Nathan Cosendine
Professor Bowman
CYSE200T
December 6 2022

Analytical Paper

Introduction(1)

The evolution of cyber-policy and infrastructure over time has had a significant impact on how businesses think and operate. Every company, big or little, uses technology, thus they must consider how to protect their resources and the data of their clients. For organizations who store personal data of their customers, such as hospitals and banks, it is expected for them to have a good cyber security plan in place to prevent this data from being stolen or altered by outside forces. The term "cyber security" describes the safeguarding against malicious attacks on an organization's computers, networks, systems, and data. These attacks can come in the form of outside hackers or from someone working inside the business.

Types of Cyber attacks

To defend against attacks, businesses must be aware of the different types of attacks and how they operate. Cyber attacks can come in the form of malware, password attacks, phishing, and many more. Malware is the umbrella term used to describe computer programs that are programmed to gain unauthorized control of a victim's computer (*Strengthen your cybersecurity*). Malware program purposes have a huge range, with some being used to monitor a victim, some steal personal or financial data, and other types such as Ransomware which holds a victims data hostage in exchange for money. Password attacks are when an attacker tries to obtain account passwords and are achieved through a variety of methods. Phishing is a type of attack in which a victim is deceived into providing information to an attacker. Phishing typically involves creating emails or websites that appear legitimate in the hopes that a target will mistake them for the authentic source. Phishing attacks are responsible for one third of all cyber attacks due to how easy they are to achieve (Stone, 2022).

As many attacks are caused by human error and can be prevented, I believe that it is vital for employees to be trained to be aware of the different types of attacks so they don't fall victim to them.

Nathan Cosendine
Professor Bowman
CYSE200T
December 6 2022

How does cybersecurity impact businesses? (6)(8)

Assuming a business is aware of the types of cyber attacks, what are some of the pros and cons of developing their own cybersecurity program? The most obvious con that every business is aware of is the cost of creating a cybersecurity program. Businesses may have to spend money to hire an outside source to create a program for them, or spend money on buying and installing more secure systems. Business's also have to think about the time and money it takes to train employees on how to use the new systems, and also making sure they are aware of the best practices they should take to keep the data and infrastructure safe.

The pros however far exceed the cons. The amount that the company spends developing a cybersecurity program can be offset by the cost of stopping cyber attacks. In the long term, preventing cyber attacks actually save the company money. The cost of data breaches has increased 10% year-over-year and is predicted to reach $10.5 trillion per year by 2025 (How much does a data breach cost? 2022). Aside from money, the business also saves losing the trust of customers who entrust their data with a company. Customers are more likely to remain loyal and stay with an organization that protects their sensitive data; this can also have the added benefit of potentially bringing in new clients.

The evolution of Cyber-policies and infrastructure and its impact on technological progress (7) (9) (10)

Due to cyber-policies and infrastructures changing every year, it is important for companies to keep looking at what they can improve on. Cyber criminals are also evolving and creating new technology as a way to extort organizations. If companies want to protect their assets the best they can, merely studying past crimes won't always help them prevent ones in the future. It is crucial for businesses to attempt to stay ahead of the development of technologies related to cybercrime. Even the largest businesses in the world, who invest millions or even billions of dollars annually in cyber security defense, are not fully immune to future attacks. This push in pull causes cyber defense and cyber attack technology to ramp up drastically in development speed.

How have small businesses been impacted by cyber security?

Cybercrime is an ever-growing concern for small businesses, cyber attacks can cost a business thousands of dollars, which is devastating for small businesses with less revenue to make up for the loss. In some cases it could cause the businesses to go bankrupt and close. By developing a cyber security program, these businesses can help protect themselves and their customer's data against threats. The first step in creating a program is to identify the risks and vulnerabilities that a business may have. The big three types of threats are environmental, business resources, and hostile actors. With these threats in mind, businesses should understand the likelihood of each of threat, and the potential harm they could have

on the business. With limited funds available, businesses can avoid spending money on unnecessary protection. Small businesses may also want to use a penetration test on themselves to further identify any weak points.

Because small businesses will have limited funds to spend on cybersecurity activities, there are things they can do without spending money, such as making sure devices are up to date, making sure devices are password locked, making sure passwords are changed regularly, ensuring a firewall is installed on the business network and on each computer system, limiting employee access to sensitive information, and installing surge protectors

Funds should be spent on ensuring that all employees are properly trained on the company's security policies and protocols. Small businesses should also invest in anti-virus programs that can detect malware and spyware, and create a response plan in case an incident is detected.

Small businesses might need outside help when creating a cyber security program. Luckily there are systems and materials in place for businesses to create a plan that best suits their needs. One of the best material resource businesses can use to get started is the NIST framework.

NIST Framework(4)(5)

NIST stands for The National Institute of Standards and Technology and was founded in 1901, the NIST is now part of the U.S. Department of Commerce (*About Nist. 2022*). The NIST created a framework for businesses to create their own cyber security plan and is a vital tool for both big and small businesses. A framework is a guideline for organizations that lays out a set of rules a business should follow to best understand and manage their cybersecurity risks. It is important to have a plan of action before a cybersecurity incident occurs to make sure an organization can mitigate damages or avoid incidents in the first place. The five core activities of NIST's Cybersecurity Framework are Identify, Protect, Detect, Respond, and Recover.

The Identify function is very important. As its name states, it is used to help an organization "identify" and understand its potential risks and assets. This function also identifies the risk management strategy, and the legal requirements for the organizations cybersecurity plan.

The Protect Function is aimed at preventing attacks before they happen. Some precautions are taken here such as maintenance of systems, implementing data security protection, and properly training employees.

The Detect Function is about discovering a cyber attack or breach as it happens as early as possible. This means making sure monitoring systems are in place and can efficiently catch any threats may they occur.

Nathan Cosendine
Professor Bowman
CYSE200T
December 6 2022

The Respond Function is the steps taken after a cyber attack has been detected. The organization should make sure the response plan is carried out. The process should aim at assessing the current damage, contain the attack to avoid future damage, and work towards eliminating the threat.

The final activity is the Recover Function. The recover function is aimed towards making the sure all the systems and services are back to working condition and have the organization back to normal.

Conclusion (11)

As technology advances, businesses must advance with it. It is essential is this day and age to have a cyber security program in every organization and can be achieved through awareness of current threats and resources like the NIST framework. Some may say that it is pointless to improve a security plan because it is a never ending struggle in developing defense technology versus hackers. I strongly disagree with this claim as cyber security plans are beneficial for both the organization and the customer.

Nathan Cosendine
Professor Bowman
CYSE200T
December 6 2022

WORKS CITED

About Nist. NIST. (2022, January 11). Retrieved December 7, 2022, from https://www.nist.gov/about-nist

Comerford, L. (2022, May 25). *Why small businesses are vulnerable to cyberattacks*. Security Magazine RSS. Retrieved December 7, 2022, from https://www.securitymagazine.com/blogs/14-security-blog/post/97694-why-small-businesses-are-vulnerable-to-cyberattacks

How much does a data breach cost? Embroker. (2022, October 5). Retrieved December 7, 2022, from https://www.embroker.com/blog/cost-of-a-data-breach/

Questions and answers. NIST. (2022, September 8). Retrieved December 7, 2022, from https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics#framework

Stone, A. (2022, October 28). *Phishing attacks are what percentage of cyber attacks?* SafeGuard Cyber. Retrieved December 7, 2022, from https://www.safeguardcyber.com/blog/security/phishing-attacks-are-what-percentage-of-cyber-attacks

Strengthen your cybersecurity. SBA. (n.d.). Retrieved December 7, 2022, from https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity

Understanding the NIST cybersecurity framework. Federal Trade Commission. (2022, October 6). Retrieved December 7, 2022, from https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework