IBIMA Publishing
Communications of the IBIMA
https://ibimapublishing.com/articles/CIBIMA/2021/589235/
Vol. 2021 (2021), Article ID 589235, 7 pages, ISSN: 1943-7765
DOI: 10.5171/2021.589235

Research Article

A Descriptive Study on Cybersecurity Challenges of Working from Home during COVID-19 Pandemic and a Proposed 8 step WFH Cyber-attack Mitigation Plan

Glorin SEBASTIAN

School of Public Policy, Georgia institute of Technology, Atlanta, GA, USA,
gsebastian6@gatech.edu

Received date: 9 November 2020; Accepted date:18 January 2021; Published date: 17 February 2021

Academic Editor: Ahmed Azam

Abstract

Organizations struggle to strike the right balance between flexibility and security for remote work. With the major portion of the workforce in every country working from home during the covid-19 pandemic, employers might not have accounted for this scale of load on their IT infrastructure, not to mention their cybersecurity preparedness. Cybercriminals have been working to exploit this unpreparedness with regards to IT Infrastructure. The purpose of this study is to discuss increased cybersecurity risks of work from home due to Covid-19 pandemic, and as part of the study, a WFH cyber-attack mitigation framework has been proposed with eight simple but effective steps to mitigate and prevent these cyber-attacks.

Keywords: Privacy risks, Cybersecurity, Covid-19, Work from Home.

Introduction

With the Covid-19 Pandemic affecting the entire Globe with over 40 Million cases, and 1 Million deaths as of October 2020, per data obtained from Johns Hopkins Coronavirus Resource Center, and with a large percentage of workers and students working from Home or remotely, could be the beginning of what William D. Eberle, Professor of Economics in Stanford's School of Humanities and Sciences in his June 2020 article on Stanford News calls the 'Work from Home' Economy. With the Covid-19 Pandemic which started in late 2019, stretching into 2021, the Pandemic is something that the world has not seen in the past 100 years, with almost everyone working from Home except the essential and front-line workers.

According to PwC'S COVID-19 CFO Pulse survey, 41% of the finance leaders surveyed in North America said that they struggle to strike the right balance between

Cite this Article as: Glorin SEBASTIAN (2021)," A Descriptive Study on Cybersecurity Challenges of Working from Home during COVID-19 Pandemic and a Proposed 8 step WFH Cyber-attack Mitigation Plan", Communications of the IBIMA, Vol. 2021 (2021), Article ID 589235, DOI: 10.5171/2021.589235

flexibility and security for remote work. With the major portion of the workforce in every country working from Home, employers might not have accounted for this scale of load on their IT infrastructure, not to mention their cybersecurity preparedness. With these record numbers of employees working from Home, companies are struggling not just to cope with the need for IT infrastructure to support the increased load on their IT servers but also to cope with the increase in cyber-attacks on their IT infrastructure. Cybercriminals have been working to exploit this unpreparedness of the employers with regards to their IT Infrastructure as is clear from the increased number of Cyber-attack complaints received by the FBI and Interpol.

The FBI reported in April 2020 that the number of complaints received by its Cyber Division was up to 800% increase from the numbers pre-coronavirus. Monster Cloud, a Managed Cybersecurity Services firm in its August 2020 Blog, noted that Interpol reported an "alarming rate of cyber-attacks aimed at major corporations, governments, and critical infrastructure". There have also been corporate ransomware attacks around August 2020, on multinational companies such as Honda, Garmin and Canon.

Given these circumstances, it is extremely timely and crucial for not just Multinational companies but also healthcare providers with significant amount of Health information, PII (Personally Identifiable Information) and PHI (Protected health information) to be aware and enforce proactive controls towards mitigating this very real risk. For example, the twitter handle hack in July 2020, in which twitter employees were targeted in a phone spear phishing attack, led to bad actors assuming control of celebrity twitter handles including that of a former US President as reported in Twitter Blog. All these point to the proliferation of cyber-attacks against corporations and their employees.

There are multiple types of cyber-attacks, however the common types that could affect work from Home systems include:

1) ***Social Engineering such as Phishing:***

Social Engineering refers to cyber-attacks that are accomplished through the weakest link i.e., humans. The bad actor who performs Phishing attacks uses social engineering techniques to deceive end-users, most times relying on human error, which indicates the importance of user-focused studies to help prevent future attacks as noted in the Systematic Literature Review by Das, Sanchari. (2019). Social engineering attacks are becoming very common even on corporate networks. An advanced version of Phishing is Spear phishing, which targets a specific person or group and often includes information known to be of interest to the target, such as current events or financial documents." Like other social engineering attacks, phishing attacks take advantage of the human tendency to respond to an emergency, hence most phishing emails would include a scenario that requires immediate action from the reader.

2) ***DoS and DDoS Attacks:***

A denial-of-service (DoS) attack occurs when legitimate users are unable to access resources such as information systems, devices, or network resources due to the actions of a malicious cyber attacker. A distributed denial-of-service (DDoS) attack is similar to DoS attacks, but usually includes multiple machines that are operating together to attack one target. DDoS attackers often leverage the use of a botnet—a group of hijacked Internet-connected devices to carry out large scale attacks as per Security Tip (ST04-015) (2019). These attacks are specially of increased prominence with the emergence of 5G technology and IoT (Internet of Things) since increased Internet speeds and interconnected IoT devices form the perfect scenario for these attacks.

3) ***Ransomware Attacks:***

Ransomware is a malware that, when infects systems, usually encrypts all the data including critical information and is perpetrated by bad actors or attackers who often demand money in return to the organization getting back access to their data. Ransomware attacks are particularly seen to target healthcare clients to gain

access to the PII (Personally identifiable Information) and PHI (Personal health information).

Given this proliferation of Cyber-attacks specially on work from home setups, we also performed a study as part of this research. The main objectives for this study are as follows:

1. To measure the awareness among everyday company employees on the proliferation of the cyber-attacks, accelerated by the work from Home due to the Covid-19 Pandemic. This awareness is essentially also a measure of the effectiveness of employees' cyber awareness training that they received from their respective corporate firms.

2. To suggest effective methods that companies could use to proactively detect and mitigate these Cyber risks, so that these attacks do not obstruct the work from home environment as well as to meet the most common security objectives for remote work as defined by NIST Special Publication (SP) 800-46 which is the CIA triad:

    - Confidentiality - ensuring that remote communications and data cannot be read by unauthorized parties;
    - Integrity - detect any changes to remote access communications that occur in transit; and
    - Availability—ensure that users can access resources through remote access.

Materials and Methods

The study included a survey conducted over 2 weeks in October 2020 and surveyed 109 participant responses. The survey was conducted over Google forms and shared individually to professionals on LinkedIn. To maintain uniformity, the study was conducted only on professionals who could work from home completely.

The survey included questions on topics such as:

1. Ensure all the respondents had the required IT infrastructure to work from Home;
2. Enquire if the respondent company has enabled extra security measures/ controls such as VPN, Two Factor Authentication etc. to counter this increase in spam or phishing attempts;
3. If the extra security measures enabled by company has affected the employee productivity;
4. If since start of the Covid-19 Pandemic, while working from Home, the end user has experienced an increase in fraudulent emails, Phishing attempts, or spam to his/her corporate email.

Finally, the users are also asked to share suggestions on how to mitigate these Cyber security and Privacy related concerns that they might have with working from Home or remotely. The Data collected were analyzed and expressed as percentages and proportions. Please refer to Table-1 for the survey responses from the study participants.

Results

All the 109 respondents have been working from Home, 75% or more for the past 6 months, and most of them had enough IT infrastructure to work from Home and also had their company enable extra security measures or controls to counter increase in spam or phishing attempts.

Over 60% of the respondents agreed that there has been an increase in fraudulent emails, Phishing attempts, and spam to corporate email, since start of Covid-19 Pandemic, while 15% of the respondents thought that extra security measures had an adverse impact on their productivity. (Table 1)

Table1: Survey responses of the study participants

What percentage of your work have you been doing remotely for the past 6 months?	***Response***
96-100%	89%
76-95%	11%
Do you have enough IT Infrastructure e.g.: Strong Internet connection, Laptop/ Desktop with the required specifications etc. to effectively work from Home?	**Response**
Yes, I had the required IT infrastructure to effectively WFH before the Pandemic	94%
did not have it prior to the Pandemic, company helped with setup during Pandemic	6%
Has your company enabled extra security measures/ controls such as VPN, Two Factor Authentication etc. to counter this increase in spam or phishing attempts?	**Response**
Yes	66%
No	28%
Did not notice	6%
If you answered Yes for above question, have these measures, affected your productivity?	**Response**
Yes	15%
No	85%
Since start of Covid-19 Pandemic, while working from Home, have you experienced an increase in fraudulent emails, Phishing attempts, and spam to your corporate email?	**Response**
Yes, there has been an increase	**62.4%**
No, there has not been an increase	37.6%

Measures for Mitigation of Cyber security Challenges

The Information Technology Laboratory (ITL), a component of the NIST Computer Resource Center, has issued a bulletin that reiterates NIST standards for teleworking. We compiled the mitigation measures suggested by the study participants and Special Publication (SP) 800-46 Revision 2 to come up with an 8 step WFH (Work from Home) Cyber-attack mitigation plan. (Figure 1). These should be included as part of internal controls by the Risk and Controls team as noted in the review article by Sebastian, G (2020) to ensure their implementation within the firm. While coming up with this framework, we focused on effective and Policy friendly techniques which would be easy for the management to understand as well.

They include both detective and preventive controls, as described below and we recommend these Remote work security controls to be included in the firms' security policy. However, each organization can decide on the level of enforcement of these controls based on a Risk based approach.

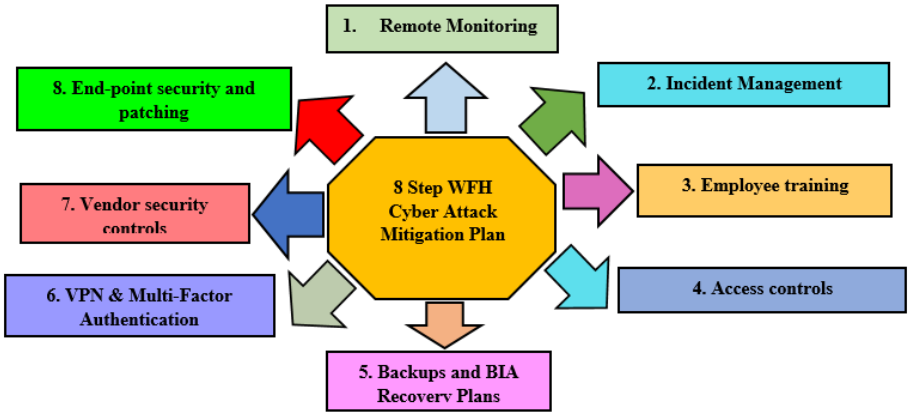

Fig 1: Cyber mitigation steps that help combat cyber-attacks in workplace

Detective Control

1) Remote Monitoring:
Installing network scanning techniques including firewalls that restrict network traffic, DoS protection service that detects abnormal traffic flows and filters out such traffic. Active monitoring is one of the best detective controls to prevent Cyber-attacks.

2) Incident Management:
Incident management is a continuation of Monitoring and includes SIEM (Security information and event management) that provides a real-time analysis of security issues generated from the IT layers including application, network, and Databases. The technologies used for this incident management often have the ability for Data aggregation, correlation and sharing the information in form of Dashboards which can be used by management to assess risks and determine mitigation methods.

Preventive Control

3) *Employee training:* Humans are the weakest links in every cyber environment, and hence it is to be made sure that they are provided with appropriate training to ensure they are aware of the various attacks that they could face in a corporate environment. It is not just sufficient to have proper Employee security training, but there needs to be put in place a cyber-aware employee culture at workplace, and this awareness should be tested periodically with mock cyber-attack simulations.

4) *Access controls:* Ensuring the users have proper access controls, and making sure to maintain proper segregation of duties between two conflicting business functions is important. Also there needs to be periodic review controls to ensure that the employees are not misusing their elevated access.

5) Backups and BIA-Recovery Plans:
Create a disaster recovery plan which includes backups and BIA (Business impact assessment) to set precedence for effective communication, mitigation, and recovery in case of critical cyberattacks. The backup plan specially helps in the case of Data loss. Also ensure the Data are encrypted on the device built-in storage including removable media used by the device.

6) VPN, MFA:
Both using VPN (Virtual private network) and MFA (Multi Factor authentication) ensures the user Data are protected. Employees that access company Data while connected to a

VPN ensure that the Data in motion are protected between 2 devices on the Public network, same as they are connected over a Private network. Using the VPN provides security specially when connected to unsecured networks causing attacks such as man-in-the-middle attacks (MITM), eavesdropping, etc. A Microsoft security blog dated August 2019 noted that enabling MFA reduced cyber incidents by 99.9%. VPN and MFA together are the two most important preventive controls that can thwart the majority of the Cyber-attacks in a Work from home environment.

7) *Vendor security controls:*
Given a lot of critical Business processes and Data are outsourced to vendors, it is critical to ensure that the controls, especially Security controls on the Vendor side are effective. This usually is ensured via contract terms, and regular SOC (System and Organization Controls) audits. SOC-2 audit reports which includes the audit details about the vendor Cyber and Data protection controls in place and its effectiveness is to be reviewed periodically. SOC-2 reports summarize how the company safeguards customer data and how well those internal controls are operating.

8) *Endpoint security (including Wi-Fi and Access points) and Patching:*
Endpoint Security ensures each end point that is connected to the central corporate network is compliant to the organization standards and thus protects you from malware, ransom ware and other similar cyber-attacks. It manages the user access on an ongoing basis over the corporate network. It includes not just Anti-virus which is usually based on signature-based protection, but end point security also includes, regular patching at Network, Application, Operating System and even at Database level, and this can be remotely monitored by Corporate IT Admin using technologies which recently have been using even Fuzzy logic, AI (Artificial Intelligence) etc. VPN discussed in #6 could be considered as part of end point security as well, but we included it as a separate point, since VPN is critical to Data protection for working from home, especially when connected to unprotected networks e.g.: in coffee shops. Endpoint security also includes central authentication techniques monitored by the Corporate IT Admin.

Discussion

This study tried to understand the perceived privacy and cyber security challenges faced by professionals when working from home during COVID-19 Pandemic and the best practices on effective mitigation of risks. According to a similar study, by B. Gyunka and O. Christiana Abikoye (2017), one of the reasons for increase in cybersecurity risks is because we are lacking common practice and training on security. Another study by "Malicious Insider", Science Direct, 2020, found that the major challenge in cybersecurity is people risk management, authorization, and access control. In this paper, based on a survey study on work from home employees, we studied the perceived privacy and cyber security challenges faced by professionals when working from home during COVID-19 Pandemic. It is a fact that there has been a proliferation of Cyber-attacks since the start of the Covid-19 Pandemic, from the study we understand that most users are aware of this, but in Cyber security most is not good enough as it takes only one mistake from anyone of the employees to give a bad actor access to the enterprise resources.

Conclusion

In addition to the uncertainty caused by the Covid-19 Pandemic to health and the Economy, it is seen that cybercriminals are using this as an opportunity to launch cyber-attacks as most of the employees have been working from home for more than 6 months. We see that the employees are aware of this cyber-attack proliferation, but it needs to be made sure

that all of them are fully aware of the cyber security and privacy risks posed by working from home. We also suggest an 8 step Work from home best practice framework for effective cyber risk mitigation while working from home. These steps in the framework are extremely effective to thwart cyber-attacks and have been explained in a concise and simple manner, so that they can easily be used as a checklist for companies looking to incorporate remote work best practices into their security policy.

References

- Adam Gorlick, Stanford Institute for Economic Policy Research: (415) 823-5460.Available at https://news.stanford.edu/2020/06/29/snapshot-new-working-home-economy/
- B. Gyunka and O. Christiana Abikoye, Analysis of Human Factors in Cyber Security: A Case Study of Anonymous Attack on HBgary. 2017, pp. 10-14.
- Das, Sanchari. (2019). All About Phishing Exploring User Research through a Systematic Literature Review.
- Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, NIST Special Publication (SP) 800-46 Revision 2
- JHU COVID-19 Map, Johns Hopkins Centers for Civic Impact. https://coronavirus.jhu.edu/map.html
- Monster Cloud (Aug 11, 2020), Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic
- "Malicious Insider", Science Direct, 2020. [Online]. Available: https://www.sciencedirect.com/topics/ computerscience/malicious-insider.
- "Microsoft Security Blog", 2019. [Online]. Available: https://www.microsoft.com/security/blog/ 2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/
- PwC's COVID-19 CFO Pulse Survey. Available from https://www.pwc.com/us/en/library/covid-19/pwc-covid-19-cfo-pulse-survey.html
- Sebastian, G (2020), Evolution of the role of risk and controls team in an ERP Implementation, IJMPERD, ISSN (P): 2249–6890; ISSN (E): 2249–8001 Vol. 10, Issue 3, Jun 2020, 15529–15532
- Sebastian, G., 2021. An Exploratory Survey On The Perceptions Regarding The Inclusion Of Security And Privacy By Design (SBD, Pbd) Principles During Software Development Lifecycle (SDLC) Requirements Gathering Phase Among Business Analysts. Zenodo. Available at: https://doi.org/10.5281/zenodo.4427206
- Security Tip (ST04-015) (November 20, 2019) Understanding Denial-of-Service Attacks. Available at https://us-cert.cisa.gov/ncas/tips/ST04-015
- Twitter Inc. (18 July 2020) An update on our security incident. Available at https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html.