business you have, so it is important to understand and reduce these risks. This framework enables you to do that and provides a common language in managing these risks, thus making communication between businesses much easier. This is also a non-mandatory framework that gives a starting base on how to handle risks. From here, it enables the business to form a system that works best for them depending on their circumstances. Lastly, one of the top benefits of this would be the fact that it enables businesses to have a cost effective approach to improving security and reducing risks. Since it is usually the main goal of a business to increase profits, it is essential that there are methods available to be used in tandem to overall grow the business. In contrast, just as the PCI DSS, its compliance does not fully ensure the security of the business but in reality, there will likely never be a method that would provide this for anyone. As security measures adapt to the attacker’s methods, the attackers do the exact same thing.

Nonetheless, I can understand why these are two of the top frameworks available as they provide an efficient means of securing the networks and systems of businesses. While they both have their pros and cons, I can confidently say that if I were to own a business pertaining to retail or anywhere else, I would utilize these frameworks to the best of my ability. I believe the key lies in constant adaptation to your environment. When there are economic changes, social changes, attacks, and other fluctuations that can occur when conducting a business, one has to adjust accordingly to ensure that the business still can run smoothly.

References

Strauss, S. (2017, October 20). Cyber threat is huge for small businesses. Retrieved from https://www.usatoday.com/story/money/columnist/strauss/2017/10/20/cyber-threat-huge-small-businesses/782716001/

Cybersecurity Framework. (n.d.). Retrieved from https://www.us-cert.gov/ccubedvp/cybersecurity-framework

Verify PCI Compliance, Download Data Security and Credit Card Security Standards. (n.d.). Retrieved from https://www.pcisecuritystandards.org/about\_us/

Anderson, Erin. “How to Comply with the 5 Functions of the NIST Cybersecurity Framework.” Home, www.secmatters.com/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework.