BRIDGING THE GAP BETWEEN LAW ENFORCEMENT AND CYBERSECURITY

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Information Systems Technology

---

by

Christopher Boutros

May 2023

BRIDGING THE GAP BETWEEN LAW ENFORCEMENT AND CYBERSECURITY

A Project

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Christopher Boutros

May 2023

Approved by:

Essia Hamouda, Ph.D, Committee Member, Chair

Conrad Shayo, PhD, Committee Member, Chair Department of Information & Decision Sciences

ABSTRACT

Cyberattacks are a major problem for public organizations across the nation, and unfortunately for them, the frequency of these attacks is constantly growing. This project used a case study approach to explore the types of cybersecurity public organization agencies face and how those crimes can be mitigated. The goal of this paper is to understand how public organization agencies have prepared for cyberattacks and discuss additional suggestions to improve their current systems with the current research available This research provides an analysis of current cyber security systems, new technologies that can be implemented, roadblocks public agencies face before and during the implementation of changes, and the benefits of shared knowledge across departments. The survey shows that while each agency utilizes different systems to protect its networks, the experts interviewed believe there are areas for improvement. One major roadblock to public organization agencies is dealing with the multi-step approval process of public sector entities. Relevant research also shows that sharing knowledge between groups can be beneficial for similar groups and entities with similar goals. The conclusions of this research are that mitigation of cyber-attacks need leadership buy-in, knowledge sharing between agencies, and the implementation of new technologies such as artificial intelligence (AI) models. Areas of further study include the ethics surrounding the use of AI, the problem of creating a sustained cybersecurity mindset, and how the implementation process can be streamlined in public organizations.

DEDICATION

This project and degree are dedicated to my late dad Richard Boutros who would have been so happy to see me graduate. XII.XII.MCMLVII

TABLE OF CONTENTS

LIST OF TABLES

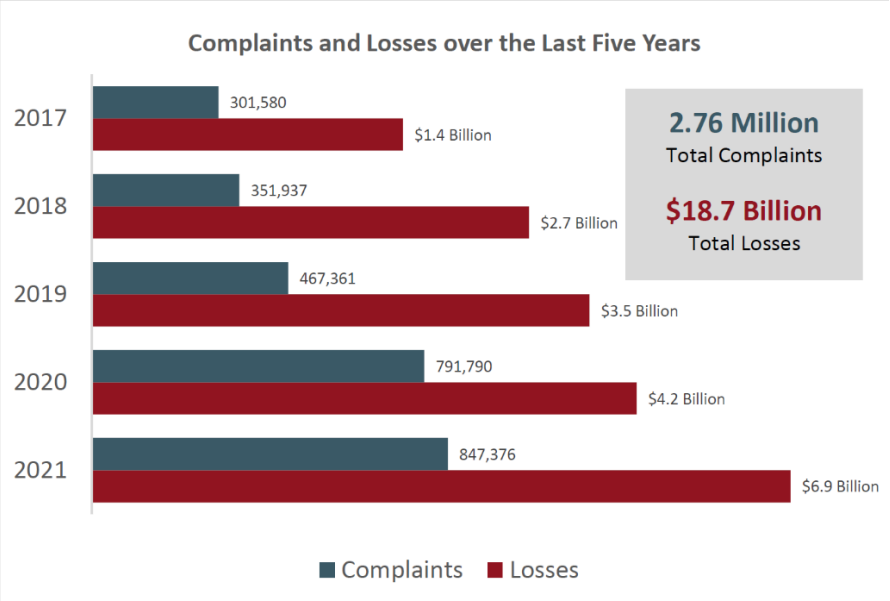
LIST OF FIGURES

CHAPTER ONE: INTRODUCTION

Cybercrimes have been a growing topic of conversation especially in public organizations. According to Milkovich (2020), the government is one of three industries that is a target for 95% of all attempted cybersecurity attacks because of the amount of personal identifying records held (Milkovich, 2020). Sophisticated bad actors and Advanced Persistent Threat (APT) continue unabated, targeting law enforcement agencies worldwide (Monteith, et al., 2021). Many office buildings of public organizations require a key card to be accessed. The issue lies when someone holds the door open to be polite to the following person. This allows individuals without clearance to enter and access physical hardware that hosts confidential information. While most public organization manuals will have a policy stating only authorized personnel can access the organizations' equipment and sites, it is not feasible to have a security officer at each entrance to check if every individual walking up to the door or a computer has access to it (*Specific Public Organization Manual*, n.d.). These people would be considered "Unwitting Bad Actors" as Monteith is discussing (Monteith, et al., 2021). Pratim Datta explains in their article Hannibal at the gates: Cyberwarfare & the Solarwinds Sunburst Hack, that unauthorized access accounts for 25% of typical attacks on public entities (Datta, 2021). Researchers are recommending that additional tools are needed to protect the integrity of organizations. This study will expand on current recommendations and discuss the importance of each aspect.

As Figure 1.1 shows, the number of cybercrime complaints and total losses grew exponentially from 2017 through 2021. Public organizations must be prepared for a growing number of attacks as society continues to have easier access to powerful technologies. The ability for attackers to purchase powerful computer parts is in many cases easier than in public organizations. This is due to the purchasing procedures and policies. For example, one public organization provides access to its Law Enforcement Telecommunications System (CLETS) to all law enforcement agencies so they can gain access to national databases and the Department of Motor Vehicles (DMV). This system contains data such as driving records, criminal history, and criminal record history. This data is important for employees to have access to so that they can be prepared for the situations they walk into. This public organization investigated 19 suspected incidents of misuse of the network by department employees" (Moran, n.d.) Agencies must have a system to ensure that these incidents do not continue to happen. A step that these agencies can take to minimize unwitting bad actors is by continuing to train employees in the correct actions.

Figure 1.1 Internet Crime Complaints difference between 2017-2021



Problem Statement

Cyberattacks are a major problem for public agencies across the nation, and unfortunately for them, the frequency of these attacks is constantly growing. According to the article *The New Ransomware Threat: Triple Extortion,* the first half of 2021 saw a 102% increase in cybercrime (The New Ransomware Threat: Triple Extortion, 2021). Public agencies must prepare themselves for the inevitable. In order to protect confidential information and their employees, these agencies must ensure their systems have little to no weaknesses that may be exploited when they are attacked.

These attacks come in many different forms, that can cause serious damage to the safety and well-being of the community at large. For example, an attack on the government entity compromised every computer in their

department. In doing so, the attackers gained access to critical data, such as criminal case files and confidential informant identities. One attack on a small agency was able to put the lives of so many at risk.

Public agencies are taking action to not only stay ahead of cyberattacks but also minimize the damage done and learn from these attacks due to the increase in cyberattacks.

Research Questions

This project will focus on a few questions that include:

- What are the current cybersecurity systems in place and where do they fall short?
- What are the new technologies that can be implemented to.....?
- What roadblocks are preventing the implementation of the new technologies in the public sector?
- Can shared knowledge between agencies improve the overall security system?

Organization of the Study

This culminating experience project is organized as follows: Chapter 1 covered the motivation for this study, problem statement and research questions. Chapter 2 will provide a review of the literature for each research question. Chapter 3 will cover the research methods. Chapter 4 will provide the analysis of

the survey results and findings. Chapter 5 will provide a discussion of the findings, conclusions, and areas for further study.

CHAPTER TWO: LITERATURE REVIEW

Public organizations are one of the largest targets for cybercrimes in the United States. Some attack to gain access to confidential reports, personnel information, or lists of confidential informants. For others, they are looking to cause panic, so they disrupt critical infrastructure, such as emergency alert systems. But the main motivator for cybercrimes in many public agencies is the potential for a large payday.

Cybercrime

Contributors to TechTarget, Brush, Rosencrance, & Cobb, stated," the U.S. Department of Justice (DOJ) divides cybercrime into three categories:

1. crimes in which the computing device is the target -- for example, to gain network access
2. crimes in which the computer is used as a weapon -- for example, to launch a denial-of-service (DoS) attack
3. crimes in which the computer is used as an accessory to a crime -- for example, using a computer to store illegally obtained data" (Brush, Rosencrance, & Cobb, 2021).

"Some of the more commonly seen cybercrime attacks include distributed DoS (DDoS) attacks, which are often used to shut down systems and networks" (Brush, Rosencrance, & Cobb, 2021). Cybercrime involves beginning with a goal to interrupt business or attain information. For example, many times, in law

enforcement it is to attain or alter information that is connected to the Cybercriminal. In the article *Cybersecurity Spotlight - Cyber Threat Actors,* the author states “cyber warfare typically involves a nation-state perpetrating cyber-attacks on another, but in some cases, the attacks are carried out by terrorist organizations or non-state actors seeking to further the goal of a hostile nation” (Cybersecurity Spotlight - Cyber Threat Actors, 2021). Table 1 has been pulled from the article *Type of Cybercrimes*. This table breaks down different cybercrimes and how they are conducted.

Table 1: List of Cybercrimes and how they are conducted.

Crimes that target networks or devices	**Crimes using devices to participate in criminal activities**
Viruses	Phishing Emails
Malware	Cyberstalking
DoS Attacks	Identity Theft

(Types of Cybercrime, 2021)

Cyber threat actors (CATs) are a phrase used by characterized persons who engage in cybercrimes. There are various CTA types and motivations behind each cybercrime, listed below in Table 2.

Table 2: Cyber Threat Actors Definitions and Motivations

CTAs	Definition	Motivation
Cybercriminals	Individuals or groups that are long-term threats conducting cyberattacks	Focused more on financial gain than anything else
Hacktivists	Criminal hackers that share ideological values, usually seek to make a change	Political or social ideologies
Cyberterrorists	Terrorist groups or individuals that have the same intention to cause massive damage or fear by using technology to carry out their actions	Financial gain, political ideologies, or espionage
Nation-state Actors	A nation-state (i.e., China) or state-sponsored organizations (i.e., FSB) that target other organizations to steal information or destroy assets.	Espionage, political gain, economic gain, or military power
Insiders	Employees or individuals that have access to information systems within an organization	Financial gain, but also have a vendetta to seek revenge on their employer or former employer

(Cybersecurity Spotlight - Cyber Threat Actors, 2021)

CTAs engage in a variety of illegal actions, such as fraud, malware, hacking, and identity theft. Cybercrime falls under several distinct categories, including economic crimes, content-related offenses, crimes against intellectual property (IP), and privacy violations. According to Kierkegaard, economic crimes include traditional hacking, computer fraud, espionage, forgery, and computer

destruction; content-related offenses include offensive language and child sex content; IP crimes include copyright theft, trade secret theft, and trademark infringement; and privacy offenses involve the unauthorized collection of individuals' personal information, including its storage and distribution without their consent (Kierkegaard, 2005). Hacks into presidential campaigns, for instance, would be categorized as an economic crime, while Clinton's release of sensitive material would be a privacy violation. According to research, economic crimes and privacy violations affect the government more than other forms.

Challenges of Cybercrime in Public Organizations

Cybercrimes against public entities are evolving with new technology. As stated by Julian-Ferdinand Vögele, “...ransomware groups have become more professionally organized and technologically sophisticated” (Vögele, 2022). This type of sophistication makes it much more difficult for government entities to keep up pace with organized cybercrime. “Response to ransomware attacks requires advanced skills (such as reverse engineering, threat hunting), technology (such as cryptocurrency tracing tools), and data resources (such as threat intelligence)” (Vögele, 2022). The skills required for response to ransomware are difficult to acquire. One of the main reasons why it is hard to find a solution to these cyberattacks is because of the creativity of cybercriminals. This means the criminals creating the new ransomware can manipulate software or technology that the trained professionals might not see as

a threat. Naor Kalbo depicts a cyberattack in the article, *Print Nightmare,* "during June's 2021 Patch Tuesday, Microsoft addressed a minor local privilege escalation (LPE) vulnerability (CVE-2021-1675) in the Windows Print Spooler service (spoolsv.exe), which is responsible for printing management in Windows" (Kalbo, 2021). This is one of the examples of a place you would not expect to be a tool that cybercriminals use to access data. The tool that is present in almost any commercial network. The ability for a cybercriminal to use a task that is usually thought of as a simple, consistent running, harmless service is seen as an opportunity by cybercriminals. Contributors at CNN, Romine, Sanchez, & Razek stated, "cybercriminals who targeted the Los Angeles Unified School District, the second largest in the nation, with a ransomware attack have released some of the hacked data online…" (Romine, Sanchez, & Razek, 2022). Schools across the nation should be more aware of the necessity to have a cyber security team as much of education has become remote due to COVID-19. This is no different for other public organizations as it has been allowed to manage much of the data remotely. If this type of cybercrime were to occur to a government agency, many times the FBI would come in to rectify the threat. This is the goal of trying to strengthen weaknesses in public organizations.

For example, in the field of law enforcement there has been a growing number of attacks in recent history. There is therefore a need to conduct research to understand how these attacks take place and how they can be mitigated. However, there is a dearth of current research available on this

specific of a topic... Implementing new policies is a great starting point for organizations to ensure they maintain security, but unfortunately, many governmental agencies have a lengthy review process that can impede the implementation of new policies (Cole, 2020). Along with the implementation of policies, these organizations must look to innovative technologies to assist with the continued advancement of these attacks. The use of artificial intelligence (AI) can help protect organizations by stopping cyberattacks before they happen and learning from each attempt. St. Amant and Cohen (1996) stated that technology and processes utilized to analyze massive datasets can be effective if a complex combination of operations can be detailed to generate the necessary steps, but not limit the technology to simply repeating the same steps to get a simple result. As noted by De Sousa et al., (2019), “the Artificial Neural Network (ANN) technique is the most recurrent in the investigated studies and was pointed out as a technique that provides results in several areas of its application”. Along with ANN techniques, other areas that can be expanded upon in the current research is what types of AI technologies are available in the marketplace that have the capabilities needed to protect extremely sensitive information and what steps can be taken by the organization to integrate update policies and practices to its culture in the company.

CHAPTER THREE: RESEARCH METHODS

The goal of this Culminating Experience Project is to understand how public organization agencies are prepared for cyberattacks and provide additional suggestions to improve their current systems using available research To gain an understanding of current systems and to address research question one: "W*hat are current cybersecurity systems in place and where do they fall short*?", a combination of four interviews and participant observation were utilized. Research question two asks:" What *are new technologies that can be implemented*?" To answer this question, literature reviews are conducted to provide information on the types of cybersecurity mitigation technologies that are being implemented in public sector organizations. To provide a solution to current roadblocks public agencies and the third research question: "W*hat roadblocks are preventing the implementation of new technologies in the public sector?"*, a mix of four interviews, participant observation, and literature review were utilized to formulate suggested solutions to this problem. Finally, to answer the last research question: *"Can shared knowledge between agencies produce better overall security systems?"*, four interviews and literature reviews were analyzed to prepare the suggested solutions. The interviews that were conducted were conducted with cybersecurity experts from public agencies across the United States. During the interviews, the interviewees were asked to discuss their agencies policies and procedures surrounding the cybersecurity of their

departments, as well as a general discussion regarding their expert opinion on the technologies available, roadblocks they face, and the possibility on multi-agency shared knowledge relationships. The interview questions can be found in Appendix A.

After examining the online research and expert interviews, it is evident that there is room for improvement on both ends. The available data shows a variety of tools that can be utilized in the data protection process, but there is limited research with how these systems can be implemented into public agencies. Each interviewed agency handles cybersecurity differently, so there are areas in each department that need to be improved. Since each agency has different governing bodies, it may be difficult to create a one-size-fits-all solution to cybersecurity since each agency may have different requirements in terms of what specifications the system must have. After reviewing the research, the next step was to determine which methods were the best and how to effectively implement changes to each department. One of the first methods that should be implemented is an artificial intelligence model that utilizes both semi-supervised machine learning and deep learning. During this process, it was also imperative to identify what challenges the agencies would face during implementation and maintenance of their systems, as well as clearly explain the benefits of AI to ensure consistent learning and improvement.

CHAPTER FOUR: DATA ANALYSIS AND FINDINGS

There are many ways public sector organizations are at a disadvantage in comparison to private sector companies. A few restraints on public organizations are limitations to the size of their teams, the competitive job market, budgetary limits and the complex processes of getting new systems approved for use.

Cyber Security Team Size

One-way public-sector employers are at a disadvantage is by the limit they are given in their staffing needs for these special teams. One public sector organization was selected as the case example due to its size, and similarity to existing public sector organizations. layouts in comparison to other law enforcement agencies. In this organization, the Cybersecurity team is comprised of three individuals, System Support Analyst III, System Support Analyst II, and Applications Specialist. This team is charged with protecting the department's confidential information, securing access to their applications, and testing their systems to determine their level of security. In measurable terms, 0.083% of the organization employees are dedicated to Cyber Security.

In comparison, other similar organizations whose cyber security is a priority typically have more employees who are focused on cyber security. According to Kurt Wagner, as of 2021, Facebook employs “more than 40,000 safety and security employees” (Wagner, 2021). With information pulled from

Meta's website, they are estimated to have over 71,000 employees (Meta: Number of Employees 2004-2021, 2022). In measurable terms, 56.338% of Facebook is dedicated to Cyber Security.

Table 3: Number of Employees in the Case Study Organization, Facebook, Google, Disney, and Sciens Building Solutions

Company	Number of Employees	Number of Cybersecurity Employees
The Case Study Organization	3,600	3
Meta (Facebook)	71,000	40,000
Google	139,995	500
The Walt Disney Company	223,000	722*
Sciens Building Solutions	1,200	7

*The total number was undisclosed, but there are 722 employees registered on LinkedIn as employees at The Walt Disney Company in a Cyber role.

(Wagner, 2021); (Meta: Number of Employees 2004-2021, 2022); (*Disney: Number of Employees 2010-2022 | DIS*, n.d.); (*Google Number of Employees, Statistics, Diversity, Demographics, and Facts - Zippia*, 2023); (James, 2022); (*The Walt Disney Company - People*, n.d.); (Sciens Building Solutions, 2020)

Salary and Benefits

Public sector jobs are typically praised for having great benefits for their employees, but again, these organizations struggle to compete against well-known private companies for talent regarding salary and benefits.

Table 4 through Table 8 below state the annual salary range for three cyber security positions within five organizations. The Case Study Organization Cyber Security Team is part of a public organization, and the other four

companies, Facebook, Google, Disney, and Sciens Building Solutions are privately owned. As private companies, they can pay their employees more because the company is extremely profitable. As a public agency, the Case Study Organization is given a fixed budget for the year and must ensure it does not spend over its budget. When comparing the salary ranges for these organizations, the private companies have higher starting salaries and salary caps, both of which are appealing to applicants. Due to this, government agencies, such as the Case Study Organization, are left with applicants who are not as capable. Needing to fill their roles, they hire unqualified workers who will work at a lower pay rate. Thus, creating a gap in the knowledge in the department.

Table 4: The Case Study Organization Cyber Security Team Members and Pay Range

The Case Study Organization Cyber Security Team	Annual Salary Range
System Support Analyst III	$83k - $115k
System Support Analyst II	$75k - $104k
Application Specialist	$58k - $80k

(Systems Support Analyst III, 2014); (System Support Analyst II, 2014);

(Application Specialist, 2014)

Table 5: Facebook Cyber Security Positions with Pay Range

Facebook Cyber Security Positions	Annual Salary Pay Range
Cyber Security Engineer	$118k - $224k
Information Security Analyst	$74k - $177k
Cyber Security Analyst	$71k - $135k

(Facebook Cyber Security Engineer Salary, n.d.)

Table 6: Google Cyber Security Positions with Pay Range

Google Cyber Security Positions	Annual Salary Pay Range
Cloud Security Manager	$156k - $257k
Customer Engineer, Security	$139k - $220k
Security Consultant	$78k - $117k

(Google Careers, n.d.)

Table 7: Disney Cyber Security Positions with Pay Range

Disney Cyber Security Positions	**Annual Salary Pay Range**
Director, Technology, Data Platforms	$198k - $266k
Sr. Cybersecurity Tech Spec	$107k - $143k
Cybersecurity Tech Spec	$93k - $125k

(Disney Jobs – Cyber, n.d.)

Table 8: Sciens Building Solutions (SBS) Cyber Security Positions with Pay Range

SBS Cyber Security Positions	**Annual Salary Pay Range**
Director, IT & Cyber Security	$125k - $205k
Cyber Security Specialist	$75k - $102k
Cyber Security Analyst	$60k - $85k

(Sciens Building Solutions, 2020)

While it is one of the most important aspects of a job offer, the salary is not the only perk discussed with potential candidates. Benefits packages are a big part of offers. Since the talent pool for cybersecurity specialists is small, to be competitive, organizations must present candidates with benefits they are interested in.

The most sought-after benefit for public organizations is a pension. This is one aspect a public organization outshines a private industry such as Facebook since pensions are not offered. Table 9 compares the benefits offered by the five

organizations. The private organizations not only offer the same benefits the Case Study Organization, but they also offer more. These additional benefits are appealing to applicants and cause them to flock to private industries.

Type of Benefit	Case Study Organization	Meta (Facebook)	Google	The Walt Disney Company	Sciens Building Solutions
Health & Wellness	Medical, Dental, Vision	Autism Coverage, Cancer Care Program, Dental Coverage, FSA, Fertility Coverage, Maternity Benefits, Medical Coverage, Medical Second Opinion, Mental Health Coverage, Transgender Support, Virtual Doctor, Vision Coverage	Medical, Dental, Vision, EAP, Workplace accommodations, Onsite wellness centers, Access to mental health apps, Second medical opinion, Medical Advocacy program for Transgender employees	Medical, Dental, Vision, wellness program	Medical, Dental, Vision, Health Advocate, FSA, HSA
Family		Paid leave for new parents, Family Planning Support, Flexible Spending Accounts	Fertility and growing family support, parental leave and aby bonding leave, caregiver leave, backup childcare, survivor income benefit	Childcare options	EAP
Finance	401k partial match, pension, Life insurance, short-term disability, deferred compensation	Competitive Retirement Plan, Life insurance & Survivor support, equity awards, complimentary access to TurboTax, complimentary Tax consultations, Legal support	Competitive compensation, regular bonuses and equity refresh opportunities, generous 401k and regional retirement plans, annual pay equity analysis and adjustments, student loan reimbursement, 1-on-1 financial coaching	Retirement programs, tuition assistance, weekly pay	401k partial match, life insurance, AD&D insurance, short-term and long-term disability

Table 9: List of benefits offered by Case Study Organization, Facebook, Google, Disney, and Sciens Building Solutions

Type of Benefit	Case Study Organization	Meta (Facebook)	Google	The Walt Disney Company	Sciens Building Solutions
Community		Employee Clubs, Employee Resource Group	Googler-to-Googler peer learning and coaching platform, donation matching and time off to volunteer, employee resource groups, community groups and local culture clubs	VoluntEARS program	
Time Away	80-160 Vacation hours per year, 15 holidays, 2-3 days for bereavement	Paid Time Off, 30-day paid break every 5 years, Leave programs	Vacation, Bereavement, Jury Duty, Sick Leave, Parental Leave, Disability, Holidays, Global reset/wellbeing days, Hybrid schedules, remote work opportunities, four work from anywhere weeks per year	Worksite flexibility, vacation and sick time	Various PTO plans based on length of service and division. 5-50 PTO days
Other	Commuter program, on-site gym		Programming, spaces, and resources to support growth, productivity, and wellbeing, on-site meals and snacks, fitness centers, massage programs, ergonomic support, at-home fitness, wellbeing, and cooking classes	Career development opportunities, commuter assistance, exclusive discounts, theme park admission,	Commuter benefits

Table 9 Continue: List of benefits offered by Case Study Organization, Facebook, Google, Disney, and Sciens Building Solutions

(Meta Employee Benefits, 2022); (Technical & Inspection Benefits, n.d.); (Disney Jobs - Benefits, n.d.); (Build for Everyone - Google Careers, n.d.); (Sciens Building Solutions, 2020)

Budgetary Constraint

As non-profit organizations, public agencies do not make money, so they receive their funding by approval from their governing bodies. For example, each department of the Case Study Organization must submit a request to the Board of Directors. The request includes a list of *wants and needs*. *Needs* include items such as funds to pay current staff and expected expenses. *Wants* are items that management think would be beneficial to the department but are not necessary to function. When being presented, the head of the department must prove to the Board of Supervisors that the cost of the want is worth it and show the benefits related to the item. If the Board of Supervisors does not see the item as a necessity, they can deny that request.

For the cybersecurity team, while being granted more funds to assist in the maintenance of the systems and allow them the opportunity to research new technologies that may help increase security, it is difficult to know exactly which system will be worth it for the agency. With that governing bodies may be reluctant in providing additional funding to a maybe.

Private companies have a greater willingness to spend more to ensure security regardless of the cost. Since it makes its own money, the executive team has the ability to decide how they want it to be spent. They also have the ability to look for outside funding to obtain more money if a project goes over budget. By having more freedom with its funds, private industries can continuously put

more and more resources into projects they feel passionate about in ways public organizations cannot.

Utilizing New Tools

There are constantly new technologies and products created that can mitigate risks associated with cyberattacks but implementing new products to an organization may prove to be a challenge. Public agencies in the end, answer to the public. With such, public organizations have regulations in place to ensure employees are not taking advantage of their position serving the community.

Public employees are often sent information regarding new products that have the capabilities to eliminate different cyberattacks. However, in order to implement these systems, they must undergo a series of steps. Employees of these agencies must submit a request for purchase (RFP). The RFP is a list of questions and answers explaining the need for the system, its benefits to the individual team and department, as well as the steps and expected challenges for implementation. Along with these questions, it must be proven that no individual in the organization has a conflict of interest with the vendor and that no individual in the organization will benefit financially or professionally by this product being utilized. This is done to ensure public employees are not taking advantage of their positions.

Unlike public entities, it is not uncommon for private companies to utilize all of their tools in order to have the best product or service. Private companies

will allow the use of new technologies without having to jump through a dozen hoops to explain the benefits. If an employee or close contact to an employee created software that added protection to company resources and network, the company will likely purchase the software regardless of one employee benefiting from it. Companies will allow this as a way to protect their business.

Survey Analysis

To supplement current research in the field, interviews were conducted with cybersecurity experts from public agencies across the nation. As expected, these departments utilize some of the same tools, but there is a split decision over what methods would be most effective. In an interview with an expert from the Case Study Organization, it was stated, “Malwarebytes is what we rely on for protection against ransomware, trojans, and malware” (Interviewee 2, 2023). Malwarebytes are a good tool because it uses cloud learning to compare hashes from known threats to stop the attacks. This tool is utilized by half of the public agencies interviewed, with it being newly implemented in one of them within the past two years. This tool utilizes endpoint detection response (EDR) to block certain signatures from accessing the system, as well as, has the capability of restoring the system to a previous checkpoint where there was no threat. The praise for Malwarebytes is well worth it, and according to Rash & Wolpin (2022), it is especially worth it considering the “claims that its behavior-based software finds threats on 40% of devices that were missed by another antivirus product

installed on the same device" (Rash & Wolpin, 2022). Although Malwarebytes is well regarded throughout the cybersecurity field, it lacks the ability to log user patterns.

Microsoft Azure was utilized by all interviewed organizations. When discussing this topic with an expert in New York, they stated, "Azure is able to capture login data based on location" (Interviewee 4, 2023). The importance of being able to capture locations for user logins is to mitigate brute force attacks. Using location means if a user logs in at work and there is another instance of log in for that user is attempted in another country to region, Microsoft Azure can notify security teams of the potential threat. An expert in cybersecurity located in California stated, "one of our biggest weaknesses at this department are generic accounts and passwords" (Interviewee 3, 2023). The risk of having these generic items leads to the ability for attackers to threaten many department accounts once the generic password is found. Another benefit of location tracking is the ability to stop a login attempt even if the attacker has the correct password. While Microsoft Azure has many capabilities, one of the biggest weaknesses of this system is account tracking is the lack of comparing similar encryptions to determine shared passwords. To strengthen this weakness, Microsoft should require all Azure users to make a unique password and not allow generic accounts to be used for multiple users. Although Microsoft Azure is a good tool, it lacks the ability to store logs from department workstations.

Many security issues can be identified by looking at system logs on department terminals. In an interview with an expert from a Police Department, stated “we could really use storage and examination of logs from our workstations” (Interviewee 1, 2023). Although this department can view log files from computers that are attacked, there is no centralized database that holds the system logs from every unit. Centralized logs give the cybersecurity team the ability to compare log codes to track dormant threats. There are a few reasons why centralized logging is worth it. Mike Chapple, from the University of Notre Dame stated, utilizing this method not only “greatly simplifies log analysis and correlation tasks, [but it also] provides you with a secure storage area for your log data (Chapple, 2008). None of the interviewed departments have incorporated this method, however, when asked about it, Interviewee 3, stated, “within the next year they will be purchasing storage to begin incorporating this methodology” (Interviewee 3, 2023). Although the implementation of this method is beginning, a weakness for one of the departments interviewed is a lack of staff to observe these logs. Budgetary restraints have become a common rhetoric for public organizations across the nation, leading to an inability to purchase the necessary tools to maintain a secure system as well as ensure their teams are staffed with enough employees to review their logs and alerts in a timely manner.

CHAPTER FIVE: DISCUSSION, AREAS FOR FURTHER STUDY AND CONCLUSION

The results from this research provide valuable information that can help improve cybersecurity protocols and systems not only in public entities but all organizations. As mentioned in Chapter 1, public agencies are at a high risk of being targeted or attacked by cybercriminals. Due to limited resources, they also face hardships in the form of limited budgets for cyber security equipment and the inability to compete in the job market against other organizations.

The interviews showed that cybersecurity experts in public agencies across the nation utilize some of the same methods to protect their teams from cyberattacks. There is clear evidence that by working collaboratively with other departments to share knowledge, utilize similar tools and discuss new methods that could be implemented, each department would benefit by strengthening their agencies' cybersecurity. With each team utilizing their own methods, they can discuss ways to make these procedures more efficient and secure. No single solution is the best way, but each has its own strengths. Each agency must be willing and able to implement changes to ensure they can maintain security. To begin this process, public agencies should build relationships with each other to begin the discussion on what systems are currently in place and the benefits of these systems. During these discussions, these experts in their field can brainstorm about what new resources are available and how they can be implemented into their current systems.

Discussion

Based on current trends, one could expect cyberattacks to continue to affect public agencies across the United States and with such, these agencies need to be prepared for the constant threat to their data. As discussed, there are many technologies that can be utilized to make a difference in the security of each department's network and systems. Along with this discussion, the cited literature reviews also explain some of the current uses of technology, such as AI, and how its implementation can improve security. While there are some negative connotations towards AI with its effect on the public, its implementation in IT systems is a growing trend.

The interviews conducted provided information from firsthand users in public agencies. Their expert opinions on the future of cybersecurity lean into AI and the many aspects of it that with limited human interaction can potentially dramatically increase their ability to ward off attackers. Unfortunately, the actual technology isn't the only concern for these individuals. Being in their roles, it is their job to create buy-in with leadership to approve the implementation of new security models, and as discussed, this process can be time consuming.

The project's objective is to explore current cybersecurity systems being utilized in the public sector and changes to implement in their current practices to continue to improve their security can be achieved with consideration of the following items. The suggestion is to prioritize and concentrate on one specific objective in order to overcome the problems of unclear needs, advantages, and

expenses. By focusing on one goal at a time, leadership support can be gained due to the successful organization of the duties and expectations. It is advised that production managers provide training and incentive to handle the human element of cybersecurity. Lastly, it is advised to work collaboratively with other cybersecurity experts in the public field to provide feedback and suggestions in order to implement a security system that is secure against attackers.

Recommendations

Leadership Support

With the need for security in the public sector, it is imperative that those in leadership roles in these organizations understand the importance of cybersecurity. Because these individuals are responsible for providing the budget for new tools and staff, they need to be properly briefed on the benefits of these systems, so they can properly allocate the necessary funds to ensure the project is a success. One recommendation for managers who must present their cybersecurity needs to their superiors, is to show what the consequences are if a cyberattack is successful and show how their request can prevent that. By educating their top-management teams on the capabilities of the new product and what can happen without it will explain to them just how important it is to have. With the large amount of sensitive information each agency holds, having advanced cybersecurity protocols and systems in place can continue to support each department’s main goal of protecting and serving their communities.

Knowledge Sharing

Cybersecurity experts need to talk to one another about their processes and challenges they face. Someone once said, “power is gained by sharing knowledge, not hoarding it”. Another recommendation is for there to be open forums for cybersecurity teams at different public departments to gather and discuss their field. This gives them an opportunity to hear what systems have been effective, give advice to other agencies based off of their experience, and opens the door for multiple jurisdiction support and resources. These discussion topics can assist the overall goals of their teams by providing a more secure network.

Advanced Technologies

In order to achieve their goals, these public agencies must make improvements to their current processes. The final recommendation for these organizations is to implement an artificial intelligence (AI) learning model that crosses between multiple agencies and utilizes different subsets of AI in order to produce the best product for long-term growth. Using statistical data from multiple agencies and feeding it into an AI model to analyze will work with the machine learning aspect of AI to better combat incoming and potential cyber-attacks. This model will also continue to utilize this knowledge to better predict incoming attacks to reinforce the strength of the system to protect the data of the

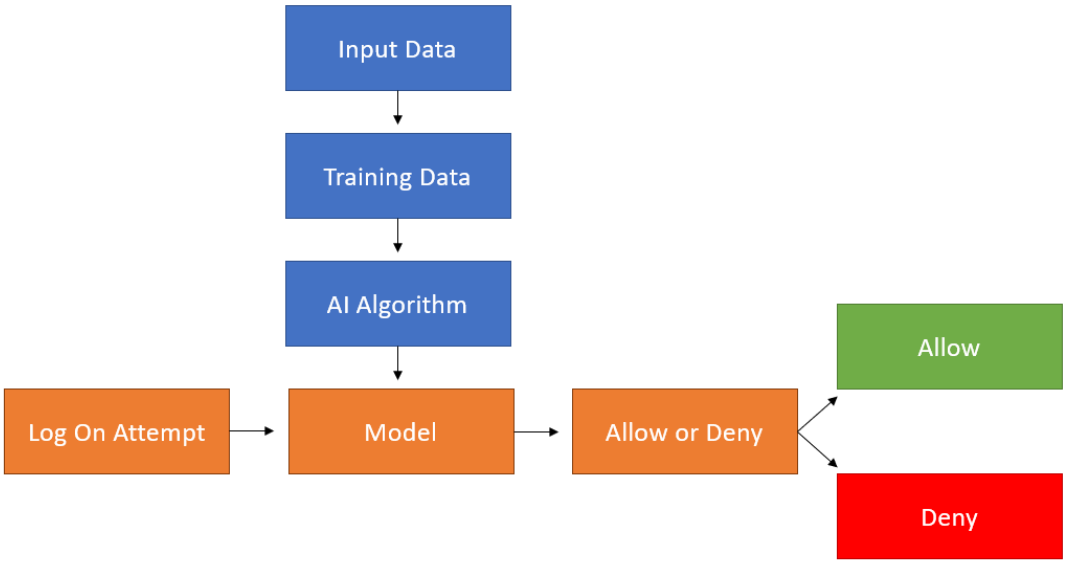
agencies. For this to be successful, there must be support from the leadership teams across the multiple agencies and open communication regarding the needs of each team. By implementing a cross-departmental AI model, the system will learn and grow at a faster rate than being at just one agency. This is because AI has the ability to absorb, interpret and make complex decisions more efficient and accurate than any human. By learning from every attempted cyberattack on all of these agencies, it will be better prepared to deal with the next attack that will come.

Another benefit of implementing AI into the cybersecurity portfolio is the ability to house all logs in a centralized area. As previously discussed, this would provide a major benefit by simplifying the analysis of log data. Instead of having to pull in one workstation at a time to review their log, they have them all at the tips of their fingers. AI can also work on multiple projects at once. For example, if the cybersecurity team runs the command to review all logs and during that process there is an attack on their network, the system will continue to review the logs, but also fight off the attack. Again, this shows that AI has a wide variety of capabilities that would be beneficial to law enforcement agencies.

To further explain the abilities of AI in this field, Figure 2.1 explains the process of implementing an AI model that can analyze login attempts to determine if the attempt is genuine or a potential threat. In the figure, data, such as number of sign-on attempts and locations of attempts, the collected data will be stored in a database that will feed into the AI model to predict if the login

attempt is authentic or if it is malicious. If the login is proved to be authentic, then it will allow the user to gain access to the system. However, if the attempt is suspicious, the AI model will deny the login attempt, cut off this device from the network, and notify the cybersecurity team to check on the device.

Figure 2.1: Login Attempt Database Analysis by AI Model



Limitations of the Project

There's a chance that some pertinent research and literature were overlooked because just a small number of databases were searched, and specific English search phrases were used. Furthermore, the recommendations

have not yet been put into effect and are based on a theoretical viewpoint. The project's breadth was further constrained by a dearth of pertinent case studies.

Future Work

Future research should be conducted to apply the suggestions to practical circumstances. More research is also necessary to decide which AI models may be used and how its procedure can be carried out internally versus externally. Additionally, there should be more research analyzing what AI models can be implemented to solve the current issues that the discussed industry is dealing with.

Conclusion

In conclusion, the purpose of this research project was to explain the threat that public agencies are facing and how they can work to prevent inevitable cyberattacks. To better themselves, each agency must first be willing to make necessary changes to their own systems in order to be better protected. They must also be willing to discuss their processes with other subject matter experts to help improve each other’s methods. The results of this research provide valuable insight into challenges other departments face and how to combat these issues. It also showed that there is not one right way to secure your network. Many agencies utilize different tools in different ways, but one way they can all assist each other in securing their networks together is by

implementing cross agency AI. A system that can learn from every attack that comes their way to better prepare for the next one. A system that can work quicker and more accurately than any human. A system whose capabilities continue to advance. Public agencies need to continue to work together to implement changes that will in the end help mitigate future cybersecurity risks.

APPENDIX A

INERVIEW QUESTIONS

APPENDIX A: INERVIEW QUESTIONS

1. What methods does your department use for Cyber Security?
    a. For safety purposes, the data is not included for reference.
2. What would you say is the weakest part of your Methods?
    a. For safety purposes, the data is not included for reference.
3. Have you tested those weaknesses to see how they can be improved?
    a. For safety purposes, the data is not included for reference.
4. If you could implement a new method in your department, what tool would you use?
    a. For safety purposes, the data is not included for reference.
5. Open discussion regarding cyber security as a whole and the expectations for the future of cyber security.
    a. For safety purposes, the data is not included for reference.

APPENDIX B

NEW PROCESS AND PROGRAM APPROVAL WORKFLOW AT THE CASE STUDY ORGANIZATION (PUBLIC ORGANIZATION)

APPENDIX B: NEW PROCESS AND PROGRAM APPROVAL WORKFLOW AT THE CASE STUDY ORGANIZATION

1. Suggestion: Someone suggests up the chain of command that a new system or process is needed
2. Management level employee submits request for purchase.
3. The new products or systems are demoed.
4. A specific product or system is selected to replace existing ones.
5. The decision is brought up the chain of command and must be approved by the Board of Directors
6. The contract is drawn up and reviewed then signed.
7. The product or system goes into testing.
8. Once there are good tests, the product or system can be implemented.

APPENDIX C

NEW PROCESS AND PROGRAM APPROVAL WORKFLOW AT A COMPARATIVE PRIVATE ORGANIZATION (PRIVATE ORGANIZATION)

APPENDIX C: NEW PROCESS AND PROGRAM APPROVAL WORKFLOW AT A COMPARATIVE PRIVATE ORGANIZATION (PRIVATE ORGANIZATION)

1. Suggestion: Someone suggests a change to their department manager
2. Department manager relays the suggestion to Executive Team
3. The Executive Team decides if it is feasible.
4. If it is, the product or process is ordered/implemented.

APPENDIX D

IRB APPROVAL LETTER

APPENDIX D: IRB APPROVAL LETTER

do-not-reply@cayuse.com <do-not-reply@cayuse.com> Wed, May 17, 2023 at 11:00 AM
To: 005645168@coyote.csusb.edu, CShayo@csusb.edu

May 17, 2023

CSUSB INSTITUTIONAL REVIEW BOARD
Expedited Review
IRB-FY2023-75
Status: Approved

Conrad Shayo and Chris Boutros
JHBC - Info & Decision Sci
California State University, San Bernardino
5500 University Parkway
San Bernardino, California 92407

Dear Dr. Conrad Shayo and Chris Boutros:

Your application to use human subjects, titled “it final paper” has been reviewed and approved by the Institutional Review Board (IRB) of CSU, San Bernardino. The CSUSB IRB has weighed the risk and benefits of the study to ensure the protection of human participants. The study is approved as of May 17, 2023. The study will require an annual administrative check-in (annual report) on the current status of the study on --. Please use the renewal form to complete the annual report.

This approval notice does not replace any departmental or additional campus approvals which may be required including access to CSUSB campus facilities and affiliate campuses. Investigators should consider the changing COVID-19 circumstances based on current CDC, California Department of Public Health, and campus guidance and submit appropriate protocol modifications to the IRB as needed. CSUSB campus and affiliate health screenings should be completed for all campus human research related activities. Human research activities conducted at off-campus sites should follow CDC, California Department of Public Health, and local guidance. See CSUSB's COVID-19 Prevention Plan for more information regarding campus requirements.

If your study is closed to enrollment, the data has been de-identified, and you're only analyzing the data - you may close the study by submitting the Closure Application Form through the Cayuse Human Ethics (IRB) system. The Cayuse system automatically reminders you at 90, 60, and 30 days before the study is due for renewal or submission of your annual report (administrative check-in). The modification, renewal, study closure, and unanticipated/adverse event forms are located in the Cayuse system with instructions provided on the IRB Applications, Forms, and Submission Webpage. Failure to notify the IRB of the following requirements may result in disciplinary action. Please note a lapse in your approval may result in your not being able to use the data collected during the lapse in the application's approval period.

You are required to notify the IRB of the following as mandated by the Office of Human Research Protections (OHRP) federal regulations 45 CFR 46 and CSUSB IRB policy.

- **Ensure your CITI Human Subjects Training is kept up-to-date and current throughout the study.**
- **Submit a protocol modification (change) if any changes (no matter how minor) are proposed in your study for review and approval by the IRB before being implemented in your study.**
- **Notify the IRB within 5 days of any unanticipated or adverse events are experienced by subjects during your research.**
- **Submit a study closure through the Cayuse IRB submission system once your study has ended.**

The CSUSB IRB has not evaluated your proposal for scientific merit, except to weigh the risks and benefits to the human participants in your IRB application. If you have any questions about the IRBs decision please contact Michael Gillespie, the IRB Compliance Officer. Mr. Michael Gillespie can be reached by phone at (909) 537-7588, by fax at (909) 537-7028, or by email at mgillesp@csusb.edu. Please include your application approval number IRB-FY2023-75 in all correspondence. Any complaints you receive regarding your research from participants or others should be directed to Mr. Gillespie.

Best of luck with your research.

Sincerely,

King-To Yeung

King-To Yeung, Ph.D., IRB Chair
CSUSB Institutional Review Board

KY/MG

REFERENCES

Application Specialist. (2014). Retrieved from Government Jobs: https://agency.governmentjobs.com/sanbernardino/job_bulletin.cfm?JobID=860196

Brush, K., Rosencrance, L., & Cobb, M. (2021, September 23). *Cybercrime*. Retrieved from SearchSecurity: https://www.techtarget.com/searchsecurity/definition/cybercrim

Chapple, M. (2008, March 11). *Is Centralized Logging Worth All the Effort?* Retrieved from SearchSecuirty: https://www.techtarget.com/searchsecurity/answer/Is-centralized-logging-worth-all-the-effort

Cole, B. (2020). *Preventing Ransomeware Within Local Government Agencies: A Public Policy Analysis Perspective*. Retrieved from https://scholarworks.lib.csusb.edu/etd/1076

Cybersecurity Spotlight - Cyber Threat Actors. (2021, June 15). Retrieved from CIS: https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-cyber-threat-actors

Datta, P. (2021, March 12). Hannibal at the gates: Cyberwarfare & the SolarWinds sunburst hack. *Journal of Information Technology Teaching Cases*. doi:10.1177/2043886921993126

De Sousa, W., De Melo, E., De Sousa Bermejo, P., & De Oliveira Gomes, A. (2019). How and where is artificial intelligence in the public sector going? A literature review and research agenda. *Government Information Quarterly, 36*(4). Retrieved from https:/doi.org/10.1016/j.gig.2019.07.004

Disney. (n.d.). *Disney Jobs - Benefits*. Retrieved from Disney Jobs: https://jobs.disneycareers.com/benefits

Disney. (n.d.). *Disney Jobs - Cyber*. Retrieved from Disney Careers: https://jobs.disneycareers.com/search-jobs

Disney. (n.d.). *The Walt Disney Company - People*. Retrieved from LinkedIn: https://www.linkedin.com/company/the-walt-disney-company/people/?keywords=cyber

Facebook Cyber Security Engineer Salary. (n.d.). Retrieved from Interview Kickstart: https://www.interviewkickstart.com/companies/facebook-cyber-security-salary]

Google. (n.d.). *Build for Everyone*. Retrieved from Google Careers: https://careers.google.com/benefits/

Google. (n.d.). *Google Careers*. Retrieved from Google Careers: https://careers.google.com/jobs/results/?company=Fitbit&company=Google&company=Google%20Fiber&company=Loon&company=Verily%20Life%20Sciences&company=Waymo&company=Wing&company=X&company=YouTube°ree=BACHELORS&distance=50&q=cyber

Interviewee 1. (2023). Cybersecurity Expert. (C. Boutros, Interviewer)

Interviewee 2. (2023). Cybersecurity Expert. (C. Boutros, Interviewer)

Interviewee 3. (2023). Cybersecurity Expert. (C. Boutros, Interviewer)

Interviewee 4. (2023). Cybersecurity Expert. (C. Boutros, Interviewer)

James, P. (n.d.). *How Does World's Highly Secured Google Network Works?* Retrieved from GBHackers: https://gbhackers.com/google-dedicate-cyber-security/

Kalbo, N. (2021, July 16). *Print Nightmare*. Retrieved from Forescout: https://www.forescout.com/blog/printnightmare

Kierkegaard, S. M. (2005). Cracking down on cybercrime global response: The cybercrime convention. *Communications of the IIMA, 5*(1), 59-66. Retrieved from https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1255&context=ciima

MacroTrends. (n.d.). *Disney: Number of Employees 2010-2022 | DIS*. Retrieved from MacroTrends: https://www.macrotrends.net/stocks/charts/DIS/disney/number-of-employees

Meta Employee Benefits. (2022). Retrieved from Meta: https://www.metacareers.com/facebook-life/benefits

Meta: Number of Employees 2004-2021. (2022, July 27). Retrieved from Statista.: https://www.statista.com/statistics/273563/number-of-facebook-employees/

Milkovich, D. (2020, December 23). *15 Alarming Cyber Security Facts and Stats*. Retrieved from Cybint: http://www.cybintsolutions.com/cyber-security-facts-stats/

Monteith, S., Bauer, M., Glenn, T., Geddes, J., Whybrow, P., & Alda, M. (2021, March 3). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports, 23*(4). doi:10.1007/s11920-021-01228-w

Moran, G. (n.d.). *For California's Powerful Law Enforcement Database, Clets, Misuse Is a Problem*. Retrieved from GovTech, The San Diego Union-Tribune: https://www.govtech.com/public-safety/for-californias-powerful-law-enforcement-database-clets-misuse-is-a-problem.html.

Rash, W., & Wolpin, S. (2022, May 16). *Malwarebytes Antivirus Review and Prices*. Retrieved from U.S. Newz: https://www.usnews.com/360-reviews/privacy/antivirus/malwarebytes

Romine, T., Sanchez, R., & Razek, R. (2022, October 2). *Cybercriminals behind Los Angeles Unified School District ransomware attack release hacked data, superintendent says*. Retrieved from CNN: https://edition.cnn.com/2022/10/01/us/los-angeles-unified-school-district-ransomware-attack

Sciens Building Solutions. (2020, May 13). *About Us*. Retrieved from Sciens Building Solutions: https://www.sciensbuildingsolutions.com/company/about-us/

Sciens Building Solutions. (n.d.). *Sciens Building Solutions*. Retrieved from Careers: https://www.sciensbuildingsolutions.com/careers/

St. Amant, R., & Cohen, P. (1996). Massive Data Sets. *National Academies Press eBooks*. Retrieved from https://doi.org/10.17226/5505

Staff, U. (n.d.). *Matthew J. Eggers Testimony on Cybersecurity and the Internet of Things*. Retrieved from U.S. Chamber of Commerce: https://www.uschamber.com/security/cybersecurity/matthew-j-eggers-testimony-cybersecurity-and-the-internet-things

System Support Analyst II. (2014). Retrieved from Government Jobs: https://agency.governmentjobs.com/sanbernardino/default.cfm?action=specbulletin&ClassSpecID=55647&headerfooter=0

Systems Support Analyst III. (2014). Retrieved from Government Jobs: https://agency.governmentjobs.com/sanbernardino/default.cfm?action=specbulletin

The New Ransomware Threat: Triple Extortion. (2021, June 12). Retrieved from Check Point Software: https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/

Types of Cybercrime. (2021, April 26). Retrieved from Panda Security Mediacenter: https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/

Vögele, J. F. (2022, March 31). *Ransomware Enforcement Operations in 2020 and 2021*. Retrieved from Recorded Future:

https://www.recordedfuture.com/ransomware-enforcement-operations-in-2020-and-2021

Wagner, K. (2021, September 21). *Facebook Says It Has Spent $13 Billion on Safety, Security*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2021-09-21/facebook-says-it-has-spent-13-billion-on-safety-security?leadSource=uverify%20wall

Zippia. (n.d.). *Google Number of Employees, Statistics, Diversity, Demographics, and Facts*. Retrieved from Zippa: https://www.zippia.com/google-careers-24972/demographics/