International Journal of
Business Diplomacy and Economy

ISSN: 2833-7468
Volume 2 | No 4 | April -2023

Cybersecurity for Business

Matthew N. O. Sadiku [1], Uwakwe C. Chukwu [2], Janet O. Sadiku [3]

[1] Department of Electrical & Computer Engineering, Prairie View A&M University, Prairie View, TX USA

[2] Department of Engineering Technology, South Carolina State University, Orangeburg, SC, USA

[3] Juliana King University, Houston, TX, USA

Abstract: Cyber crime is a serious issue that affects everyone. The number of cyber threats to businesses increases daily. There are many ways which cyber criminals operate and attack businesses of all sizes. Cybersecurity is a body of technology, process, and practice designed to protect the system from cyber. Some businesses take their cyber protection lightly, do not invest in basic security measures, and find themselves victims of cyber attacks. A lot of small businesses fail to realize that hackers after them and are aware of their faulty defenses. They may think that they do not have anything worth stealing. However, small businesses have started to face the reality that they are targets, just like larger corporations. This paper is an introduction on Cybersecurity for businesses, especially for small businesses.

Key words: business, cyber attacks, cyber threats, Cybersecurity in business.

INTRODUCTION

Technology has become an indispensable necessity for business and government. Only few small businesses today can function without technology. Businesses in all sectors are being built and run on digital devices and every information and sensitive data are stored in the form of databases. Protecting these sensitive data becomes pertinent for all businesses. The major challenge for any business is to protect these data from cyberattacks [1].

Cyberattacks are now one of the most pressing issues for both large and small-scale businesses. Criminals are increasingly targeting the information stored by businesses. Businesses need to understand the importance of Cybersecurity so that they can maintain high levels of Cybersecurity to control their network resources while still achieving business goals. Cybersecurity refers to the practice of protecting systems, networks, and programs from all sorts of cyber threats. It is the protection of information and digital assets from compromise, theft or loss. Cybersecurity is important in business for the following reasons [2]:

- ✓ Increasing cyber crimes
- ✓ Use of more Internet of things devices
- ✓ Increasing technology usage
- ✓ The deep web and crypto currency
- ✓ Evolving ransom ware
- ✓ High productivity

- ✓ Sensitive data like credit card information, social security numbers, and bank account details are now held in cloud storage services.
- ✓ Cybersecurity protects your business as the whole
- ✓ It restricts spyware and adware from causing a hindrance to your business
- ✓ It saves your website from going down

OVERFVIEW ON CYBERSECURITY

Cybersecurity refers to a set of technologies and practices designed to protect networks and information from damage or unauthorized access. It is vital because governments, companies, and military organizations collect, process, and store a lot of data. As shown in Figure 1, Cybersecurity involves multiple issues related to people, process, and technology [3].

A typical cyber attack is an attempt by adversaries or cybercriminals to gain access to and modify their target's computer system or network. Cyberattacks are becoming more frequent, sophisticated, dangerous, and destructive. They are threatening the operation of businesses, banks, companies, and government networks. They vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists) [4].

The Cybersecurity is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity. A security incident is an act that threatens the confidentiality, integrity, or availability of information assets and systems [5].

- ➢ *Availability*: This refers to availability of information and ensuring that authorized parties can access the information when needed. Attacks targeting availability of service generally leads to denial of service.
- ➢ *Authenticity*: This ensures that the identity of an individual user or system is the identity claimed. This usually involves using username and password to validate the identity of the user. It may also take the form of what you have such as a driver's license, an RSA token, or a smart card.
- ➢ *Integrity*: Data integrity means information is authentic and complete. This assures that data, devices, and processes are free from tampering. Data should be free from injection, deletion, or corruption. When integrity is targeted, nonrepudiation is also affected.
- ➢ *Confidentiality*: Confidentiality ensures that measures are taken to prevent sensitive information from reaching the wrong persons. Data secrecy is important especially for privacy-sensitive data such as user personal information and meter readings.
- ➢ *Nonrepudiation*: This is an assurance of the responsibility to an action. The source should not be able to deny having sent a message, while the destination should not deny having received it. This security objective is essential for accountability and liability.

Everybody is at risk for a cyber attack. Cyberattacks vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists). The following are typical examples of cyberattacks or threats [6]:

- ➢ *Malware*: This is a malicious software or code that includes traditional computer viruses, computer worms, and Trojan horse programs. Malware can infiltrate your network through the Internet, downloads, attachments, email, social media, and other platforms. Spyware is a type of malware that collects information without the victim's knowledge.
- ➢ *Phishing*: Criminals trick victims into handing over their personal information such as online passwords, social security number, and credit card numbers.
- ➢ *Denial-of-Service Attacks*: These are designed to make a network resource unavailable to its intended users. These can prevent the user from accessing email, websites, online accounts or other services.

- *Social Engineering Attacks*: A cyber criminal attempts to trick users to disclose sensitive information. A social engineer aims to convince a user through impersonation to disclose secrets such as passwords, card numbers, or social security number.
- *Man-In-the-Middle Attack*: This is a cyber attack where a malicious attacker secretly inserts him/herself into a conversation between two parties who believe they are directly communicating with each other. A common example of man-in-the-middle attacks is eavesdropping. The goal of such an attack is to steal personal information.

Cybersecurity involves reducing the risk of cyber attacks. Cyber risks should be managed proactively by the management. Cybersecurity technologies such as firewalls are widely available [7]. Cybersecurity is the joint responsibility of all relevant stakeholders including government, business, infrastructure owners, and users. Cybersecurity experts have shown that passwords are highly vulnerable to cyber threats, compromising personal data, credit card records, and even social security numbers. Governments and international organizations play a key role in Cybersecurity issues. Securing the cyberspace is of high priority to the US Department of Homeland Security (DHS). Vendors that offer mobile security solutions include Zimperium, MobileIron Skycure, Lookout, and Wandera. Cybersecurity can benefit a business in many ways such as shown in Figure 2 [8].

CYBERSECURITY FOR SMALL BUSINESSES

Threat actors target both small and big enterprises. They know that small businesses (with less than 100 employees) are easy to get to, due to a lack of proper security system protection. Cyberattacks on small businesses have been on the rise in recent years.

Cybersecurity for small businesses should be a top priority for all organizations. The following tips will help small businesses implement Cybersecurity [9,10]:

- *Educate your employees*: Your employees are your first line of defense as well as your greatest point of vulnerability. To make your employees vigilant to cyber attacks, you need to begin with your employees' awareness. To protect your business, make sure the people that work with you are well informed on Cybersecurity issues. Educate and train your employees about cyber threats.
- *Have your network well protected:* To protect your business, have a good antivirus, have a firewall, have a threat prevention tool, and have a good ransomware encryption tool. Each of these tools is not enough, but a combination will help you reach ultimate protection.
- *Back up your data:* A backup and disaster recovery plan is crucial if you want to keep your business safe from Cybersecurity incidents. A backup solution is vital to ensure your small business cybersecurity. You can do a full backup, by taking all your information and moving it somewhere else, or an incremental backup by storing it gradually.
- *Strong passwords and two-factor authentication:* These are a must if you want to increase Cybersecurity for small businesses. Use strong passwords and regularly change them. A password manager will help your employees remember just one password to access everything they need, so they only need to remember one unique, complicated password. Common sense tips include employees should not share passwords, should not store them in unsafe and visible places, and should not let their computers unlocked while going out for a break. The two-factor authentication method is the most common multi-factor authentication method. If your employees have to access sensitive data and have to follow two steps to do it and hackers managed to compromise the first step, they still do not have access to anything, as they cannot bypass the second security step.
- *Use VPN and secure your Wi-Fi:* A VPN (a virtual private network) works like a shield on a public internet connection. It creates a private network and your employees are protected and anonymous while surfing on the internet. Also, home Wi-Fi should be encrypted and the default router password changed.

- *Implement privileged access*: By strategically assigning employees the correct level of access depending on their role and responsibilities in the organization, the overall risk of damage from a cyber attack is effectively minimized.
- *Monitoring System:* Businesses need to monitor their systems and networks on a 24/7 basis to ensure that there is no suspicious activity that may point to an attack or breach.

Some of these tips are shown in Figure 3 [9].

CHALLENGES

Even though cybercrime is getting more sophisticated, so are the solutions. As threats continue to evolve, so will ways to combat them. Cyber crime is at an all-time high, with cyber-attacks becoming more frequent. They are increasingly targeting the information stored by businesses. The damaging effects of a cyber attack are numerous and impact a company's finances, customer relations, and reputation. In this jungle of cyber attacks, one can be out of business in a wink. It will cost you a lot to recover from a cyber attack and notify all your customers. If your customers hear that your company was hit by a cyber attack because of poor security measures, they will not trust. You may lose your business as well as your customers. Your damaged reputation is hard to restore. Almost half of the people in the US would be less likely to continue doing business with companies that are breached.

CONCLUSION

In essence, Cybersecurity denotes a series of procedures and techniques to guard a business's confidential data against cyber threats and cyber crimes. It has been a major pillar for the information security framework to maintain the privacy and data consistency in ecommerce. Businesses are exposed to a growing source of risk as criminal actors, hackers, state actors and competitors. It is one of the leading business success factors today. It is a major problem for small business.

Cybersecurity has become necessary for companies of all sizes as systems possessing confidential data have become exposed to malicious attacks. Without a comprehensive Cybersecurity strategy, your organization is vulnerable to cyber criminals [11]. So you need to be ahead of hackers and start implementing businesses' Cybersecurity best practices right now. As shown in Figure 4, you must treat Cybersecurity like a business decision [12]. Cybersecurity should be a priority when you are planning your business. If you follow the best practices, your business will likely be better off. More information about Cybersecurity for business can be found in the books in [13-23].

REFERENCES

1. "Importance of Cybersecurity in business," July 2022,

   https://www.znetlive.com/blog/why-cybersecurity-is-important-for-businesses/

2. P. Dadhich, "Top 5 reasons why Cybersecurity is important for businesses," April 2022,

   https://www.znetlive.com/blog/why-cybersecurity-is-important-for-businesses/

3. "Eliminating the complexity in Cybersecurity with artificial intelligence,"

   https://www.wipro.com/cybersecurity/eliminating-the-complexity-in-cybersecurity-with-artificial-intelligence/

4. M. N. O. Sadiku, S. Alam, S. M. Musa, and C. M. Akujuobi, "A primer on cybersecurity," *International Journal of Advances in Scientific Research and Engineering*, vol. 3, no. 8, Sept. 2017, pp. 71-74.

5. M. N. O. Sadiku, M. Tembely, and S. M. Musa, "Smart grid cybersecurity," *Journal of Multidisciplinary Engineering Science and Technology*, vol. 3, no. 9, September 2016, pp.5574-5576.

6. FCC Small Biz Cyber Planning Guide,

https://transition.fcc.gov/cyber/cyberplanner.pdf

7. Y. Zhang, "Cybersecurity and reliability of electric power grids in an interdependent cyber-physical environment," *Doctoral Dissertation*, University of Toledo, 2015.
8. "How data-driven Cybersecurity can enable your business,"

   https://www.boozallen.com/markets/commercial-solutions/how-data-driven-cybersecurity-can-enable-your-business.html
9. A. Andrioaie, "Cybersecurity for small businesses. What can you do to protect your business from cyber threats? Tips and solutions on small business cybersecurity," July 2021,

   https://heimdalsecurity.com/blog/cybersecurity-for-small-businesses/
10. A. Unni, "Why Cybersecurity is important for business," February 2022,

    https://www.stickmancyber.com/cybersecurity-blog/why-cyber-security-is-important-for-business
11. P. Narasimman, "Cybersecurity for business: Importance, use cases, tips," January 2023,

    https://www.knowledgehut.com/blog/security/importance-of-cyber-security-for-business
12. "Security and risk management as an inherent part of business,"

    https://www.i-scoop.eu/cybersecurity/cybersecurity-business/
13. A. Gobeo, C. Fowler, and W. J. Buchanan. *GDPR and Cybersecurity for Business Information Systems*. CRC Press, 2022.
14. M. Christen, B. Gordijn, and M. Loi. *The ethics of cybersecurity*. Springer Nature, 2020.
15. D. Blum, *Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment*. Springer Nature, 2020.
16. S. Sacks and M. K. Li, *How Chinese Cybersecurity Standards Impact Doing Business in China*. Center for Strategic and International Studies (CSIS), 2018.
17. G. J. Touhill, and C. J. Touhill, *Cybersecurity for Executives: A Practical Guide*. John Wiley & Sons, 2014.
18. S. J. Shackelford, *Managing Cyberattacks in International Law, Business, And Relations: In Search of Cyber Peace*. Cambridge University Press, 2014.
19. J. A. Lewis, *Raising the Bar for Cybersecurity*. Center for Strategic and International Studies, 2013.
20. C. Moschovitis, *Cybersecurity Program Development for Business: The Essential Planning Guide*. Wiley, 2018
21. F . Liu et al., *Science of Cybersecurity.* Springer, 2018.
22. J. M. Kaplan et al. *Beyond Cybersecurity: Protecting Your Digital Business*. John Wiley & Sons, 2015.
23. L. Clinton, *Cybersecurity for Business: Organization-Wide Strategies to Ensure Cyber Risk Is Not Just an IT Issue*. Kogan Page, 2022.

Figure 1. Cybersecurity involves multiple issues related to people, process, and technology [3].

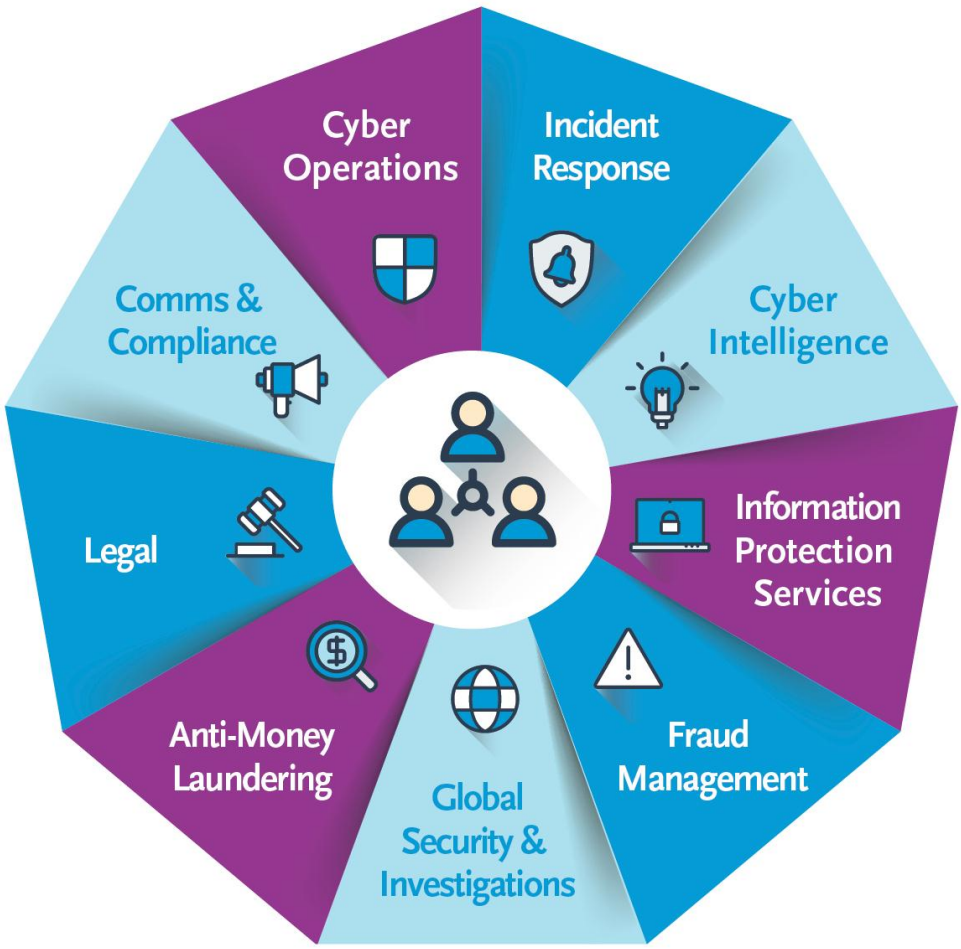

Figure 2. Cybersecurity can benefit a business in many ways [8].

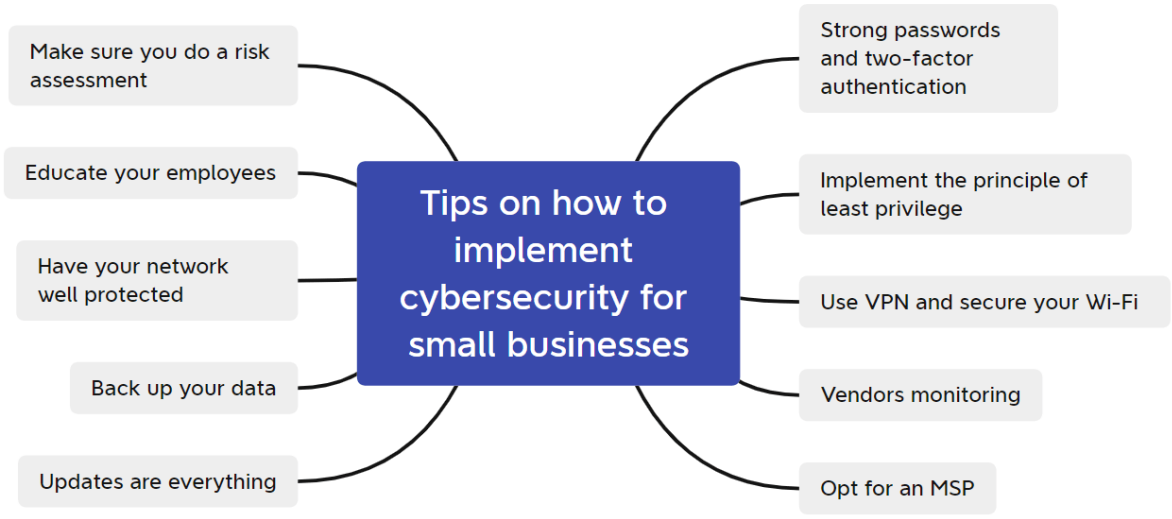

Figure 3. Some tips for implementing Cybersecurity [9].

Figure 4. Treat Cybersecurity like a business decision [12].