Cyber Security Traits of a Future-Ready Organization

Anupama Mishra[1] and Francesco COLACE[2]
[1] Swami Rama Himalayan University, Dehradun, India, (e-mail: anupamamishra@srhu.edu.in)
[2]University of Salerno, Italy. (email: fcolace@unisa.it)

ABSTRACT For the past decade, we've seen businesses and individuals who have been victimized by cybercrime. Every day we hear reports of new variations on malware and ransomware that's wreaked havoc on people's data and finances. These threats are not slowing down, but in fact increasing. While no one would argue that the business at the center of these threats is not important, it can't be your sole focus. The article discusses how to identify key traits of cyber security of a future-ready organization.

KEYWORDS cybercrime, protecting data, cyber security.

I. INTRODUCTION

Cyber security, just like physical security, it also means protecting computer systems, back end systems, and end-user applications, their users, and the data they hold from criminal activity or accidental damage. Cyber security attack is a major threat to all devices, with the most damaging attacks being those that target enterprise and government networks. IT systems and applications can be harmed or disrupted by fraudulent outsiders, as well as by cyber criminals and insider threats. Cyber security is the process of protecting your devices, networks, and data from unauthorized access, use, or interference. No business can afford to be vulnerable on the Internet. With so many ways for cyber criminals to attack, it's not a question of if you'll be targeted - it's a question of when. A business needs to have cyber security processes in place that will put them on the offensive against hackers trying to steal sensitive information [1]–[3]. Cyber security is a major concern for businesses. Failure to protect data could result in lost customers and money, as well as lawsuits and government penalties. It's no surprise that companies are investing more in cyber security now than they have before. A key step to keeping your business secure is developing a strong strategy that includes the use of technology, people, and processes. There are many cyber threats like Identity Theft, Data Theft, Unauthorized Access, DDoS, Phishing, Social Engineering Attack etc. Figure 1 shows some common attack and their percentage [4]–[6]. Some Commonly used attacks are:

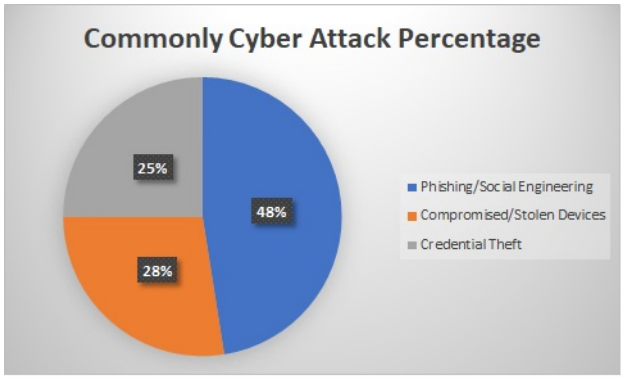

FIGURE 1: Commonly Used Cyber Attacks.

A. DDOS

A distributed denial of service (DDoS) attack is a type of cyber-attack in which the target machine is overwhelmed with messages, sometimes referred to as a Distributed Denial of Service attack.Figure 2 presents the Flow of DDoS Attack. DoS attack is a type of cooperative attack model that is more fragile and larger in scope than a general distributed attack model (DDoS) [7]–[10]. Attackers use a large number of puppet machines under their control to launch denial of service (DoS) attacks on a single target at the same time. Eventually, the system resources or network bandwidth are depleted, and the system may even fail completely [11]–[14]. Globally, distributed denial of service (DDoS) has become a deadly, widespread, and rapidly evolving threat. Currently, the most common attack vectors are UDP flood, HTTP flood, SYN flood, ICMP flood, DNS flood, and others, all of which pose a serious threat to both systems and networks.

B. PHISHING

Phishing is a method of obtaining sensitive information such as usernames and passwords, without the user being aware that this is happening [15]–[18]. The term comes from the English verb "to fish", which is defined as to catch prey by

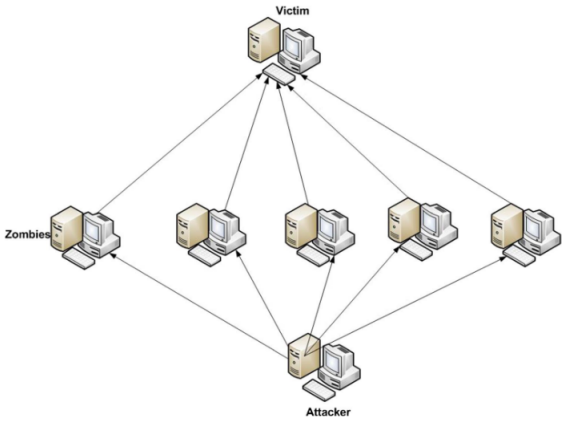

FIGURE 2: Distributed Denial of Service Attack

using a hook and line. The attacker creates a bogus email that looks as though it's sent from a bank or another institution asking for personal information. Phishing is when people use fraudulent tactics to obtain personal information from unsuspecting users [19]–[22]. Cross Site Scripting Cross site scripting is a type of attack in which an attacker injects malicious code on a website that causes unintended harmful effects when the script is executed. It can be used to steal information from users and change their data [18], [23], [24]. The most common way to perform cross-site scripting is by using HTML forms that are vulnerable to invalid input. Another way is by using other methods to attack a site like SQL injection, or performing XSS in JavaScript, CSS or Flash objects.

This article is written to warn about the dangers of a cyber security attack and how easy it can be for hackers to get into your computer. For instance, there's a new type of ransomware called crypto-jacking that takes over computer's processing power in order to mine for crypto currency, like bitcoin. This will slow down your computer and can sometimes cause it to crash.

II. POSSIBLE CONSEQUENCES OF BEING HACKED

A cyber security attack is a major threat for companies of all sizes. Individuals can also be hacked and consequently lose their identity, privacy, or even money [1], [25]–[27] . It is difficult to prevent an attack because it is hard to know how it will happen. However, there are some things you can do to protect your privacy such as changing passwords regularly and deleting old data. A cyber security attack is a major threat for companies of all sizes. Individuals can also be hacked and consequently lose their identity, privacy, or even money. It is difficult to prevent an attack because it is hard to know how it will happen. However, there are some things you can do to protect your privacy such as changing passwords regularly and deleting old data.

III. THE 3 KEY COMPONENTS OF A SUCCESSFUL CYBER SECURITY STRATEGY

To fight with the insider threats as well as outsiders threats, the organizations need to focus on the three important components as strategy, Training and Retaining the technical talented members who helped to make secure the organization. Figure 3 presents the vital three components of popular cyber attacks [28]–[31]. The Components are:

Strategy - The cyber security team should develop an effective strategy to combat the most common threats that are encountered.

Training - The team should be trained on the latest trends and on the defenses available to them.

Personnel - Recruiting and retaining talented members is key for any organization's success.

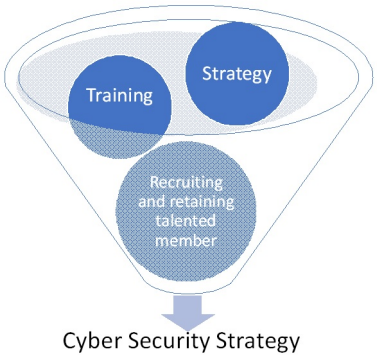

FIGURE 3: Three Key Components of a Cyber Security Strategy.

IV. KNOWING YOUR ENEMY: IDENTIFYING POTENTIAL RISKS

Cyber security risks can be difficult to anticipate, but that doesn't mean you should ignore them. You need to take the time and assess your company's vulnerabilities and then determine how you can reduce those risks [32], [33]. Sometimes the following signs are needed to be watched out [34], [35]:

-The employees use traditional passwords that are easy to remember or share.

-Don't regularly install software updates.

-Using an unsecured wireless network.

-The employees work remotely but there is no mobile security solution to protect their devices while they're away from the office.

Start by taking a look at your employees, clients, and other vendors in order to assess their vulnerability factors. We can identify potential risk by doing the followings:

-Reduce the scope of your project by breaking it into manageable components.

-Ask for help from a knowledgeable and technically expert person.

-Investigate both internally and externally to identify the risk

and threats.
-Consistently solicit the opinions of your workers
-Investigate any complaints and feedback received from clients.
-The modern tools can be used for the same.

V. PROTECTING YOUR DATA: IMPLEMENTING SECURITY MEASURES

Cyber security is one of the most important processes in an organization, since it guards data from potential threats and other personal information. With cyber security becoming more and more common, it's important to understand what makes a company secure from fraudulent activities. Cyber attacks have become more common in the past few years. Each year, an average of 1 billion cyber attacks occur worldwide. Recently, technology has been used to defend cyber-attacks in order to protect against them. When attacks are not successful, the victim's computer can automatically notify the user and the companies that the attack is occurring [**?**], [36]–[38]. The cyber security software also allows you to set up a custom firewall for your computer. Cyber security professionals use a variety of technology to safeguard the networks that their organizations rely on for work. One way that cyber security professionals protect their networks by using encryption. Encryption scrambles data so that it's unreadable by anyone except those with the key, like cyber security professionals. There are many technology and algorithms are being used to defend from the cyber attacks [39]–[41].

VI. TECHNIQUES USED FOR DEFENSIVE MECHANISM AGAINST CYBER ATTACK

There are plenty of mechanisms are being used to protect our cyber space such as Statistical methods, Machine Learning, Intrusion Detection/Prevention Systems [42]–[45] etc.

-Statistical Methods:There are so many statistical techniques, and based on the quality of data, it can be applied to analyse that when the system needs to send alert messages or take decisions for starting the prevention.Data science techniques are being developed by the statistical cyber-security group, which will allow large dynamic computer networks to detect intrusions and anomalous behaviour, and thus protect against cyber-attacks and fraudulent activity.

-Machine learning:Machine learning is a process of creating models and algorithms using data collected from sets of previously analyzed inputs, by using algorithms that analyze data in order to make predictions or decisions. As the use of machine learning increases in many different industries, the world of defensive mechanism design will be no different. In fact,many researchers and developer using machine learning to help designers make their products more secure. The models that they are creating are able to design an effective locking mechanism by being trained on millions of images and videos of how people pick or try to pick locks.

-Intrusion Detection Systems(IDS): A basic Intrusion Detection System can detect whether a person is in a room and give audio or visual warnings of their presence. [46]–[51] The more advanced versions can monitor activity on cameras, doorways, and even tell when an intruder's fingerprints are present.When suspicious activity is detected in network traffic, an IDS is activated, and an alert is sent to the system's administrator. When a malicious activity or policy violation is detected, it is detected by a software application that scans the network or the system. Any malicious venture or violation is typically reported to an administrator, or data is collected centrally using a security information and event management system, depending on the circumstances. [52], [53] As a response from multiple sources are integrated, and alarm filtering techniques are used to distinguish between malicious activity and false alarms.

VII. CONCLUSION

From a cyber security perspective, organizations should maintain a constant awareness of the threat landscape and ensure that their IT systems are up-to-date. They should also have a plan in place that is predicated on risk assessments and management strategies to reduce their risk. Cyber security is a challenge for all organizations. Understanding the full scope of your cyber risk and implementing strategies to mitigate these risks from an earlier point in time will ensure that you are able to better protect your business interests.

REFERENCES

[1] B. B. Gupta and et al., "Handbook of computer networks and cyber security," Springer, vol. 10, pp. 978–3, 2020.
[2] N. A. Khan, S. N. Brohi, and N. Zaman, "Ten deadly cyber security threats amid covid-19 pandemic," 2020.
[3] M. R. Sri, S. Prakash, and T. Karuna, "Classification of fungi microscopic images–leveraging the use of ai," 2021.
[4] B. B. Gupta and Q. Z. Sheng, Machine learning for computer and cyber security: principle, algorithms, and practices. CRC Press, 2019.
[5] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," Journal of Cyber Security and Mobility, pp. 65–88, 2015.
[6] A. Dahiya and et al., "How iot is making ddos attacks more dangerous," 2021.
[7] A. Mishra and et al., "Defense mechanisms against ddos attack based on entropy in sdn-cloud using pox controller," Telecommunication systems, vol. 77, no. 1, pp. 47–62, 2021.
[8] S. Gupta and et al., "Detection, avoidance, and attack pattern mechanisms in modern web application vulnerabilities: Present and future challenges," International Journal of Cloud Applications and Computing (IJCAC), vol. 7, pp. 1–43, 05 2017.
[9] M. Chhabra and et al., "A novel solution to handle ddos attack in manet," 2013.
[10] S. Gupta and et al., "Php-sensor: a prototype method to discover workflow violation and xss vulnerabilities in php web applications," in Proceedings of the 12th ACM international conference on computing frontiers, 2015, pp. 1–8.
[11] A. Gaurav and et al., "A novel approach for ddos attacks detection in covid-19 scenario for small entrepreneurs," Technological Forecasting and Social Change, p. 121554, 2022.

[12] A. Khan and et al., "Future scope of machine learning and ai in 2022," Future, 2021.

[13] F. Mirsadeghi and et al., "A trust infrastructure based authentication method for clustered vehicular ad hoc networks," Peer-to-Peer Networking and Applications, vol. 14, no. 4, pp. 2537–2553, 2021.

[14] M. Al-Ayyoub and et al., "Accelerating 3d medical volume segmentation using gpus," Multimedia Tools and Applications, vol. 77, no. 4, pp. 4939–4958, 2018.

[15] A. K. Jain and et al., "A survey of phishing attack techniques, defence mechanisms and open research challenges," Enterprise Information Systems, pp. 1–39, 2021.

[16] K. Yadav, "Blockchain for iot security," 2021.

[17] P. Negi and et al., "Enhanced cbf packet filtering method to detect ddos attack in cloud computing environment," arXiv preprint arXiv:1304.7073, 2013.

[18] A. Almomani and et al., "Phishing dynamic evolving neural fuzzy framework for online detection zero-day phishing email," arXiv preprint arXiv:1302.0629, 2013.

[19] B. B. Gupta and et al., "Artificial intelligence empowered emails classifier for internet of things based systems in industry 4.0," Wireless networks, pp. 1–11, 2021.

[20] B. B. Gupta and et al., "Enhancing the browser-side context-aware sanitization of suspicious html5 code for halting the dom-based xss vulnerabilities in cloud," International Journal of Cloud Applications and Computing (IJCAC), vol. 7, no. 1, pp. 1–31, 2017.

[21] A. M. Manasrah and et al., "An optimized service broker routing policy based on differential evolution algorithm in fog/cloud environment," Cluster Computing, vol. 22, no. 1, pp. 1639–1653, 2019.

[22] I. Cvitić and et al., "Ensemble machine learning approach for classification of iot devices in smart home," International Journal of Machine Learning and Cybernetics, vol. 12, no. 11, pp. 3179–3202, 2021.

[23] P. e. a. Chaudhary, "Shielding smart home iot devices against adverse effects of xss using ai model," in 2021 IEEE International Conference on Consumer Electronics (ICCE). IEEE, 2021, pp. 1–5.

[24] S. Tripathi and et al., "Hadoop based defense solution to handle distributed denial of service (ddos) attacks," 2013.

[25] M. Zwilling and et al., "Cyber security awareness, knowledge and behavior: A comparative study," Journal of Computer Information Systems, vol. 62, no. 1, pp. 82–97, 2022.

[26] B. B. Gupta and et al., "An isp level solution to combat ddos attacks using combined statistical based approach," arXiv preprint arXiv:1203.2400, 2012.

[27] B. Gupta and et al., "Cross-site scripting (xss) abuse and defense: exploitation on several testing bed environments and its defense," Journal of Information Privacy and Security, vol. 11, no. 2, pp. 118–136, 2015.

[28] I. A. Elgendy and et al., "Joint computation offloading and task caching for multi-user and multi-task mec systems: reinforcement learning-based algorithms," Wireless Networks, vol. 27, no. 3, pp. 2023–2038, 2021.

[29] A. Mishra and et al., "A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques," in 2011 European Intelligence and Security Informatics Conference. IEEE, 2011, pp. 286–289.

[30] A. K. Jain and et al., "Phish-safe: Url features-based phishing detection system using machine learning," in Cyber Security. Springer, 2018, pp. 467–474.

[31] A. Tewari and et al., "A lightweight mutual authentication protocol based on elliptic curve cryptography for iot devices," International Journal of Advanced Intelligence Paradigms, vol. 9, no. 2-3, pp. 111–121, 2017.

[32] G. Tsochev and et al., "Analysis of threats to a university network using open source technologies," in 2021 International Conference Automatics and Informatics (ICAI). IEEE, pp. 366–369.

[33] A. Bhardwaj and K. Kaushik, "Predictive analytics-based cybersecurity framework for cloud infrastructure," International Journal of Cloud Applications and Computing (IJCAC), vol. 12, no. 1, pp. 1–20, 2022.

[34] G. I. Shidaganti and et al., "Scef: a model for prevention of ddos attacks from the cloud," International Journal of Cloud Applications and Computing (IJCAC), vol. 10, no. 3, pp. 67–80, 2020.

[35] A. Gaurav and et al., "Security of cloud-based medical internet of things (miots): A survey," International Journal of Software Science and Computational Intelligence (IJSSCI), vol. 14, no. 1, pp. 1–16, 2022.

[36] J. M. Couretas, "Measures of cyber performance and effectiveness," in An Introduction to Cyber Analysis and Targeting. Springer, 2022, pp. 197–219.

[37] J. Lu and et al., "Blockchain-based secure data storage protocol for sensors in the industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 18, no. 8, pp. 5422–5431, 2021.

[38] B. B. Gupta and et al., "Phishing attack detection using a search engine and heuristics-based technique," Journal of Information Technology Research (JITR), vol. 13, no. 2, pp. 94–109, 2020.

[39] S. Gupta and et al., "Js-san: defense mechanism for html5-based web applications against javascript code injection vulnerabilities," Security and Communication Networks, vol. 9, no. 11, pp. 1477–1495, 2016.

[40] B. B. Gupta and et al., Smart Card Security: Applications, Attacks, and Countermeasures. CRC Press, 2019.

[41] R. Kumar and et al., "Stepping stone detection techniques: Classification and state-of-the-art," in Proceedings of the international conference on recent cognizance in wireless communication & image processing. Springer, 2016, pp. 523–533.

[42] S. R. Sahoo and et al., "Hybrid approach for detection of malicious profiles in twitter," Computers Electrical Engineering, vol. 76, pp. 65–81, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790618322766

[43] B. B. Gupta and et al., A Beginner's Guide to Internet of Things Security: Attacks, Applications, Authentication, and Fundamentals. CRC Press, 2020.

[44] A. Tewari and et al., "A lightweight mutual authentication approach for rfid tags in iot devices," International Journal of Networking and Virtual Organisations, vol. 18, no. 2, pp. 97–111, 2018.

[45] P. Gulihar and et al., "Cooperative mechanisms for defending distributed denial of service (ddos) attacks," in Handbook of Computer Networks and Cyber Security. Springer, 2020, pp. 421–443.

[46] Z. Zhou and et al., "A statistical approach to secure health care services from ddos attacks during covid-19 pandemic," Neural Computing and Applications, pp. 1–14, 2021.

[47] J. Peng and et al., "A biometric cryptosystem scheme based on random projection and neural network," Soft Computing, vol. 25, no. 11, pp. 7657–7670, 2021.

[48] A. Mishra and et al., "Intelligent phishing detection system using similarity matching algorithms," International Journal of Information and Communication Technology, vol. 12, no. 1-2, pp. 51–73, 2018.

[49] A. P. Pljonkin and et al., "Features of detection of a single-photon pulse at synchronisation in quantum key distribution systems," in 2017 6th International Conference on Informatics, Electronics and Vision & 2017 7th International Symposium in Computational Medical and Health Technology (ICIEV-ISCMHT). IEEE, 2017, pp. 1–5.

[50] A. Gaurav and et al., "Ddos attack detection in vehicular ad-hoc network (vanet) for 5g networks," in Security and Privacy Preserving for IoT and 5G Networks. Springer, 2022, pp. 263–278.

[51] B. B. Gupta and et al., "Identity-based authentication mechanism for secure information sharing in the maritime transport system," IEEE Transactions on Intelligent Transportation Systems, 2021.

[52] Z. Zhou and et al., "Coverless information hiding based on probability graph learning for secure communication in iot environment," IEEE Internet of Things Journal, 2021.

[53] B. B. Gupta and et al., "Soft computing techniques for big data and cloud computing," pp. 5483–5484, 2020.