Technical: Data metrics dashboard security analysis

STS: How has COVID influenced the cybersecurity of employees working in a new environment

A Thesis Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science, School of Engineering
,

Technical Project Team Members
Davin Um

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature: Davin Um **Date: 12/4/20**

Approved James Cohoon **Date** 12/4/20
, Department of Computer Science
Approved Sharon Tsai-Hsuan Ku **Date** 12/4/20
, Department of Engineering and Society

Introduction

Since the coronavirus pandemic, employees were forced to change their working environment to almost virtually. This impacted the cybersecurity of different organizations, which cyber threats became more prevalent towards employees' devices. The project carefully analyzes the general information of cybersecurity and cyber threats, and the impact of cybersecurity due to shifts in the working environment. The project will put emphasis towards finding how the perception of employees towards cybersecurity has changed, as well as its impact on their work in general. The research will be conducted through analysis and gathering of data, carefully conducting surveys to people who fall into the category and studying documents that have corresponding data. The project will ultimately find the difference in awareness of cybersecurity since the pandemic and spread the knowledge that cybersecurity has a significant role in protecting our daily life.

The technical report discusses the threat dashboard that allows the user to see the visualization of cyber threats happening to their system. The dashboard has multiple panels that visualize the data, such as number of logs, graphs showing the trend of the data, etc. Because of the coronavirus, it became essential for companies and small businesses to depend on other companies' security systems for the protection against cyber threats. The technical project will provide the solution to the approach which the user will be able to identify if the threat is currently happening through looking at that security dashboard. The data will be transmitted from the database to the dashboard, and the panels will be updated accordingly. If malicious behavior is detected from the dashboard, then the user will be able to analyze it and contact the security team of either their own security team or the company that provides the protection.

Technical Topic

The COVID-19 has impacted businesses critically, which have caused employees to work in remote environments. While these workers are working separately, the hackers have been trying to take advantage of the situation where the workers are ill prepared for security. According to Furnell and Shah (2020), the data indicates that 30% of UK companies are well prepared for user education and awareness. This is directly related to how the companies have a set of rules on cybersecurity that explicitly sets what the employees are demanded to perform with their devices. The percentage shows that the employees are not well trained with regards to cybersecurity, which can lead to leak of information in unprotected networks. Funnel et al (2020) also demonstrates that 25% of companies are well prepared for home and mobile working, which indicates that there is a lack of cyber security-framed, written rules that employees should follow.

In order to solve this problem, companies have been providing personal devices that have security systems implemented, employees have been utilizing VPN and authorized software to interact with others and increasing awareness of phishing scams, avoiding any suspicious emails received through company accounts. However, some companies do not have well-built security systems, as they have to depend on external services to provide security into their system. They lack the technology to prevent which attacks happen most frequently and respond to them, which can ultimately lead to fatal results, such as data loss and DDoS. This project will provide an efficient way of analyzing threats that the company is facing, which will allow them to see different types of attacks happening.

The project itself will involve a data metrics dashboard, which is composed of different panels that have data representation. There will be multiple dashboards that the user will be able to see, such as Malware, Network traffic, and phishing. These dashboards will allow the user to see detailed reports related to the threats and analyze the information. If the dashboard shows critical information, then the

user can contact the security team directly and handle the problem effectively. This solution tends to provide better performance of the security system, as the customer and the security provider can communicate with each other instead of only the security team dealing with the situation.

The technical report incorporates open source called Grafana, which it provides a default database that can be utilized to visualize the data. Multiple panels are created for different dashboards, which the dashboards are specifically assigned to different types of cyber threats. Before creating the dashboard, the prototype of the dashboard is created using design applications to enhance user experience of the project. After the prototype is finished, the dashboards are created to provide threat information to the user. The designing and implementation of the project was done during early November for a week and a half, which the approval delay from technical advisors has caused issue related to the layout of the project timeline.

CS Capstone

Data metrics dashboard

Davin Um
School of Engineering and Applied Science – Computer Science
University of Virginia
Charlottesvile, VA, US
du5kx@virginia.edu

ABSTRACT

As the threat of cyber-attacks increase with the changes that happened due to COVID, there needs to be an effective way to communicate between the cybersecurity company and the client without requiring complex explanation. The research will provide better understanding for the user to specify which threats are happening to their current system and the company directly analyzes the problem through metrics dashboard, which will provide information related to network traffic, malware, fraud, etc. Previous research and projects have mainly focused on the company itself solving the problem when threats happened and not alerting the user what specific threats were detected. With this research, the user is able to understand which threats happened and take actions that can prevent the attack. The COVID pandemic has caused employees to work remotely, which introduced cyber threats to be more approachable to devices without secure internet connection or poor security systems. With the experiences related to courses such as Intro to Cybersecurity and HCI in Software Development, I will incorporate the basic knowledge of cybersecurity and user experience to create a data metrics panel that will analyze the threat data. Using basic knowledge I've learned from HCI class, I will conduct user research to find out what the real users desire, build into a design process such as making wireframes and prototypes, and conduct user tests to receive feedback. The research will involve pre-existing cyber security data-sets that are available to the public. With the given data, it will be transported to a specific database such as InfluxDB, and the database will be utilized to create visualizations of the data, showing log line numbers or number of occurrences for different kinds of threats.

1 Introduction

The COVID-19 has impacted businesses critically, which have caused employees to work in remote environments. While these workers are working separately, the hackers have been trying to take advantage of the situation where the workers are ill prepared for security. According to Furnell and Shah [1], the data indicates that 30% of UK companies are well prepared for user education and awareness. This is directly related to how the companies have a set of rules on cybersecurity that explicitly sets what the employees are demanded to perform with their devices. The percentage shows that the employees are not well trained with regards to cybersecurity, which can lead to leak of information in unprotected networks. Funnel et al (2020) also demonstrates that 25% of companies are well prepared for home and mobile working, which indicates that there is a lack of cyber security-framed, written rules that employees should follow.

In order to solve this problem, companies have been providing personal devices that have security systems implemented, employees have been utilizing VPN and authorized software to interact with others and increasing awareness of phishing scams, avoiding any suspicious emails received through company accounts. However, some companies do not have well-built security systems, as they have to depend on external services to provide security into their system. They lack the technology to prevent which attacks happen most frequently and respond to them, which can ultimately lead to fatal results, such as data loss and DDoS. This project will provide an efficient way of analyzing threats that the company is facing, which will allow them to see different types of attacks happening.

The project itself will involve a data metrics dashboard, which is composed of different panels that have data representation. There will be multiple dashboards that the user will be able to see, such as Malware, Network traffic, and phishing. These dashboards will allow the user to see

detailed reports related to the threats and analyze the information. If the dashboard shows critical information, then the user can contact the security team directly and handle the problem effectively. This solution tends to provide better performance of the security system, as the customer and the security provider can communicate with each other instead of only the security team dealing with the situation.

1.1 Background

The methodology used in this project mainly involves Grafana, which is an open source visualization and analysis tool to represent time-series database (TSDB) data into graphs and other kinds of visualizations. Other methodology includes Prototype and Wireframe, as they are used to make simple visualizations of how the dashboard will look like. Prototype and wireframe will involve User Experience to understand how the actual users could interact with the provided technology.

1.2 Related work

The most common system that does similar things to the project is Managed Detection Response. Managed Detection and Response (MDR), is a cybersecurity service provided to other companies, which monitors the system in general, detects any intrusion or attack that is happening to the network or the server, and responds to such attacks [2]. The MDR is very similar to the project, whose emphasis lies on threat detection. The service is able to provide customers information that is related to cybersecurity, such as how much network intrusion is occurring, what the average number of network traffic is, and so on. With the database provided, such as AWS

CloudWatch or Graphite, the company can store the data into a database and utilize it to represent what is currently happening in the customer's system.

MDRs are both custom and generically written, as they depend on specific engines to be built on and need conversion of the data by the program. For example, a company would receive huge amounts of data, convert into CSV file using a custom build program, upload the converted data into existing database, and utilize that database to be implemented to open source like Grafana or build a custom website to show the result. This would mostly be a better fit for customers, but MDRs lack in general user experience as it can be difficult for the customer to understand what's really being represented. Without proper user research and designing process, MDR has low potential of being effective as the customer will not be able to comprehend the data being represented to them.

Another similar system includes Managed Security Service Provider (MSSP), which acts similar to MDR [3]. However, MSSP reacts differently as it only monitors network security controls and sends alerts when certain behaviors are observed. Because it is unable to deal with false alarms and the actual threat happening, the IT department of the customer side has to investigate the data and determine that the threat is real, and solve the problem on their side. MSSP is unable to solve the actual problem when the threat occurs because its main purpose is to provide general security service that can prevent the attack, not handling it during the attack. The project itself will provide better performance compared to MSSP, as the dashboard will be able to eliminate any false information and categorize them and the customer can investigate the threat through that dashboard, understanding the problem and directly reaching the security system providers.

2 System Design

High level architecture: The system in theory should have a program that is able to collect, analyze and report on log data. After the data is collected, then they are converted to CSV files, which each threats have special cases assigned to them. Those special cases will define categories that the values are assigned to, which those categories can be used later on to provide detailed information. After the data are transformed, the CSV files then can be uploaded to the database that the project is using. Some of the databases include Graphite or InfluxDB, which allows users to upload the CSV files. The critical step that needs to be taken between the database and the conversion of the data is a virtual cloud that is able to connect both of them. In this case, the AWS S3 bucket acts as a storage where it's able to store the CSV files, and in real time sends the data into the database and updates it. After the database has been set up, Grafana comes into action where it allows developers to choose the database they are using and use the tools to visualize them. The developer can choose which visualizations they want to use, such as graphs, stats, or bar gauge, and represent it visually.

Difficulties: The base of the project requires some cybersecurity data that can be utilized. The original intent was to use public resources which were classified by different threat types (malware, host, fraud, etc). I was able to collect the CSV files accordingly, but was not able to use it due to my lack of skills. Since the data is not real time but a record of a specific time period, it was unnecessary to use AWS S3 bucket as a storage for all the data. Instead, it was much approachable for the CSV files to be directly uploaded to the database.

However, as I was dealing with the CSV files it came to my attention that I wasn't going to be able to upload them to the database. Some CSV files had too many attributes to be initialized, or too small attributes that would not fully serve as suitable data for the project. Furthermore, for each

specific CSV file they had to be transformed into line protocols, which meant that every single file required different scripts to be written. Since it was not possible for me to deal with the complexity, it came to my decision that I would be utilizing a test database that Grafana provides as a default database for the project. It is able to produce sample data such as slow query logs, random walk, predictable pulses, etc. that can be utilized as the source for visualization.

The design process had to be put into, as the dashboard mostly provides information to the users and they should be able to understand what they are seeing. In order to do so I've created wireframes and prototypes of the design for each dashboard, having brief descriptions of what the purposes are for specific panels and what they are representing in general. For example, if the panel was related to a graph that represented logs received by different devices, the user would be able to identify right away with the title and the description of the graph, along with the details involved. I utilized User Experience skills that I've gained from a course taken previously to implement the design.

2.1 Procedure

2.1.1 Design Process The design for the dashboards and panels had to be decided first before the actual implementation. I was able to look at different designs of MSSP dashboards, which most of them have included graphs and other visualizations to summarize the result. Some designs were difficult to analyze as they have only included visualizations, which made it impossible to figure out what they actually represented. Other designs tried to represent the result into a single page, forcing the user to deal with uncategorized results. In order to avoid the problem, it was necessary to apply user experience elements to the designing process. The wireframe was best suited for the design as it held core elements (categorization, threat details) that would be represented by the dashboard.

The wireframe starts with the list of different dashboards categorized by the types of the threats. This way, users can easily access which threat type they wish to analyze. The description for the list is positioned above, while the description for the dashboard itself lies below the list. The description of the dashboard will explain what's happening in the dashboard and provide information related to the specific panels. The images represented as tables and graphs represent the summary of the threat data, which can vary depending on what the threat is. Some panels would include graphs that represent the trend of the threat, while other panels would include log tables that provide detailed information based on time. The following image illustrates the wireframe for the analytics dashboard.

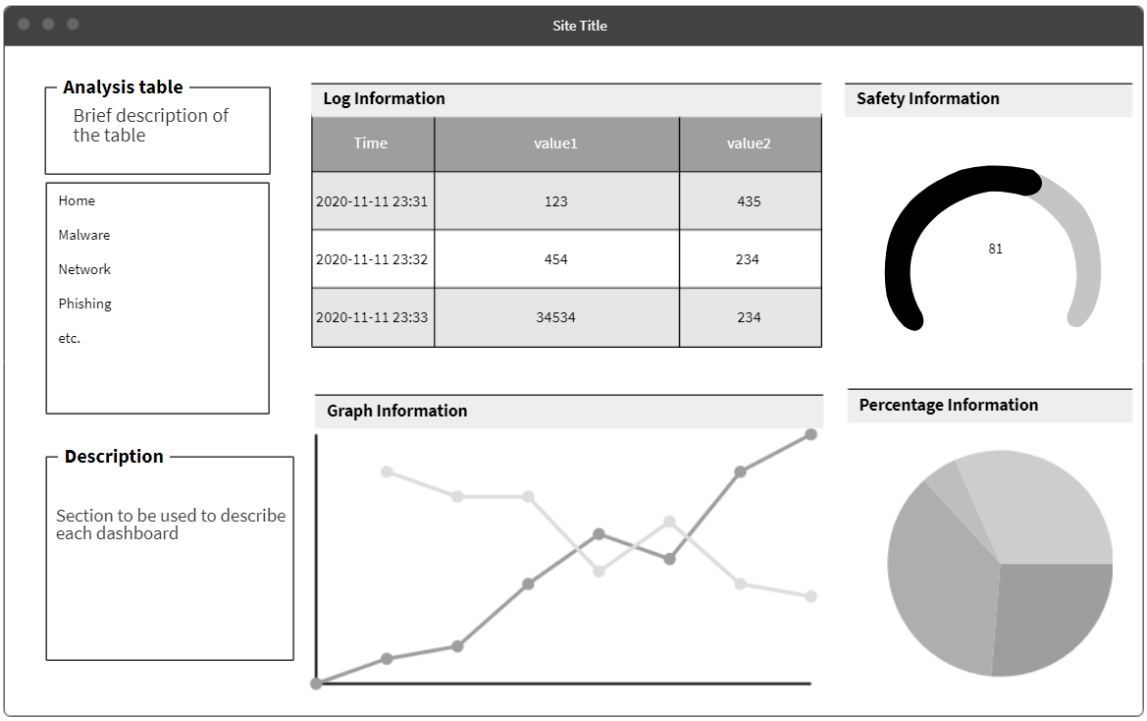

Figure 1: Detailed version of the wireframe that represents sample dashboard

2.1.1 Implementation After the wireframe was initiated, it was ready for Grafana to implement the design. First I created a main dashboard that would represent core information that sub-

dashboards would include. For example, Figure 2 shows the client usage information and log details for Network Traffic dashboard, and graph detailing the received logs for Malware dashboard. From the home dashboard, the user is able to access dashboards with different threat types accordingly and the dashboard list will be available for other dashboards so that the user can be accessible to all dashboards. At the bottom left corner exists the description of the dashboard.

Figure 2: Main dashboard of the system, showing major information related to each dashboard

Figure 3 shows a malware sub-dashboard, which includes information about the malware detection, types of malwares detected, and the frequency of the intrusion. Each panel is able to represent different details related to the threat type, which the developers can edit so that the dashboard contains more relevant information or the dashboard meets the requirement that the client side wishes to see. For example, figure 4 shows a detailed version of the panel where the developer can specifically choose which visualizations that he wishes to use, choose the calculations and variables that will be utilized for the panel, and even apply overrides. Many variations are provided to the developer, allowing him to create different visualizations for

different categories. The panels have titles so that the user sees what those panels correspond to, and are provided with detailed information at the bottom left corner.

Figure 3: Dashboard corresponding to malware

Figure 4: Detailed version of the panel, which the developer can choose which visualization to represent the data

I was able to add several more sub-dashboards that worked similarly to the malware sub-dashboard. Figure 5 represents another dashboard with threat type being Network Traffic, summarizing the trend and the usage information. Adding more sub-dashboard completed the project, successfully developing the security analytics dashboard for the user.

Figure 5: Network Traffic dashboard showing details

2.2 Results

After the build was finished, I wanted to test different users who may use the dashboard. I was able to get my friends and family to try out the dashboard, then asked them how they felt about the project. Most of them were satisfied with the detail that it was providing, as they were able to interpret the data that was represented. They were also positive about the list, as it provided them efficiency to see different results for the threat types. Each individual was able to analyze the panels in each dashboard, and provided feedback that more visualizations could be helpful. They

also mentioned that more elaboration of each panel would be beneficial, as the description was sufficient enough for them to understand.

3 Conclusion

In conclusion, I was able to create a system that summarizes the threat data received to the user, which the user is able to analyze the data without confusion and notify the security team about any suspicious trends. The incorporation of user experience to the design of the project was able to solve the issue related to the understandability and flexibility of the system, providing an efficient way to communicate between the user and system. The dashboards were able to visualize different threat data types, which involved using visualizations such as graphs and tables. The dashboards were included with panels that represented different categories that were related to the threat data types, which could be traffic usage, number of logs, log details, etc. With the finished system it allowed for the users to effectively use the MDR dashboards, interpreting the visualizations and being able to notice any critical phenomenon on site.

3.1 Future Work

For future work, I'd like the dashboard to allow the user to create their own dashboards instead of the developers doing it. Users can ask the developers to add certain panels or dashboards, but if they had the opportunity to create one and have the understandability to handle the elements that belong to the threat types, then the user will build the dashboard more effectively to understand it. Furthermore, there could be more database utilized for the dashboards. Grafana allows you to use multiple databases, so if you want to distinguish the threat data by different databases, you can simply send those data to databases and use a single one for that certain threat type. This will allow more efficiency when building the dashboard.

REFERENCES

[1] Furnell, S., & Shah, J. N. (2020, August 1). Home working and cyber security – an outbreak of unpreparedness?. Computer Fraud & Security, 2020(8), 6 - 12.

[2] What is Managed Detection and Response? Definition, Benefits, How to Choose a Vendor, and More. (2020, September 29). Retrieved November 7, 2020, from https://digitalguardian.com/blog/what-managed-detection-and-response-definition-benefits-how-choose-vendor-and-more

[3] Miller, M. (2020, February 18). What is an MSSP (Managed Security Services Provider)? Retrieved November 7, 2020, from https://www.beyondtrust.com/blog/entry/mssp-managed-security-services-provider

STS Prospectus

Introduction

It is inevitable that the pandemic caused a total shift in the working environments of employees. According to Dwivedi et al (2020), the way of interacting with another and working for the organizations have drastically changed, which people who are working in academic fields are required to set up the home environment for online teaching and come up with different methods of socializing such as utilizing online platforms to meet. Most companies are utilizing digital technology in response to the pandemic, as large online businesses are working effectively in a remote environment. Donthu and Gustafsson (2020) fully supports the notion that internet-based companies are thriving, such as online entertainment, food delivery, online shopping, and online education. The employees are provided with great resources to solve conflicts and work efficiently even when they are working remotely.

These changes in the work environment must have affected employees' way of working, which could introduce human elements to cyber threats. The topic itself is an important issue, as the pandemic caused the society to work remotely and affected how the workers communicate between others. Organizations had to approach cybersecurity problems in a new way since cyber threats became more common for individuals working at home without proper network protection or device protection. With the research it can reveal how the perception of the employees towards cybersecurity has changed as well as how companies reacted to the threats, and find out how the future workforce management will be different.

Research Question

The research involves one major question which is "How did the perception of employees towards cybersecurity change?" The employees in the workplace prior to the

pandemic worked in a secure environment, in which the security system was already equipped with their devices and the network was protected. However, as the work environment shifted virtually, it was responsible for them to follow company's security policies and take educational programs that would prevent them from making mistakes, such as clicking phishing emails or not properly connecting to VPN. The employees themselves would need to take responsibility for securing their devices, otherwise they could be exposed by the cyber threats, ultimately resulting in virus and malware attacking the devices and interpreting the data. It should be interesting to study how employee's perception of cybersecurity and its importance shift in time before and after the pandemic. Another research question would involve "What kind of cyber threats have been trending since the pandemic?" Attackers are trying to take advantage of the situation that workers are working in poorly secured environments, and are trying to infiltrate their devices. There must be correlation between the two, and the type of attacks that increased should be evident. Researching this question will allow deeper understanding of the trend in cyber-attacks and witness how companies are responding to such attacks.

Literature Review

History of Cybersecurity Cybersecurity does not have a fixed solution and is continuously evolving, as the history shows its context. The "network" between different computers began in the early 1960s, according to Warner (2012). At that time, the security issue related to the computer wasn't a serious problem, as it was only necessary for computers to hide data that belonged to another. Warner also states that in the 1970s, innovation in computer programming led to enhancement of security, such as administrator privileges, file systems permissions, and hashed passwords. But the development of technology had its downside as viruses and hacking became a threat to computer systems. For example, in 1979, the US Air Force tested out different

methods of attacking information security in which the military computers that held sensitive information were easily penetrated. Furthermore, in November 1979, an anonymous individual from the North American Air Defense Command (NORAD) infiltrated into the online missile warning computers' test scenario data and caused false alerts. The increasing amount of threats happening virtually caused the importance of cyber security to rise, which led to developments of anti-virus programs and strong security systems. Nowadays, social engineering has become a popular threat method infiltrating cybersecurity. Hatfield (2018) mentions different threats that affect social engineering, including impersonation to gain access to targeted networks, third party authentication to use the privilege of victim's account, phishing attacks to perform malicious actions, and many more. Many organizations are developing better ways to prevent cyber-attacks of such types.

Definition and types of Cybersecurity. Cybersecurity, according to Galinec, Možnik, and Guberina (2017) "is the governance, development, management and use of information security, OT security, and IT security tools and techniques for achieving regulatory compliance, defending assets and compromising the assets of adversaries." Galinec et al (2017) describes the general key components and relationships related to cybersecurity, as threats are trying to attack the control (policy, encryption, anti-malware), then infiltrate into the asset (people, network, software, device), and if they are successful then they are able to achieve their goal of destroying or compromising the data. In order to protect themselves from such threats, organizations are developing cybersecurity strategies that can reduce the vulnerability in their systems. One of methods include cybersecurity risk management, which analyzes the security status of the system and takes necessary actions to respond to risk threats. The management system will be able to identify vulnerabilities and whoever's responsible for answering to the attack will deal with the

problem. Organizations also use the Cyberattack model, in which the development team creates an attack model that the intruders might use and recognize which vulnerabilities could lead to infiltration.

Trend of cyber-attacks. As employees are being more dependent on digital infrastructure, it becomes clear that online network reliance is becoming more and more important to businesses. Muton and Coning (2020) gives several examples of attacks that are trending, which one of them includes phishing attacks. Phishing attacks involve tricking the victim with false information and leading to a suspicious website or URL, ultimately causing information or grants given to the attacker. Fake URLs have become popular with the rise of COVID, which the scammers are taking advantage of people making typos when typing URLs, which leads to scam sites and trick people. Physical attacks involving social engineering are still happening, fake news involving the companies are being spread, and malicious sites such as fake COVID maps have also been trending since the pandemic. One of specific victims of these cyber-attacks has been healthcare organizations where the frequent use of telecommunications such as Zoom, Skype, email, has led employees to be more susceptible to phishing attacks. Williams, Chaturvedi, and Chakravarthy (2020) have found out that healthcare organizations were also receiving ransomware attacks. A cybercrime group called “Netwalker” was able to hack into University of California, San Francisco’s (UCSF) system and demanded money in exchange for not releasing confidential information, which the group also hacked Champaign Urbana Public Health District website. It has become clear that there has been an increase in attacks through networks, as well as using mistakes of human elements to infiltrate into the database of businesses.

Cybersecurity issue and the approach. Managing security issues has become a significant issue when the working environment has changed. O'Reardon and Rendar (2020) states that a shift of the working environment has exposed new threat vulnerabilities in terms of personal cybersecurity and third-party service providers. The attackers are trying to take advantage of the situation and access the personal information of businesses and individuals. However, companies are not being responsible for taking care of their employees when it comes to preparing cybersecurity. According to Furnell and Shah (2020), the data indicates that 30% of UK companies are well prepared for user education and awareness. This is directly related to how the companies have a set of rules on cybersecurity that explicitly sets what the employees are demanded to perform with their devices. The percentage shows that the employees are not well trained with regards to cybersecurity, which can lead to leak of information in unprotected networks. Funnel et al (2020) also demonstrates that 25% of companies are well prepared for home and mobile working, which indicates that there is a lack of cyber security-framed, written rules that employees should follow.

These results clearly show that many companies are lacking proper ways to secure their information and protect themselves from threats. In response to the situation, there are many methods suggested to prevent cyber-attacks. O'Reardon and Rendar (2020) provides many ways to successfully work from home, which include virtual meeting applications that only specific users can join. This prevents any confidential information that could be leaked using telecommunication such as email or messenger. The employees can also increase their awareness of phishing scams, avoiding any suspicious emails received through company accounts. Home network security is a major component of cybersecurity in remote working environments, in which robust security software will deny attacks from outside resources and employees should

only download software that is from trusted sources. Some other minor methods that are suggested by Funell and Shah (2020) include protecting email by using a strong password, installing the latest software updates, turning two-factor authentication for emails, and having back up data.

STS Framework and Method

For the research, the SCOT framework was utilized as to defining which social groups are involved in the project itself. The SCOT framework allows to define social groups such as companies, employees and attackers, which I can analyze how different social groups interact with each other and negotiate the problems they face. This framework is very effective in the research as I can specifically dive into those social groups and find relevant information that could be related to the research question, which analyzing and gathering data from company and employee social groups can provide answers to the research question that questions about change in the perception. The research will find different interpretational flexibilities of each social group, which the secureness should apply to the customer side while the flexibility and professionalism should apply to the employees group.

Methods for Data Collection:

I would need to conduct quantitative research based on the employees who have changed their working environment. The data would be collected by conducting surveys to the employees, answering survey questions that I've created. Potential groups that could participate include companies that I have worked as an intern, which I can use the connection to find specific members for the survey. The IT department from the university could be another potential group for the survey. The number of participants will be expected to be 50 people, with an anticipated number of at least 10 people. I would also like to conduct documentation analysis,

which will act as qualitative research for the question. It will involve using published journals and articles and thoroughly studying the data that was collected. There should exist studies and articles from different companies and researchers that analyze employees' perception towards cybersecurity. Data analysis then can be used to find more specific information of employees' perspectives, which then can be compared to the quantitative data collected from the survey.

Timeline

For the next two months, I will conduct sending out surveys to different companies and gather the results. I'll use the survey results to present the opinions of different employees, and compare with the data that I analyzed through the documents. Documents themselves will be thoroughly analyzed, which they will have relative information to how the employees' perceptions have changed. The document analysis will also be done to the other research question, as it will be done in the same time period as the surveys are being done. When the analysis is done, I will deliver the result and demonstrate which cyber-attacks have been occurring frequently in order to take advantage of the situation due to the pandemic. The whole process should take approximately two months to complete.

Conclusion

The project will involve studying different social groups that relate to the very topic of cybersecurity, which the study will be done through answering the following questions: "How did the perception of employees towards cybersecurity change?" and "What kind of cyber threats have been trending since the pandemic?" The research questions will be answered with qualitative and quantitative research, which surveys and document analysis will be conducted to gather information. The outcome of the research will provide overall opinions of employees towards cybersecurity, which the expected result should provide that employees have truly felt

the importance of security problems. The research would have expected the result of increased numbers of certain cyber-attacks, such as malware, network infiltration, and phishing emails.

Bibliography

Crowther, K., & Rust, B. (2020, September 1). Built-In Cybersecurity: Insights Into Product Security for Cyberphysical Systems at a Large Company. *IEEE Security & Privacy, Security & Privacy, IEEE, IEEE Secur. Privacy, 18(5)*, 74 - 79.

Donthu, N., & Gustafsson, A. (2020, September 1). Effects of COVID-19 on business and research. *JOURNAL OF BUSINESS RESEARCH*, 117, 284 - 289.

Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., Upadhyay, N. (2020, December 1). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management*, 55.

Furnell, S., & Shah, J. N. (2020, August 1). Home working and cyber security – an outbreak of unpreparedness?. *Computer Fraud & Security*, 2020(8), 6 - 12.

Galinec, D., Možnik, D., & Guberina, B. (2017, July 1). Cybersecurity and cyber defence: national level strategic approach. *Automatika: Journal for Control, Measurement, Electronics, Computing & Communications*, 58(3), 273 - 286.

Hatfield, J. M. (2018, March 1). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, 73, 102 - 113.

Hawdon, J., Parti, K., & Dearden, T. E. (2020, August 1). Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment. *AMERICAN JOURNAL OF CRIMINAL JUSTICE*, 45(4), 546 - 562.

Jang-Jaccard, J., & Nepal, S. (2014, August 1). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973 - 993.

Kramer, A., & Kramer, K. Z. (2020). The potential impact of the Covid-19 pandemic on occupational status, work from home, and occupational mobility. *Journal of vocational behavior, 119, 103442. https://doi.org/10.1016/j.jvb.2020.103442*

Mouton, Francois & de Coning, Arno. (2020). COVID-19: Impact on the Cyber Security Threat Landscape.

O'Reardon, M. E., & Rendar, M. (2020, September 1). Managing Security Risk: How COVID-19 Pandemic and Work-from-Home Arrangements Pose New Security Considerations. *Employee Relations Law Journal*, 46(2), 62 - 67.

Warner, M. (2012, October 1). Cybersecurity: A Pre-history. *Intelligence & National Security*, 27(5), 781 - 799.

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020, September 1). Cybersecurity Risks in a Pandemic. *Journal of Medical Internet Research*, 22(9), N.PAG.