International Journal of Information and Communication Sciences
2020; 5(2): 12-16
http://www.sciencepublishinggroup.com/j/ijics
doi: 10.11648/j.ijics.20200502.12
ISSN: 2575-1700 (Print); ISSN: 2575-1719 (Online)

Emerging Cyber Security Threats in Organization

Hailye Tekleselase Woldemichael

Department of Information Systems, School of Informatics, Addis Ababa University, Addis Ababa, Ethiopia

Email address:
hailye83@gmail.com

To cite this article:
Hailye Tekleselase Woldemichael. Emerging Cyber Security Threats in Organization. *International Journal of Information and Communication Sciences*. Vol. 5, No. 2, 2020, pp. 12-16. doi: 10.11648/j.ijics.20200502.12

Received: December 27, 2019; **Accepted**: April 29, 2020; **Published**: August 27, 2020

Abstract: Background Cyber-security is a preventive preparation of protecting sensitive information, information systems, computers, servers, critical infrastructure, mobile devices, and computer networks from unauthorized access or hackers. Now a day digital technology takes the most significant role in growth effectiveness and efficiency in the organization. However, new technologies like mobile technologies (5G), IoT and cloud computing are Coming with new information security threats. Study design qualitative, survey, case study and an in-depth literature review were conducted. Employees still using the old software, they didn't update the software (operating system), they use a permanent password, they are still using weak and default password (Wife name or her phone number) information security literacy and behavior end users or IT staff. They don't have awareness about proactive cyber-attacks prevention policies and procedures. Because they have not took short and long term training on most serious cyber-attacks like ransom ware, social engineering, malware, DDoS, and phishing. This study aims to assess the most common and emerging cyber security threats. That the organizations are facing. The main objective of these investigations is to create awareness about the emerging and the most serious cyber-attacks occurring in the organization. The findings/results demonstrate that cyber security preparations and trained employees are very low; hackers becoming more sophisticated. Conclusion based the findings we conclude that cyber security protection using current method is not sufficient; employees have no idea about security threats due to lack of awareness and training.

Keywords: Cyber Security, Sensitive Information, Threats, Information Security

1. Introduction

"Cyber security is information system management by individuals or organizations to manage end-users' security behaviors, on the basis of personal perceived behaviors toward potential security breach in work and non-work environment." Information security can't be achieved through technology alone, it also includes the use of procedures, policy and people. Also, it needs identify who the attackers are, what their inspirations are, where the vulnerabilities lie, and how prevented the systems are [1].

By the growth of technologies of internet of things (IoT) and cloud computing, surrounded employees and organizations have greatly transformed. Cyber security is one of the serious issues in organizations. Complementary the spiteful benefits of technologies, security attacks and deliberate misconduct reason great suffering to people [1]. A 'Cyber Security Breaches Survey 2018' revealed that over four in ten (43%) businesses and two in ten (19%) charities in the UK suffered a cyber-attack. The survey found that 38% of small businesses had spent nothing at all to protect themselves from cyber security threats. Information security consciousness is about ensuring that all personnel are aware of the rules and regulations regarding securing the information within organization [2].

2. Objective

The main objective of this study is to examine evolving cyber security threats, awareness creation, to show an effective methods to protect our self and organization from cyber-attacks.

Methodology

3. Research Design

A qualitative (interview), survey, case study, and an in-depth literature review approach were used. Survey direct observation and experiment using wire shark and snort

network monitoring (security) tools was conducted in sample organizations. Interview related to employees' knowledge and attitudes towards information security and on cyber-attacks.

4. Literature Review

25+ million records exposed every day in 2018; 300 billion passwords will be generated by 2020 60% of frauds originate form mobile devices 90% of hackers use encryption Healthcare ransom ware attacks will quadruple Personal data is chap (SANS 2019). From at least in or about 2017, up to and including at least about in or about September 28, 2018, LIRIANO misused administrative access provided to him as an information technology employee at a New York City-area hospital ("Hospital-1"), to log in to employee accounts, and copy other employees' personal documents, including tax records, and personal photographs onto his own workspace computer for his own personal use.

Fraudulent emails designed to make recipients hand over sensitive information, extort money or trigger malware installation on shore-based or vessel IT networks remains one of the biggest day-to-day cyber threats facing the maritime industry. These threats often carry a financial liability to one or all those involved in the maritime transportation supply chain.

CIA triad

Confidentially asserts authorized part can access the information Example military secret. Integrity Authorized people can add, remove or alter the information. Availability Information must be available on demand

CIA Model

The CIA model defines the three significant aims of cyber security. The C stands for confidentiality, I for integrity, A stand for availability. Cyber security wants privacy in data and information. End user, devices, should be acceptable from accessing data and information, like username, password, credit card medical records, etc. Confidentiality is worried with watching of data or information because if unauthorized people access data or information they are not legal [3].

5. Results and Discussion

Peace State Minister Zeynu Jemal said on his part "we have reached a point when individuals and institutions are widely exposed to global cyber-attacks." Since cyber security is new to Ethiopia and needs many trained human resource, the government is ready to provide all the necessary inputs and technological supports to tackle cyber-attacks, he stressed. Yet Zeynu urged all stakeholders to collaborate in fighting cyber-attack by considering its nature of complexity. The world has lost 1.5 trillion USD in 2018 due to cyber-attacks. The world is also predicted to loss 6 trillion USD by 2021.

Ethiopia needs to develop a well-organized legal framework to tackle the ever-increasing cyber-attacks at the national level, Cyber Expert said. An expert on cyber security, Dr. Henok Mulugeta, told ENA that currently Ethiopia has no organized system to tackle cyber-attacks. Countries even which have well organized technologies are exposed for the global cyber-attacks due to the complexity of its nature, he said. Cyber-attacks have increased from 479, 576 to 791 per annum during the past three successive years in Ethiopia, of which 15 percent of the attacks during the last nine months of 2018/19 were cyber hacking attempts.

About 87.4 percent of the government institutions have not any recognized legal frameworks to tackle cyber-attacks though some 11.6 percent are being at their trial level. There is no well-developed and governed legal framework at the national level.

Henok urged the country to act swiftly in collaborative manner as cyber security needs governance and management from the highest to the lowest level. Referring to a study, Head of Cyber Engineering at Information Network Security Agency (INSA), Tigst Hamid said that most of the attacks observed during the concluded Ethiopian fiscal year were web and infrastructural attacks. Sources of cyber-attacks are employees, partners, well organized criminal, cyber terrorists and government and non-government sponsored.

> *"Apart from lack of legal frameworks, lack of awareness on cyber security, lack of well-trained human resources and there is poor cyber security governance at the institutional level. Head of Cyber Governance and Management at INSA, Temesgen Kitaw said for his part that considering the legal frameworks which other countries have been developed, Ethiopia has much to do."*

According to the agency, websites are the majority of the cyber-attacks followed by key infrastructure facilities. The agency were able to prevent the attacks without causing serious damages, said Abrham Gebretsadik, emergency preparedness and response division head at the agency. Ethiopia is currently on a drive to upgrade its largely traditional basic services infrastructure and government bureaucracy, using cyber technology as a key component. Ethiopian Prime Minister Abiy Ahmed, who was previously head of INSA has since assuming office in April 2018, engaged on an ambitious drive to introduce cyber technology across all public and private sectors.

Emerging cyber security threats we should take very seriously

Phishing

Phishing can be well-defined as "…the fake practice of transferring emails asserting to be from reliable (legal) companies in order to persuade individuals to disclose personal information such as passwords and credit card numbers" (Oxford Online Dictionary). This ensued to most Ethiopians are incapable to recognize phishing emails because no training is given to create awareness. The innovative inform in the news newly is about ransom ware attack called 'WannaCrypt'. Ransom ware is a kind of spiteful software planned to block access to a computer system until an amount of money is paid. A year ago, malware was normally apparent to be the highest threat

facing companies. As we approach 2020, phishing attacks are the main concern.

Phishing is a method of social engineering where an illegal hacker attempts to fake the user into clicking a malicious link or downloading an infected attachment or exposing sensitive or confidential information. Hackers and/or social engineering attack techniques use numerous up to date methods to gain personal information, including passwords. Five common contemporary attacks include phishing, baiting, quid pro quo, pretexting, and piggybacking [3].

Ransom ware

Ransom ware is a form of malware that locks users out of their devices in a pay-to-unlock your-device trick; it has grown by increases and limits as a threat category since 2014. Ransom ware is getting more sophisticated Consider the case of ransom ware attack on the NHS in May 2017. The attack resulted in a significant meltdown of emergency services in the UK. It is now being argued that the attack on NHS could have been prevented through due care, regular updates to NHS IT infrastructure and employee training [4].

APT Threats

Advanced Persistent Threats are a method of cyber-attack wherever an illegal attacker encryption enters an innocent organization network and remainders there for a long dated hidden. Rather than imposing harm to these systems, APTs will gently be seated, theft sensitive information and other critical security information.

Distributed Denial of Service attacks

A distributed denial-of-service (DDoS) attack is a malicious effort to disturb usual traffic of a directed server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DoS attacks, as well as Distributed Denial of Service attacks, are the main categories of attacks that can affect availability at the network level [5].

SQL injection

A SQL (Structured Query Language) injection happens while an attacker enclosures malicious cypher into a server that uses SQL (a domain-specific language). SQL injections are only effective when security weakness exists in an application's software. Fruitful SQL attacks force a server to deliver access to data. Human error is to fault for 88% of data breaches in the UK according to research by Kroll [6].

Internet of Things (IoT) device threats

Companies are adding more and more devices to their infrastructures, said Forrester's Zelonis. "Organizations are going and adding solutions like security cameras and smart container ships, and a lot of these devices don't have how you're going to manage them factored into the design of the products."

Mobile malware

Mobile devices are increasingly a top attack target -- a trend rooted in poor vulnerability management, according to Forrester. But the analyst firm said many organizations that try to deploy mobile device management (MDM) solutions find that privacy concerns limit adoption.

Cyber security is worried with safeguarding organization commerce continuousness and avoiding the influence of security events that threaten information of the organization. He agreed with the cyber security is vital but the threats is to demonstrate the influences contributing to difficult itself. Due to that declaration, safeguarding company information from outsiders is becoming strictly important [7].

Besides, once argued on the cyber security, here are numerous languages might be organized to the security of sensitive information. Certain terms looked are phishing, email scam, fraud etc. Refer to Mustaffa, Cyber Security Malaysia has managed more than 57,000 incidents from 1997 to 2014. These incidents include intrusion, fraud, cyber harassment, spam and malicious code. This was supported by Norhayati & Adnan in their research, due to the point that cyber security is a complex, dynamic and multifaceted discipline in which no single component may be ignored, the effective management of this discipline is essential for any organization wishing to survive and thrive in the information age [8].

Insider Threat data breaks initiated through insiders can occur to a business of any size and in any business. According to the 2019 Verizon Data Breach Investigations Report, 34% of data breaches in 2018 involved internal actors. On behalf of companies nowadays, cyber-attack is universally. However for all the moneys they have completed to secure their systems and safeguard clients, businesses are still struggling to make cyber security an exciting, proactive part of strategy, operations, and culture [9].

Malicious Insider

This is when an employee who might have legitimate access to your network has malicious intentions and uses that access to intentionally leak confidential data. Employees who intentionally provide access to the network to an external attacker are also included in this threat. An insider attack includes employees from the inside, such as an authorize employee, attacking the network Insider attacks can be malicious or no malicious. An insider attack is a malicious attack perpetrated on a network or computer system by a person with authorized or privileged system access.

Accidental Insider

This is when an employee makes an honest mistake that could result in a data breach. Something as simple as opening a malicious link in an email or sending sensitive information to the wrong recipient are all considered data breaches. The main cause of accidental insider data breaches is poor employee education around security and data protection and can be avoided by practicing good security practices.

Third Party

There is a data protection risk that arises when third-party contractors or consultants are provided with permission to access certain areas of the network. They could, intentionally or unintentionally, use their permission to access private information and potentially cause a data breach. Past employees who haven't had their security access revoked could also access confidential information they are no longer entitled too and could be seen as a threat.

Social Engineers

Although this threat is technically external a social engineers aim is to exploit employees by interacting with them and then attempting to manipulate them into providing access to the network or revealing sensitive information.

Cyber security consciousness can be defined as the individual's inactive participation and better attention to sure matters and it is measured one of the key mechanisms of consciousness-raising the other being action [2]. According to the theory of planned behavior, the transformation in manners depends on the purpose of the person. There are two influences that effect intention. One factor is attitude and the other is subjective norms. So the level of intention towards an action will be higher if the person has a more positive attitude and more of a subjective norm towards the behavior.

Effective ways to protect our self from cyber attacks

Identify your Sensitive Data

The first step to securing your data is to identify and list all of the private information that you have stored in your network and taking note of whom in your organization has access to it. By gathering all of this information you are able to secure it properly and create a data protection policy which will help keeps your sensitive data secure [10].

Update

One of the most effective ways we can protect our computer at home is to make sure both the operating system and our applications are patched and updated. Enable automatic updating whenever possible.

Email auto-complete

Be careful with email auto-complete. This is an email feature that automatically completes a name for you when you begin typing it in the TO field. However, your email client can easily complete the wrong name for you. If you are emailing anything sensitive, always be sure to check the TO field a second time before hitting the send button.

Securely disposing mobile devices

Do you plan on giving away or selling one of your older mobile devices? Make sure you wipe or reset your device before disposing of it. If you don't, the next person who owns it will have access to all of your accounts and personal information.

Anti-virus

Make sure you have anti-virus software installed on your computer and that it is automatically updating. However, keep in mind that no anti-virus can catch all malware; your computer can still be infected. That is why it's so important you use common sense and be wary of any messages that seem odd or suspicious.

Shopping online securely

When shopping online, always use your credit cards instead of a debit card. If any fraud happens, it is far easier to recover your money from a credit card transaction. Gift cards and one-time-use credit card numbers are even more secure.

Virtual Private Network

Virtual Private Networks (VPN) create encrypted tunnels when you connect to the Internet. They are a fantastic way to protect your privacy and data, especially when traveling and connecting to untrusted or unknown networks, such as at hotels or coffee shops. Use a VPN whenever possible, both for work and personal use.

Create a Data Protection Policy

A data protection policy should outline the guidelines regarding the handling of sensitive data, privacy and security to your employees. By explaining to your staff what they are expected to do when handling confidential information you reduce the risk of an accidental insider data breach.

Create a Culture of Accountability

Both employees and managers should be aware of and understand their responsibilities and the responsibilities of their team when it comes to the handling of sensitive information. By making your team aware of their responsibilities and the consequences of mistakes and negative behavior you can create a culture of accountability. This also has the more positive effect of highlighting any issues that exist before they develop into full problems which can then be dealt with training or increased monitoring [11].

Utilize Strong Credentials & Access Control

By making use of stronger credentials, restricting logins to an onsite location and preventing concurrent logins you can make your network stronger and remove the risk of stolen credentials being used to access the network from an external location.

Review Accounts and Privileged Access

It is significant that you regularly review your user's privileges and account logins to ensure that any inactive accounts no longer have access to private information and that users don't have unnecessary access to data. This helps to reduce the risks of both accidental and malicious insider data breaches [12].

6. Conclusions

In humble languages, outdated software means unsecured software. So, all the organizations globally must switch to the latest software. The threat of an insider data breach continues to be an issue to businesses throughout a range of sectors. However, by putting a plan in place for these insider security threats it improves the speed and effectiveness of your response to any potential issues that arise. The culture and religion also another factor in information security. Employee attitudes regarding cyber-attacks must be changed. Employee (end user) of the organization in Ethiopia does not have knowledge about cyber security and they are aware of cyber security, they are not trained. Organization should make a continuous cyber security assessment. Cyber-attacks have increased from 479 and 576 to 791 grand attacks annually during the past three successive years Information Network Security Agency (INSA, 2019). Despite the growing trends of using technologies in the country, the awareness and capacity to prevent cyber-attack is still poor; and this makes the situation even worse, Ifrah stated. Lack of awareness, legal frameworks, and poor cyber security governance, among others, are among the major problems cited. Thus increasing awareness and building the capacity of citizens and institutions in cyber security are among the next

directions to be prioritized by the government and other stakeholders.

7. Recommendations

i. Organization should train their employees.

ii. Organization should make a continuous cyber security assessment.

iii. Organization should turn their employees into partners.

iv. Organization should have incident response plan.

References

[1] Yang Lu, "Cybersecurity Research: A Review of Current Research Topics," *Journal of Industrial Integration and Management*, vol. Vol. 3, no. No. 4, p. 25, Octobe 2018.

[2] Bilal Khan, "Effectiveness of information security awareness methods based on psychological theories," *African Journal of Business Managemen*, vol. Vol. 5 (26, no. pp. 10862-10868, p. 8, October 2011.

[3] Hussain Aldawood, "Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues," *MDPI*, p. 16, March 2019.

[4] Ibrahim Ghafir, "Security threats to critical infrastructure: the human factor," *doi.org*, p. 17, March 2018.

[5] Michele De Donno, "Cyber-Storms Come from Clouds: Security of Cloud Computing in the IoT Era," *MDPI*, p. 30, June 2019.

[6] Mrs. M. Kundalakesi, "Network Security with Cryptography," *International Journal for Scientific Research & Development*, vol. Vol. 6, no. Issue 01, p. 3, September 2018.

[7] Shilpa Pareek, "Different Type Network Security Threats and Solutions, A Review," *International Journal of Computer Science*, vol. Volume 5, no. Issue 4, p. 11, April 2017.

[8] Adnan Rizal, "Information Security Challenges: A Malaysian Context," *International Journal of Academic Research in Business and Social Sciences,* vol. Vol. 7, no. No. 9, p. 8, September 2017.

[9] Tooska Dargah, "ACyber-Kill-Chain based taxonomy of crypto-ransomware features," *Journal of Computer Virology and HackingTechniques*, p. 29, July 2019.

[10] Shilpa Pareek1, "Different Type Network Security Threats and Solutions, A Review," *International Journal of Computer Science*, vol. Volume 5, no. Issue 4, p. 11, April 2017.

[11] Tadas Limba[1], "CYBER SECURITY MANAGEMENT MODEL FOR CRITICAL INFRASTRUCTURE," *The International Journal ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES,* vol. Volume 4, no. Number 4, p. 16, June 2017.

[12] Yeshwanth Rao, "Artificial Intelligence and Big Data for Computer Cyber Security Systems," *Journal of Advances in Science and Technology*, vol. Vol. 12, no. Issue No. 24, p. 9, November 2016.