Enterprise Cyber Security Challenges to Medium and Large Firms: An Analysis

Emmanuel U. Opara and Onochie J. Dieli
(Corresponding author: Emmanuel U. Opara)

College of Business, Prairie View A&M University
, Prairie View, Texas - U.S.A.
(Email: euopara@pvamu.edu)

(Received April 5, 2021; Revised and Accepted May 25, 2021; First Online May 26, 2021)

Abstract

Enterprise networks are borderless and expand to limitless endpoints and networks. This can be attributed to the explosion of attacks as they come in various forms. Attacks are escalating exponentially. Nation States and various organizations have been hit with high-profile breaches over the past years resulting in millions of dollars in lost revenue, public confidence, reputation, and legal issues. Threats such as Shell Shock, Ghost RATs, Zero-Day, Stuxnet, Advanced Persistent Threats, and Ransomware, are on the rise. We will analyze activities across the cyber-security eco-system and identify actionable solutions to remedy the threats while leveraging security as a business enabler.

Keywords: Exploits; Malware; Network Security; Vulnerabilities

1 Introduction

The eco-system is witnessing security challenges of cyber-attacks as they are becoming very severe and complex to manage [7, 17]. The reasoning is because enterprise systems are borderless and expand to limitless endpoints and networks. The purpose of this study is to create awareness on enterprise cyber security challenges and recommend solutions.

The exponential growth and interconnected cyberspace have been accompanied by an increasing frequency of cyber security attacks and breaches by adversaries. As a result, enterprise systems are investing in digital transformation. The reasons in the surge are to maintain competitive advantages while driving operational and institutional efficiencies and enhancing their market share. These entities are manufacturing products faster, and quicker while advancing logistic processes. As technological breakthroughs are emerging, threat actors will continue cyber bullying by exploiting loopholes in the eco-system [2, 12].

The explosion of cyber-attacks and threats and the integration of sophisticated devices on corporate networks have created massive security challenges. Study shows that, no industry best practice exist that provides the right combinations of state of the art security protection for enterprise systems [3]. Enterprise systems are battling network vulnerabilities that include network leaks, unauthorized access, backdoors, denial of service, direct-access attacks, eavesdropping, code injections, rootkit behavior, and phishing [5, 21].

Other suspicious network activities include privileged escalations, social engineering, tampering, spoofing, IP addresses attacks, access control, etc. Some array of attacks come from these group: malware, insider threats, network intrusions, false data injection, malicious domain names used by adversaries [15]. As all systems are at risk, the number of these threats will continue to grow.

Global cyber-security expenditure to combat the threats is continuing its exponential growth while exceeding the trillion-dollar thresholds that was originally predicted in 2017 [14]. Table 1 shows an overview of data exposure in 2019 [1].

Table 1: an overview of data exposure in 2019

Institution	Category	Reported	Exposed
Orvibo	IoT	7/1/2019	2 Billions
First American	Banking/Credit/Financial	5/25/2019	885 Millions
Facebook	Social Media	3/21/2019	600 Millions
Capital One	Banking/Credit/Financial	7/19/2019	106 Millions
LabCorp	Medical/Healthcare	6/4/2019	7.7 Millions
AMC Networks	Entertainment	5/1/2019	1.3 Millions
T-Mobile	Business	11/22/2019	1 Million
Suprema	Medical/Healthcare	8/25/2019	1 Million
Chtrbox	Social Media	5/20/2019	49 Millions

IT analyst forecasts are unable to keep pace with the dramatic rise in cybercrime, the ransomware epidemic, the refocusing of malware from PCs and laptops to smartphones and mobile devices, the deployment of billions of under-protected Internet of Things (IoT) devices, the legions of hackers-for-hire, and the more sophisticated cyberattacks launching at businesses, governments, educational institutions, and consumers globally.

Some of the heavy duty malware include Shell Shock, Ghost RATs, Zero Day, Regi, Stuxnet, Advanced Persistent, Ransomware. The explosion of these attacks necessitates the development of innovative technological and strategic remedies to secure the increasingly digitized platform [8]. This study will analyze activities across the cybersecurity eco-system and identify actionable solutions to remedy the threats while leveraging security as a business enabler.

2 Literature Review

[9], in their report noted that malware is a threat to cybersecurity as it controls a massive number of compromised hosts during attacks, such as e-mail spam or launching a distributed denial of-service (DDoS) attack etc. They summarized that due to their ability to coordinate attacks at massive scale, as well as deliver diverse payloads and infect other machines, they pose a significant threat to individuals, enterprise, and government organizations.

According to [15], cyber-crime and economic espionage cost the global world more than $800 trillion annually. The study further found evidence that malware is the most expensive attack type for organizations. The noted that the cost of malware attacks has increased by 11% over the year and the cost of malicious insider attacks has increased by 15%.

Another study [1], found evidence that the total annual cost of all types of cyberattacks is increasing. Malware and Web-based attacks continue to be the most expensive. The cost of ransomware (21 percent) and malicious insider (15 percent) attack types have grown the fastest over the last year.

[14], cyber report found evidence that the expanded use of cloud services makes the investigation of cyber threats more efficient and the containment of cyberattacks more cost effective. They summarized that spending on containment has steadily increased over the period.

A study by [13], at the 26th USENIX Security Symposium noted that the Mirai malware took the cyberspace by storm in late 2016 when it overwhelmed several high-profile targets with some of the largest distributed denial-of-service (DDoS) attacks on record.

An earlier study by [8], reported that global cyber security expenditure was approximately 4.8 billion. However, a later study by [14], reveals that global spending on cybersecurity products and services will exceed $1 trillion cumulatively by 2022.

[4], Cathay Pacific Airways revealed that a hacker accessed the personal information of 9.4 million of its passengers in a security breach against the aviation industry. They found evidence that passport numbers, email addresses and credit card details were among the data leaked.

Reports from [16,18], among others, summarized that anyone and everyone is susceptible for attacks. The report concluded that criminal minded nation-states would continue espionage activities of attack against businesses that do not properly protect itself from such attacks.

In an earlier study [11]), it was found that the attack on Target 70 million stolen credit card was real. The report further narrated that over 40 million customer records containing financial data such as debit and credit card information were stolen. It concluded that seventy million addresses and mobile numbers were compromised.

[14] found evidence that in 2019, 1,473 data breaches in the U.S. led to the exposure of 164,683,455 confidential records. Due to the rising number of such attacks, their study projects that cyber security market will grow from $119.9 billion in 2019 to $433.6 billion by 2030.

[18,20] among others, found evidence that "Anthem", a U.S. health insurance company, was hacked, resulting in the theft of 80 million customers' information.

Another study [10], found evidence that the Russian and Chinese governments were key to cyber espionage across the eco-system. Their reports summarized that cybercriminals stole 40 million credit card numbers from Target and compromised 70 million accounts.

3 Methodology

A survey questionnaire was developed and distributed to technology professionals and researchers in the field of cyber-security at a Network Security 2019 conference in Washington, DC. The objective of the survey is to ascertain the challenges and issues facing both technology professionals and researchers regarding cyber-security threats at their respective organizations.

The survey respondents represent technology professionals in the cyber-security industry, governmental and university researchers. The sample population pool includes practitioners in the field, with varying years of experiences and ranks from top systems administrators to lower-level IT staff members, who handle cyber-security issues in their respective organizations. These organizations range from mid-size to Fortune 500 companies. Researchers at the conference, conduct and publish cyber-security research issues for federal agencies and universities in higher education.

A population sample size of 182 surveys responses were returned and completed. These represented a random population of technology professionals and researchers in the field. There were 15 items in the questionnaire, with Likert scales whose anchors ranged from 1 to 5, "strongly disagree" to "strongly agree," respectively. The respondents' items on gender and IT high level job ranking had categorical choices, respectively: 1 (male) and 2 (female); 1 (yes) and 2 (no). There were 100 male and 82 female respondents, representing 55% and 41% of the sample, respectively. 154 of the sample subjects reported their IT rank as Executive or a Senior IT Administrator, while 28 reported the rank as a lower-level IT employee, representing 85% and 15% of the sample, respectively.

4 Results of Statistical Analysis

The results of the statistical analysis are shown in Tables 2.

Table 2: Primary Statistics: used to gather feedback directly from targeted audience

Sample Size(n)	182	Sample size(n)	182
No of Women	82	No of IT_ADMIN	154
No of Men	100	No of Non IT-ADMIN	28
% of Women	45	% of IT-ADMIN	85
% of Men	55	% of Non IT-ADMIN	15

4.1 Survey Question 1

The study asked on a scale of 1 to 5, how secured, do you think; your company network is? Table 3 shows the response analysis of the survey question. Total percent of responses of 1 and 2 in the sample: 17%; Total percent of Responses of 3, 4 and 5 in the sample: 83%; This implies that 83 percent of the sample think their company is secure.

Table 3: Response analysis of Survey Question 1

1	Don't Know (1)	7
2	Not very secure (2)	24
3	Somewhat secure (3)	79
4	Secure (4)	52
5	Very Secure (5)	20

In order to further validate this result, we conducted a test of hypothesis (single Proportion) that the population proportion of industries workers who think that their organizations are secure at 5percent level of significance is less or equal to 50% (hypothetical population proportion).

Let P_o be the population proportion of industries workers who think they are secure.

H_o **(Null Hypothesis):** $Po \leq .50$ that think their company is secure;

H_a **(Alternative Hypothesis):** $P_o \geq .50$ that think their company is secure.

$\alpha = 5\%$ (level of Significance).

If $np \geq 10$ and $n(1-p) \geq 10$ then the study can use Z-test statistic and since $182 * .50 > 0$ and $182 * .50 > 10$ (or considering that the number of success and failures are 91 and 91 respectively are at least 10. This study estimates the test statistic by:

$$\begin{aligned} Z &= \acute{P} - P_o \\ &= \sqrt{P_o(1-P_o)/n} \end{aligned}$$

Here, $\acute{P} = 0.83$ (sample proportion); $P_o = 0.50$ (population proportion); $N = 182$; $Z_c = 8.92$; $Z_t = 1.65$ (5% level of significance) critical value = 0.05.

Since $Z_c > Z_t$, our study rejected the Null hypothesis and accepted the alternate. The test is significant. It confirms that more than 50 percent (83%) of the industries workers' population think their company is secure. This conclusion is based on the sample result (a representative sample) which is reliably predictive of the population. Sample statistics predict population parameters at point estimate or interval estimate within negligible margin of errors.

4.2 Survey Question 2

The study asked, on a scale of 1 to 5, how helpful do you find network scanning tools used in your organization in mitigating threats? Table 4 shows the response analysis of the survey question. Total percent of responses of 1,2 and 3 in the sample: 15%; Total percent of Responses of 4 and 5 in the sample: 85%.

Table 4: Response analysis of Survey Question 2

1	Very unhelpful (1)	0
2	Somewhat unhelpful (2)	13
3	Neither helpful nor unhelpful (3)	14
4	Somewhat helpful (4)	97
5	Very Secure (5)	58

This implies that 85% of the sample think that the scanning tools are helpful in mitigating threats. To further validate this result, we conducted a test of hypothesis (single proportion) that the population proportion of industries workers who think that the scanning tools are helpful in mitigating threats at 5% level of significance is less or equal to 50% (hypothetical population proportion).

Let P_o be the population proportion of industries workers who think that the scanning tools are useful in mitigating threats.

H_o **(Null Hypothesis):** $P_o \leq .50$ think that scanning tools are useful in mitigating threats;

H_a **(Alternative Hypothesis):** $P_o \geq .50$ think that scanning tools are useful in mitigating threats.

Here, $\alpha = 5\%$ (level of Significance). If $np \geq 10$ and $n(1-p) \geq 10$ then I can use Z-test statistic and since $182 * .50 > 0$ and $182 * .50 > 10$ (or considering that the number of success and failures are 91 and 91 respectively are at least 10. We calculate the test statistic by:

$$\begin{aligned} Z &= \acute{P} - P_o \\ &= \sqrt{P_o(1-P_o)/n} \end{aligned}$$

Here, $\acute{P} = 0.85$ (sample proportion); $P_o = 0.50$ (population proportion); $N = 182$; $Z_c = 9.5$; $Z_t = 1.65$ (5% level of significance) critical value = 0.05.

Since $Z_c > Z_t$, we rejected the Null hypothesis (H_o) and accepted the alternate hypothesis (H_a). The test is significant. It confirms that more than 50 percent (85%) of the industries workers' population think that the scanning tools are useful in mitigating threats. This conclusion is based on the sample result (a representative sample) which is reliably predictive of the population. Sample statistics predict population parameters at point estimate or interval estimate within negligible margin of errors.

4.3 Survey Question 3

The study asked that on a scale of 1 to 5, when threat hunting, how often do your organizations run a network security defensive as you search for threats on your network? Table 5 shows the response analysis of the survey question. Total percent of responses of 1 and 2 in the sample: 7.7%; Total percent of Responses of 3, 4 and 5 in the sample: 92.3%.

Table 5: Response analysis of Survey Question 3

1	Never (1)	7
2	Rarely (2)	7
3	Sometimes (3)	58
4	Often (4)	86
5	Always (5)	24

This implies that 92.3% of the sample think that their organizations run a network security defensive when searching for threats on the network. To further validate this result, we conducted a test of hypothesis (single Proportion) that the population proportion of industries workers who think that their organizations run a network security defensive as they search for threats on the network at 5% level of significance is less or equal to 50% (hypothetical population proportion).

Let P_o be the population proportion of industries workers who think that their organizations run a network security defensive while searching the network for threats.

H_o **(Null Hypothesis):** $P_o \leq .50$ think that their company run a network security defensive;

H_a **(Alternative Hypothesis):** $P_o \geq .50$ think that their company run a network security defensive.

Here, $\alpha = 5\%$ (level of Significance).

If $np \geq 10$ and $n(1-p) \geq 10$ then the study can use Z-test statistic and since $182 * .50 > 0$ and $182 * .50 > 10$ (or considering that the number of success and failures are 91 and 91 respectively are at least 10. The study estimates the test statistic by:

$$\begin{aligned} Z &= \acute{P} - P_o \\ &= \sqrt{P_o(1-P_o)/n} \end{aligned}$$

Here, $\acute{P} = 0.923$ (sample proportion); $P_o = 0.50$ (population proportion); $N = 182$; $Z_c = 11.4$; $Z_t = 1.65$ (5% level of significance) critical value = 0.05.

Since $Z_c > Z_t$, we reject Null hypothesis (H_o) and accept the alternate hypothesis (H_a). The test is significant. It confirms that more than 50 percent (92.3%) of the industries workers' population think that their organization run network security defensive while on threat hunting. This conclusion is based on the sample result (a representative sample) which is reliably predictive of the population. Sample statistics predict population parameters at point estimate or interval estimate within negligible margin of errors.

5 Conclusion

This study highlights the trends cyber-actors use to attack enterprise systems across all industries and gives cyber security professionals the information they need to protect their organizations from next-generation cyber-attacks.

It further established that the exponential burst of next-generation digital transformation also prompted series of security vulnerabilities. Solutions to the identified threats include isolation technologies, activity–behavior monitoring and algorithmic file classifications. The study further highlights enterprise security architecture and detection schema.

Isolation technologies as illustrated, protect the system by sandboxing processes, resulting in limited access to the enterprise operating systems [9]. Implementing activity monitoring systems help monitor and track end-user behavior on devices, organization networks and other enterprise owned IT resources. This detect and stop malicious insider threats. A classification algorithm should also be implemented because it will provide researchers the most accurate separation of two classes of data. This technology is a supervised learning technique used to identify the category of new observations based on training data [13]. When implemented, the entity forms some logical structures based on what was found and institute a best practice solution.

6 Lesson Learned

Enterprise cyber security challenges are happening more often and are becoming more severe as compared to the past. Lessons from this study revealed that cyber security are here to stay. Enterprises systems should examine and close any insecure or unused ports and protocols such as simple network management protocol and UPnP that exposes the network to adversaries. Also, to conduct reviews for connected peripheries that may have default credentials and institute new passphrase when necessary. Future research will include anomaly-based detections using deep learning, machine learning and artificial intelligence technologies.

References

[1] D. Ayrapetov, *2019 SonicWall Cyber Threat Report: Unmasking Threats That Target Enterprises, Governments & SMBs*, Mar. 26, 2019. (https://blog.sonicwall.com/en-us/2019/03/2019-sonicwall-cyber-threat-report/)

[2] H. Bradley, W. P. Strobel, D. Volz, "High-level cyber intrusions hit Bahrain amid tensions with Iran," *The Wall Street Journal*, Aug. 7, 2019. https://www.wsj.com/articles/high-level-cyber-intrusions-hit-bahrain-amid-tensions-with-iran-11565202488.

[3] F. Brown, *Highway to the danger drone*, Bishop Fox, Aug. 3, 2016. (https://www.bishopfox.com/files/slides/2016/Black_Hat_USA_2016-Danger_Drone-Brown_Petro_Latimer-03Aug2016.pdf)

[4] BBC, *Cathay Pacific Airline Report - Cathay Pacific data hack hits 9.4 million passengers*, Oct. 25, 2018. (https://www.bbc.com/news/business-45974020)

[5] CyberSource, *15th annual online fraud report: Online payment fraud trends, merchant practices and benchmarks*, San Francisco, CA: Visa-CyberSource, 2015.

[6] G. Davis, T. Birdsong, *What is wardriving?*, McAfee blogs post, Oct. 28, 2016. (https://securingtomorrow.mcafee.com/consumer/identity-protection/wardriving/)

[7] A. Dewanje1 and K. A. Kumar, "A New Malware Detection Model using Emerging Machine Learning Algorithms," *International Journal of Electronics and Information Engineering*, vol. 13, no. 1, pp. 24-32, Mar. 2020.

[8] M. Eddy, "Satellite communications hacks are real, and they're terrifying," Aug. 9, 2018. (https://www.pcmag.com/news/satellite-communications-hacks-are-real-and-theyre-terrifying)

[9] M. Hatada, M. Scholl, "An Empirical Study on Flow-Based Botnet Attacks Prediction," *National Institute of Standards and Technology Technical Note 2111*, Oct. 2020. (https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2111.pdf)

[10] D. Lawrence, "Spy vs spy: The US government designed and funds the best defense against its own surveillance," *Bloomberg Businessweek*, pp. 42-47, Jan. 27, 2014.
[11] M. Lennon, "New IE 10 zero-day used in watering hole attack targeting U.S. military," *Security Week*, Feb. 13, 2014. (https://www.securityweek.com/new-ie-10-zero-day-used-watering-hole-attack-targeting-us-military)
[12] L. Liu and Z. Cao, "Analysis of a Privacy Preserving Ranked Multi-Keyword Search Scheme," *International Journal of Electronics and Information Engineering*, vol. 12, no. 2, pp. 53-59, June 2020.
[13] A. Manos, *et al.*, "Understanding the Mirai Botnet," in *the Proceedings of the 26th USENIX Security Symposium*, pp. 1093–1110, 2017.
[14] S. Morgan, "Cybersecurity ventures' cybersecurity market report sponsored by secure anchor," *Cybercrime Magazine*, June 10, 2019. (https://cybersecurityventures.com/cybersecurity-market-report/)
[15] MSRC Team, "Corporate IoT - A path to intrusion," *Microsoft Security Response Center post*, Aug. 5, 2019. (https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/)
[16] E. U. Opara, O. A. Soluade, "Straddling The Next Cyber Frontier: The Empirical Analysis On Network Security, Exploits, and Vulnerabilities," *International Journal of Electronics and Information Engineering*, vol. 3, no.1, pp. 10-18, Sept. 2015.
[17] C. Stupp, "Fraudsters used AI to mimic CEO's voice in unusual cybercrime case," *The Wall Street Journal*, Aug. 30, 2019. (https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402)
[18] N. Villeneuve, *TeslaCrypt: Following the Money Trail and Learning the Human Costs of Ransomware*, Threat Research, May 15, 2015. (https://www.fireeye.com/blog/threat-research/2015/05/teslacrypt_followin.html)
[19] World Economic Forum, *World Economic Forum Annual Meeting 2013, Davos-Klosters*, Partnering for Cyber Resilience (PCR), Feb. 2013. (http://www3.weforum.org/docs/WEF_RRHW_PartneringCyberResilience_NewsletteFebruary_2013.pdf)
[20] K. Zetter, *Attackers stole certificate from Foxconn to hack Kaspersky with Duqu 2.0*, June 15, 2015. (http://www.wired.com/2015/06/foxconn-hack-kaspersky-duqu-2/)
[21] N. Zhao, X. W. Wang, and S. L. Yin, "Research of Fire Smoke Detection Algorithm Based on Video," *International Journal of Electronics and Information Engineering*, vol. 13, no. 1, pp. 1-9, Mar. 2021.

Biography

Dr. Opara is a Professor of Management Information Systems at the College of Business, Prairie View A&M University. He teaches Networking, Cyber Security, Digital, Media & Network Forensics, Communications in Digital Age & Fundamentals of MIS. He is a member of board of directors & a "Fellow" [FIIMA] of the International Information Management Association. His research is in Integrated Network Systems Securities, Windows – Media - Computer Network, Digital Forensics, Incident Response & Threat Hunting, Memory Analysis, Containment of Advanced Adversaries, Biometrics Technology, Network and Data Communication. His passion is in Intrusion forensics, vulnerability and exploits discovery, intrusion detection/prevention analysis, penetration testing while deploying python programming. He employs memory forensics analysis tools such as Rekall, Volatility, Memoryze, DumpIT, FTK

Imager.

Dr. Onochie J. Dieli is an Economics Instructor at the College of Business, Prairie View A&M University, Texas. As a lecturer, he taught Introductory Statistics and Economics at Howard University, Washington DC. His areas of concentration include Industrial Organization, Applied Econometrics, Statistics and Economic Theory. He is experienced with quantitative methods of social research in panel data using SARS, STATA and SPSS. He works efficiently in Windows environment, and MS-DOS. Other areas of interest include Cyber Security, Networking and Software Development.