THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Advancement of Cybersecurity Threat in Business

Obotivere Benjamin Akpojohwovwo

Chief Technologist, Department of Computer Science,
Delta State Polytechnic Oghara, Delta State, Nigeria

Enomate Joseph O

Chief Technologist, Department of Electrical/Electroninn,
Delta State Polytechnic Oghara, Nigeria

Abstract:

The ever-evolving digital age affects cybersecurity more than most people realize. The rate of cybercrimes and cyberthreats has grown exponentially and are consistent with the growth of technology. As technology expands and develops, so do the cybercrimes and cyberthreats that is committed. Fortunately, as technology has advanced, so has the ability to seek out cybercrimes and cyberthreats before they happen and protect people when they occur. This paper provides a list of best practices for businesses to help protect against cyberthreats. The study highlights an overview of expanding cybersecurity threat and the measures companies are employing to mitigate the risk for companies and individuals.

Keywords: Cybersecurity, cyberthreat, cybercrime, technology, digital age

1. Introduction

The internet has made the world smaller in many ways but it has also opened us up to influences that have never before been so varied and so challenging. As fast as security grew, the hacking world grew faster. There are two ways of looking at the issue of cyber security. One is that the companies that provide cloud computing do that and only that so these companies will be extremely well secured with the latest in cutting edge encryption technology. The process of enhancing cyber-security can also be referred to as information technology security or electronic information security. Andreea (2015) asserted that in a world driven more and more by big data, social networks, online transactions, information stored or managed through internet and automated processes performed through the use of IT systems, information security and data privacy are permanently facing risks. Ibikunle and Eweniyi (2013) defined cyber security as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Cyber-security is the body of rules put in place for the protection of the cyber space. But as we become more dependent on cyberspace, we undoubtedly face new risks. Sophisticated cyber criminals and nation-states, among others, present risk to our economy and national security. Cyber Security could be explained further as the body of technology, processes, and practices designed to protect networks, computers, programs and data from attacks, damage, or unauthorized access. (Dambo et al., 2017). Cybersecurity also relate to human factor as it is about technology. A recent survey of 165,000 U.S. workers by the Corporate Executive Board found that 93 percent of them knowingly violate policies designed to prevent data breaches. The survey also found that senior executives are the worst offenders. Another source of risk is former employees at all levels who may have the knowledge and the will to break into or encourage others to break into company systems. It is important to note that finding ways to raise awareness within organizations is crucial (Biosvert, 2014).

2. Cybersecurity

The word cybersecurity is concerned with making cyberspace safe from threats, namely cyber-threats. The notion of 'cyber-threats' is rather vague and implies the malicious use of information and communication technologies (ICT) either as a target or as a tool by a wide range of malevolent actors. According to Rec. ITU-T X.1205, cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Ang-Jaccard and Nepal (2014) added that cybersecurity involves the understanding of surrounding issues of diverse cyber-attacks and devising defense strategies (that is, counter measures) that preserve confidentiality, integrity and availability of any digital and information technologies.

- Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems.
- Integrity is the term used to prevent any modification/deletion in an unauthorized manner.

- Availability is the term used to assure that the systems responsible for delivering, storing and processing information are accessible when needed and by those who need them.

2.1. Cyber-Security Threats

A cyber security threat can be described as pertaining to anything that has the potential to influence or bring serious harm to a computer system. It is capable of causing serious damage to computer systems or servers. Abi (2020) explained the concept of cyber security threat as a malicious act that seeks to damage data, steal data, or disrupt digital life in general. He added that cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks and other attack vectors.

2.1.1. Categories of Cyber Security Threat

Obviously, there are a wide range of threats that have being detected across many platforms and devices. There is also wide range of attackers, from highly-organized criminal enterprises to individual cyber-criminals to 'hacktivists' (that is, politically motivated actors) to state-sponsored groups. The various types of threats and motivations make businesses task of identifying threats and developing protections an increasing challenge and drives its focus on the attackers' tactics, techniques, and procedures (TTP). Therefore, there is a need to understand the various attackers for effective defenses against them. McGuire (2015), classify cyber security threats into categories including data breaches, mobile and social, ransomware, cyber-espionage and internet of things.

2.1.1.1. Data Breaches

There are more than 550 million identities which were exposed due to data breaches in 2013, and Symantec expects this number to soon exceed 1 billion, which is equivalent to nearly 1 out of every 7 people on the planet, or about 1 in 3 Internet users. And, data breaches are becoming increasingly broad: intellectual property, trade agreements, and business agreements, are often now the target, not just credit card data, and so on.

2.1.1.2. Ransomware

This is a type of malware that involves an attacker locking the victim's computer system files typically through encryption and demanding a payment to decrypt and unlock them. Ransomware is becoming increasingly prevalent: Symantec observed a 500% month-on-month increase in ransomware in 2013.

2.1.1.3. Cyber-espionage

It is the practice of using information technology to obtain secret information without permission from its owners or holders. It is the most often used to gain strategic, economic, military advantage, and is conducted using cracking techniques and malware.

2.1.1.4. Mobile and Social

This is a key area where threats are proliferating and where social engineering is carried out (that is, attackers gather personal data about persons of interest via social networks and then use it to make targeted emails more convincing).

2.1.1.5. Internet of Things

The internet of Things (IoT) is an extension of the internet into the physical world for interaction with physical entities from the surrounding. Innovation in this area is happening very quickly, but the security is a step behind. Symantec believes that, to be effective, security must be built into products as they are being developed, not 'bolted on' later.

Figure 1

Source: Tim Review_march 2015_TIMLS_MCGuire_Slide.pdf

2.2. Effect of Cyber Security Threat

In view of the effects of cyber security threat, Seemma (2018) stated that cyber-attacks will cause more damage financially and reputational even to the most withstand organization. The organization which suffers cyber-attack, have to face the losing assets, business reputation and potentially the organization have to face regulatory fines and taking legal action and the costs of remediation. He added that the result of a survey taken by UK government about cyber security in 2017, found that the average cost for a large business is £19,600 and for a small to medium-sized business is £1,570. Hetram and Shashant (2014) stipulated the following as associated effect of cyber security threats:

- Economic: All types of attacks result into loss to the economy of an organization.
- Reputational: when a company faces a cyber-attack, it decreases the trust and faith among the people and people afraid to invest further in the organization.
- Loss of IP: Sometimes the Intellectual Property of an organization like patent, copyright trade secret is theft which causes a huge loss.
- Loss of sensitive business information: The data that has value in worth of money should be preserve but loss of such data harm to the organization as it can be used by the competitors.
- Lack of Trust: Once an organization faces a cyber-attack then customers does not feel safe with that organization. It compels its customers to move on other services.

2.2.1. Remedies and Best Practices for Businesses to Protect Against Cyber Threat

Finally, McGuire provided a list of best practices for businesses to help protect against cyber-threats:

- Employ defense-in-depth strategies
- Monitor for network incursion attempts and vulnerabilities
- Antivirus on endpoints is not enough
- Secure websites against man-in-the-middle attacks
- Protect private keys
- Use encryption to protect sensitive data
- Ensure all devices on company networks have security protections
- Implement a removable media policy
- Be aggressive with updating and patching
- Enforce an effective password policy
- Ensure regular backups are available
- Restrict email attachments
- Ensure an infection and incident response procedure is in place
- Educate users on basic security protocols

3. Conclusion

Cybersecurity is a threat to all enterprises or businesses. The only proven tools available for overcoming this grave challenge are information-sharing and investments in mitigation technologies that are rooted in a broader risk-management framework. The objective of this study is to increase your awareness of the various types of cyberthreats and to lay the foundation for your company's cybersecurity plan. Taking into account the objectives of a cyberattack and some of the best practices used to execute them, a small business' cybersecurity plan should address physical, network, and data security.

4. References

- i. Abi, T. T. (2020). What is a Cyber Threat? 2020 UpGuard, Inc. Retrieved from <http://www.upguard.com/blog/cyber-threat>
- ii. Andreea, B. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *7th International Conference on Financial Criminology 2015*, Procedia Economics and Finance.28(2015): 24 – 31
- iii. Biosvert, R. (2014). What every CEO needs to know about Cybersecurity: A Background Paper. Retrieved from 04, 2014.
- iv. Dambo, I. Ezimora, O. A., & Nwanyanwu, M. (2017). Cyber Space Technology: Cyber Crime, Cyber Security and Models of Cyber Solution. *International Journal of Computer Science and Mobile Computing (IJCSMC)*, 6(11): 94-113
- v. Dunn, M. (2015). A Comparative Analysis of Cybersecurity Initiatives Worldwide. *WSIS Thematic Meeting on Cybersecurity*, Retrieved June 10, 2015.
- vi. Hetram, Y. & Shashant, G. (2014). Cyber Attacks: An impact on Economy to an organization. *International Journal of Information & Computation Technology*,4 (9): 937-940
- vii. Ibikunle, F. & Eweniyi, O. (2013). Approach to Cyber-Security Issues in Nigeria: Challenges and Solution. *International Journal of Cognitive Research in Science, Engineering and Education*,1(1): 2013
- viii. Jang, J., & Nepal, S. (2014). A Survey of emerging threats. *Journal of Computer and System Sciences*. 80(5): 973-993.
- ix. McGuire, C. F., (2015).TIM Lecture Series - The Expanding Cybersecurity Threat. *Technology Innovation Management Review*, 5(3): 46-48.Retrieved from<http://timreview.ca/article/881>

- x. McGuire, C. F., (2015). The Expanding Cybersecurity Threat. *2015 Symantec Corporation. Retrieved from http://TimReview_March2015_TIMLS_MCGuire_Slide.Pdf*
- xi. Recommendation ITU-TX.1205 (04/2008), Overview of Cyber Security.
- xii. Seemma, P.S., Nandhini, S. & Sowmiya, M. (2018). Overview of Cyber Security. *International Journal of Advanced Research in Computer and Communication Engineering(IJARCCCE)*,7(11): (2018)