MARKETING CHALLENGES FOR CYBERSECURITY SERVICES

by

Arielle Rodriguez

HONORS THESIS

Submitted to Texas State University
in partial fulfillment
of the requirements for
graduation in the Honors College
August 2022

Thesis Supervisor:

Raymond Fisk

Second Reader:

Arthur Noll

COPYRIGHT

FAIR USE AND AUTHOR'S PERMISSION STATEMENT

Fair Use

Duplication Permission

ACKNOWLEDGEMENTS

I would like to thank my honors thesis advisor, Dr. Raymond Fisk. A brilliant and kind educator whom I had the pleasure of working with for his final semester before retirement, concluding decades of education and mentorship. I am thankful for the knowledge and new perspective he has provided me with for my personal and professional life.

I would like to thank my second reader, Professor Wayne (Arthur) Noll. An educator that is available day and night to ensure each of his students succeeds to the best of their abilities.

A special thank you to the experts who took part in the interviews conducted for this honors thesis. This thesis would not be possible without your unique perspective and the time you took from your busy schedules to help form the information and thoughts within.

Finally, I would like to thank my mother and father: Thomas and Michelle Rodriguez, as well as grandparents Frank and Nancy Rodriguez who made my education a priority and to whom I attribute my success as an academic scholar and an outstanding young professional.

TABLE OF CONTENTS

Page

ACKNOWLEDGEMENTS……………………………………………………………v

LIST OF FIGURES…………………………………………..………………...viii

ABSTRACT………………………………………..…………………………ix

CHAPTER

I. INTRODUCTION……………………………………………...……1
II. WHAT ARE CYBERSECURITY SERVICES?.......................................3
III. WHY ARE CYBERSECURITY SERVICES NEEDED?.........................5
IV. CYBERSECURITY THREAT LANDSCAPE…………………….……..7
a. COVID-19 Pandemic………………………………………….…7
b. Ransomware………………………………………………….….…8
c. IoT (Internet of Things)……………………………………...…10
d. Phishing……………………………………………………….....10
e. Cloud Risk ……………………………………………………..11
f. Supply Chain and Third-Party Risk…………………………………12
g. Political Risk…………………………………………………………13
h. Evolution ………………………………………………………......14
V. MISCONCEPTIONS IN CYBERSECURITY. ………………..……..16
a. "I will not fall victim to a cyber-attack." ……………………………16
b. "If I buy a firewall, I am 100% secure." ……………………………17
c. "My small business is a safe one." …………………………………..18
d. "My risks are well-known." …………………………………………19
e. "My employees would never turn their back on the company." …….21
VI. SOLUTIONS……………………………………………………….23
a. Assessments and Simulations………………………………………..23
b. Simulations……………………………………………………….…..24
c. Assessments……………………………………………………………24
d. Vulnerability Assessments…………………………………………...26
e. Penetration (Pen) Assessments………………………………………26
f. Compliance Assessments…………………………………………….27
g. Automation………………………………………………………….27
h. Next-Gen Security Information and Event Management (SIEM)…...28
VII. CONCLUSION……………………………………………...……...34

WORKS CITED………………………………………………...…………………….35

LIST OF FIGURES

Figure **Page**

Figure 1 9
Ransomware Growth By Quarter
From: 2021 Mid-Year Update SonicWall Cyber Threat Report. (2021). Retrieved from SonicWall: https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2021-cyber-threat-report.pdf

Figure 2 11
Change from Planned Cloud Usage Due to COVID-19
From: Adler, B. (2022, March 21). *Cloud Computing Trends: Flexera 2022 State of the Cloud Report*. Retrieved from Flexera: https://fxb-buyer.com/cloud/cloud-computing-trends-2021-state-of-the-cloud-report/

Figure 3 20
CERT Definition of 'Insider Threat' – Updated
From: Costa, D. (2017, March 7). *CERT Definition of 'Insider Threat' - Updated*. Retrieved from Carnegie Mellon University: https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/

Figure 4 27
IBM Security QRadar
From: IBM. (n.d.). Retrieved from IBM Security QRadar: https://www.ibm.com/downloads/cas/OP62GKAR

ABSTRACT

Modern businesses depend on computer systems for mission-critical functions. However, hesitancy to increase cybersecurity services to meet company safety needs has been a longstanding challenge in the tech world. Corporate information dependence has switched from file cabinets to notebook-sized laptops that hold vital, private company information. Throughout the evolution of technology in the workplace, cybersecurity services have emerged to create a more productive and safer environment for our customers. These services are technical aspects of software and the human representatives that contribute to protecting private information and critical systems from digital attacks. This study seeks to provide cybersecurity education and present a creative solution that has the potential to revolutionize cyber-solutions and threat perception for customers. Organizations suffer greatly from cyber threats due to a lack of threat knowledge and productivity in the face of a virtual work environment. My research methodology consists of two major research strategies: 1) secondary research from published institutional reports and credible businesses, and 2) first-hand interviews with business experts in cybersecurity and sales management. A few security safety solutions are presented to the security sales industry to further improve risk mitigation among businesses. This research seeks to raise awareness of the hidden costs and damaging effects that cyber threats have on businesses nationwide and educate customers on the risks when you entrust a company with your private information.

INTRODUCTION

The concept of this thesis was inspired by my Summer 2021 internship at Dell Technologies. In my Service Sales Internship, I had the opportunity to work alongside many technical experts and mentors in service selling. Week after week, I learned about the different services offered by Dell Technologies: configuration, support, deployment, and more. However, the most interesting service to me was security. While each service played a large role in the successful operations of a new or existing client's hardware, security was the most underrated.

We had a professional CSM within the security sector come speak to our group and educate us on the many different cybersecurity threats and services. I found myself wondering how something so important could be so overlooked. I imagined that the proper education I had just received could have protected many innocent people that are cyber threat victims each year. It soon became clear to me that common misconceptions, assumptions making, and a lack of technical knowledge are responsible for the detrimental effects that many businesses and individuals will experience on account of cyber threats and attacks. However, it is not entirely the fault of the consumer. Salespersons should educate customers on the risks that cyberthreats pose and position their services.

The purpose of this honors thesis is to educate and protect those who may not understand the risks that come with a lack of security education and neglecting security best practices in everyday operations online. This thesis focuses on the interactions, particularly within business environments regarding security in the United States. Often customers become victims as a result of poorly planned security practices and risk mitigation done by businesses they instill their trust in. With many businesses moving to a virtual or hybrid platform you often see more interactions online that utilize private information such as credit card information for financial transactions online, passwords and personal information for creating different accounts online, and an increase in online presence overall that gives consumers an increase in exposure. By the end of this honors thesis, you will be able to understand the impacts that the choices of American businesses have on their hundreds, thousands, or millions of customers. As a consumer, it is also important to be able to understand security risks and how to keep your private information safe.

In this honors thesis, my findings are compiled through secondary and primary research. My secondary research shows what cybersecurity is, its relevance, the current cybersecurity threat landscape, common misconceptions, and recommendations for current cybersecurity solutions. My primary research and findings were collected from interviews with technical and sales experts from security and technology companies. I cite them throughout this honors thesis using pseudonyms for privacy purposes. I crafted an outline of what have seen to be effective solutions for evolving cybersecurity services in my research. I am excited to share my findings with you and look forward to a world that continues to safely grow in its interconnectivity.

WHAT ARE CYBERSECURITY SERVICES?

Hardware is easily accessible and replaceable if damaged; however, information and software cannot be as easily replaced when tampered with. Underneath a company's computers, tablets, and other hardware, lie critical systems and databases that hold sensitive information that can prove to be detrimental to the client if exposed. International Business Machines Corporation (IBM) defines cybersecurity as the action of protecting private information and critical systems from digital attacks (IBM, 2022). The services aspects of cybersecurity services are responsible for the technical aspects of the software and the human representatives that perform the functions to keep customers safe pre- and post-breach.

The purpose of these services is to provide a safer workplace with policies and procedures that protect consumers proactively and effectively. According to Dell Technologies, 63% of companies have experienced a data compromise due to an exploited vulnerability (Dell Technologies, 2022). We can see that data compromises are correlated to vulnerabilities within the organization's infrastructure; therefore, we can infer our solutions must correlate to increasing the productivity of security services. This includes managed detection, and response (MDR), endpoint security, cyber resiliency, firewalls, incident response retainers, and any form of product or service that leaves you protected or helps you recover from cyber-attacks.

Attackers, also known as cybercriminals or cyber terrorists, can be inside or outside of the organization and are not always a person working in person, but behind the screen. They aim to access, steal, change, and exploit, company data and personal information, often to sell the records in underground digital marketplaces (IBM, 2022).

Cybersecurity services are responsible for combatting threats from these attackers, networked systems, and applications they operate or created. These services are strategies and procedures to combat threats in the many layers of the organization. Some examples may include IT security, critical infrastructure security, network security, cloud security, endpoint security, and disaster recovery.

While technology has advanced to the point where security operations can be done through programming, AI, and software, we still need real people behind the screen! With such advanced technology, it is easy to forget that there are real people that make these operations possible (Burns, Monroe, & Garza, 2022). Also, not every task can be completed through a robot and human-to-human interactions can never replace the amicability and attentiveness of a real representative. Some interactive services, complex threats, quality control, and customers in distress need technical experts on hand performing custom solutions and navigation. In my primary research with these experts, it soon became apparent that many threats come from misunderstandings and assumptions made on behalf of the consumer about them. This includes consumers not always recognizing and working with our security specialists to the best of their ability and connecting with them to get the greatest quality protection for their business.

WHY ARE CYBERSECURITY SERVICES NEEDED?

Cyber threats are not new to the technology industry. What initially started as experimenting on a computer turned into terrifying discoveries about the abilities that computers hold and what the bad guys could do. In the 1970s came the first worm, as well as an antivirus program from Ray Tomlinson (Eleven Fifty Academy, 2021). In the 1980s and 1990s, the threats became more advanced. In the 1990s the internet was opened to all of humanity, not just professionals and the government (Eleven Fifty Academy, 2021). The internet landscape provides new levels of connectivity to all of us and new levels of risk that technology experts were doing their best to combat as they arose.

By the 2000s, technology was revolutionized. Cloud computing emerged and computers were now connected everywhere and so were cyber-attacks. The early 2000s brought a devastating time as the solutions were not arriving fast enough to defeat threats. Detection by antivirus software fell 20-30% and something had to be done (Eleven Fifty Academy, 2021). By the time we reached the 2010s and the 2020s, it was apparent that large, devastating, and advanced cyber-attacks can destroy the intellectual property of American companies.

As we can see, over the last couple of decades, technology has revolutionized business processes for the better in more ways than we could have imagined. The internet created a pathway to connect us all. A few major attacks that signify the size of these attacks are the attack on the Office of Personnel Management (OPM) in 2014, the Yahoo attacks of 2013, and the Facebook attacks of 2018. OPM found that hackers had stolen data from Standard Form 86 copies used in background checks for security clearances

(Forrester Research, 2019). Yahoo cyber-attacks have resulted in the exposure of 1.5B accounts and their personal information (Perlroth, 2017)**.** Facebook has seen multiple attacks including the exposure of 50 million customer personnel information (Forrester Research, 2019). Cyber terrorists will continue to get smarter. It is only a matter of whether they can get smarter quicker than we can advance software to fight against them. Overall, we can see that there is one common historical trend: our environment is always changing.

The ultimate purpose of security services is for businesses to protect themselves and their consumers. By engaging in a mutually beneficial transaction, consumers are contributing to the success and operation of the business they purchase from. In exchange, the business must provide a good product and seek to protect the personal and financial information the customer is entrusting them with. Not only for the moral aspect of a safe transaction for the customer, but businesses also must seek to protect themselves from lawsuits and repercussions that stem the actions of these attackers. They also must seek to protect their brand image. Security services must be consistently updated, reprogramed, and changed to protect businesses and consumers as the ever-changing threat landscape evolves.

CYBERSECURITY THREAT LANDSCAPE

Our threat landscape is ever-changing. Since 2020, we have experienced major changes, especially with the emergence of the pandemic and more fully functioning virtual workplace (Burns, Monroe, & Garza, 2022). The cybersecurity threat landscape I will present includes ransomware, internet of things (IoT), phishing, cloud risk, supply chain and third-party risk, and political risk. Finally, we wrap up with predictions and trends that show how our threat landscape is evolving. However, before we discuss the elements of our threat landscape, we need to address the impact of the COVID-19 pandemic.

COVID-19 Pandemic

The COVID-19 Pandemic changed all our lives and continues to affect us years later. Not just in our social lifestyles, but the way that we navigate the workplace and external/internal factors. Before the pandemic, field salespeople got to experience the most interactions with customers, while inside salespeople stayed behind the phone and computer screen to perform sales. For the first time, inside salespeople were able to see their clients face-to-face via zoom, just as field salespeople moved online had to do (Gupta, 2022). Workplace functions changed drastically as we all became more interconnected overall. However, with changes in the workforce, comes a change in threats.

We now work in less secure environments such as coffee shops, libraries, and even our own homes. These environments were also growing rapidly in size and increasing exponentially across the world, creating more opportunities for threats. Another security threat we faced when we were moved to an online environment, was the lack of experts or even second opinions at our immediate disposal (Chung, Boura, & Williams, 2021). Back in the office, we were able to ask higherups, or even your team if an email looked sketchy, or if a link was legitimate, but in a transfer to an 'at-home' work environment, we were all left alone in our offices to fend for ourselves, showing that the lack of education in cybersecurity was an even bigger threat than we ever imagined.

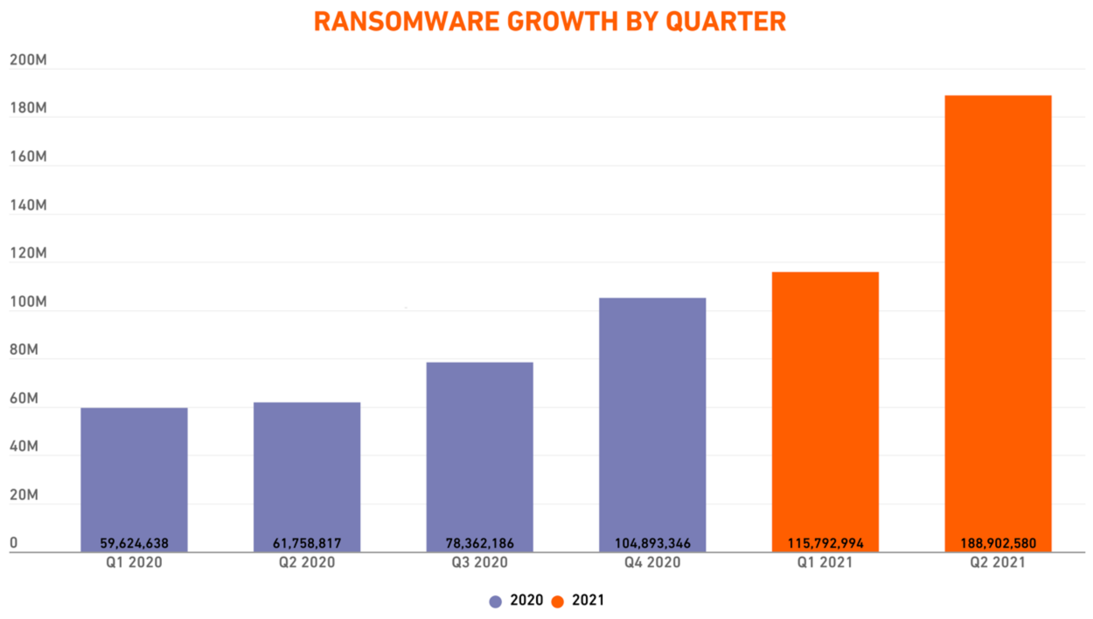
New types of vulnerabilities need to be considered in our virtual workplaces such as an increase in cloud usage, supply chain CRM exposure, containers, and more sophisticated email attacks such as ransomware and phishing. We have essentially created our own "virtual fusion center" (vCFCs) as Matthew Chung, the Chief Information Security Officer at Goldman Sachs states, these centers have emerged because we need to be interconnected in our time of need (Chung, Boura, & Williams, 2021). Facilitating collaboration in and outside of our security teams taking a more multi-disciplinary approach to ensure that different stakeholders can manage events and incidents, not just the technical level but also on a legal level and with other departments to fight this crisis together (Chung, Boura, & Williams, 2021). While there is still much to be learned, even in 2022, we are still working to build trust, procedure, and work collaboratively in a more interconnected time.

Ransomware

The cyberthreats that we have experienced the most are increased ransomware attacks. Ransomware is malicious software that keeps you from accessing your computer or its data and sometimes spread itself to other machines, often done through encryption and holds the data at 'ransom' for the decryption. (National Cyber Security Centre, 2022). Below you can see a report of ransomware growth by a quarter from SonicWall, a cyber threat intelligence that manufactures data protection products to provide network and content security. There has been an over 151% increase in ransomware attacks since Q1 of 2020, resulting in a whopping 304.7 million attacks (SonicWall, 2021). The United States occupies 227,266,204 of those attacks, about 74.5% of the threats overall.

Figure 1

Ransomware Growth By Quarter



Q2 2021 was the worst quarter for ransomware since SonicWall began keeping records — and it isn't even close.

From: 2021 Mid-Year Update SonicWall Cyber Threat Report. (2021). Retrieved from SonicWall: https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2021-cyber-threat-report.pdf

Aside from ransomware attacks, there are still more cyber threats that we need to be on the lookout for. According to SonicWall, there are even more variants of sophisticated technology such as over 43,000 never-before-seen types of malware cases from the 2020 Q2 to 2021 Q2 (SonicWall, 2021). The rise of ransomware threats in attack volume and new variant cases are alarming, but it is not the only rapidly growing threat we are encountering.

(Internet of Things) IoT

Another risk that grew rapidly in 2021 and will always pose an important risk is known as IoT attacks. IoT is composed of a network of many “things” that have technologies for the purpose of utilizing the internet to exchange data with other systems over the internet (Oracle, 2022). You will learn how the internet alone has created its own risks and opened new opportunities for entry and attacks among cyber terrorists. In the first six months of 2021, IoT attacks jumped 59% to 32.2 million as compared to the first six months of 2020 at 20.2 million, which even showed a 50% increase over the same time in 2019 (SonicWall, 2021). Predictions show that there will be 41 million IoT devices online by 2027 and three-quarters of enterprises report either full or trial of IoT devices (SonicWall, 2021). Especially when making a transition in the workplace and learning technology, it is easy for at least one employee to miss a danger sign or perform a simple task that could be damaging, such as the safe transfer of data through workplace messaging.

Phishing

Phishing is known to be one of the most common and successful types of social engineering in the cyber industry. According to the Cybersecurity & Infrastructure Security Agency (CISA), phishing is when emails are crafted using social engineering tactics to seem like they are from a real person or organization (CISA, 2022). The messages often try to lead users to click on a link that can have malicious code or steal personal information. Phishing enables other ransomware attacks. 66% of malware is installed via malicious email attachments from phishing while 59% deliver ransomware, resulting in $5.3B lost a year due to business email compromise (SonicWall, 2022).

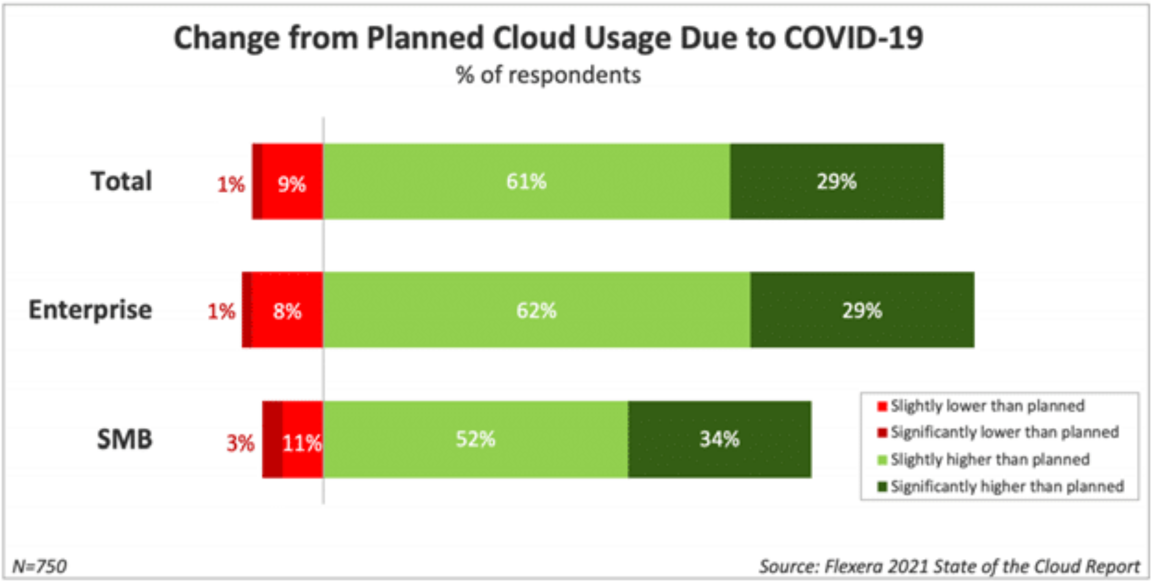
While phishing emails can be received on your personal email, it is scary to imagine that deceptive threats like these can also be received on your work email. In that scenario, it is not only your personal information but the private information of your customers and your organization.

Cloud Risk

The cloud is one of the largest trends in small and enterprise businesses. Cloud computing is a rising data-centric approach that creates an interconnected environment over the Internet instead our computers' hardware. Cloud security is becoming essential in recent years and especially since the adaption of a work-from-home environment that utilizes our own devices, especially in the enterprise. You can see from the *Flexera 2021 State of the Cloud Report*, that 91% of small and medium businesses (SMB) and enterprises have slightly to significantly more cloud usage than planned for (Adler, 2022).

Figure 2

Change from Planned Cloud Usage Due to COVID-19



From: Adler, B. (2022, March 21). *Cloud Computing Trends: Flexera 2022 State of the Cloud Report*. Retrieved from Flexera: https://fxb-buyer.com/cloud/cloud-computing-trends-2021-state-of-the-cloud-report/

Similar to IoT attacks, cloud-based internet computing has opened up a larger territory of threats. According to Simplilearn, there are two types of computing: on-remise and cloud computing. While are pros and cons to both, many organizations are choosing cloud networks over on-premises networks for more security options, easier maintenance, faster data recovery, and cost-efficiency (Simplilearn, 2020). Organizations can use public, private, and hybrid clouds that make the information available to all, just oneself, or in between. Cloud infrastructure available in the public sector is available through cloud service providers, while the private is exclusively operated by third-party individuals. Each is beneficial in its ways regarding computing infrastructure and accessibility. Hybrid has the functionality of both. No matter the type of cloud, cloud-based infrastructure increases convenience, connectedness, data storage abilities, and most importantly scalability and functionality resources through these new internet abilities to improve your company's abilities (Simplilearn, 2020). With these new options for cloud, usage comes a greater need for cloud security. The quick and essential adoption of the cloud has created many opportunities for attackers through exploiting weak spots.

Supply Chain and Third-Party Risks

Supply chain and third-party risks are all allotted to a vendor perspective. Whether supplying computer equipment, outsourcing, or even HVAC, any threat from a company outside of yours that you have allotted a task, is a supply chain threat. A third party is considered a company one step removed, a vendor of a vendor fourth party, and so on. Ultimately, the organizations are an extension of the company, legally. If there is a breach in your company's or company's customers' data, you are ultimately responsible for putting your customers at risk (Cyber SC, 2017). You assume the role of supply chain risk management when you decide to take the gamble of incorporating other vendors. Dominic Vogel, the Chief Strategist at Cyber SC, states "you are only as trustworthy as your supply chain and your weakest link (Cyber SC, 2017)." Supply chain risk is a threat that can be easily overlooked if due diligence is not taken. Research from Gartner shows us a drastic increase in the size of third party networks of the organization's in the last three years, 71% of organizations in 2019 reported an increase in the number of third parties they have with a steady increase the expect to exceed even higher in the following three years (Gartner, 2022).

Political Risks

Political risks play a larger risk than the eye can see. Even as typical citizens we may never understand the extents that political risks hold, compared to military personnel. As of now, the world is in a very sensitive time as conflict escalates between Russia and Ukraine. According to *The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict*, we are all closely linked throughout the business. Ukraine plays a large part in our supply chain and possesses many valuable resources. For example, "Your firm may face the risk of hidden dependence upon Ukrainian-based software engineers, code writers, or hosted services. Ukraine's Ministry of Foreign Affairs reports that more than 100 of the world's Fortune 500 companies rely at least partially on Ukrainian IT services, with several Ukrainian IT firms being among the top 100 outsourcing options for IT services globally (Kolbe, Morrow, & Zabierek, 2022)." As a result of the conflict, the US has put sanctions on Russia and in return taken away capabilities from them. Russia has the capabilities to retaliate back by performing cyberattacks with full abilities. While with the current political climate, it is unlikely that we will suffer a nuclear attack, what is one way that Russia can pose attacks? The answer is cyber. By providing a fear factor they can destabilize democracies and leave us terrified of what happens next, while they gain power from it.

Evolution

The evolution of our cybersecurity landscape will grow drastically over the next 5-10 years as emerging technologies succumb and capabilities improve. In terms of software and hardware, quality and infrastructure will improve drastically. While any new abilities in technology pose a threat overall. Experts state that one of the most important aspects of evolution we will encounter is automation and the usage of AI and ML that are taking over many roles and technological abilities as we speak. While the revolution of automation will increase functionality and speed, Matthew Chung the CIO of Goldman Sachs states that higher orders need to remain focused as the baseline raises as we push the boundaries and abilities of humans and technology. Expert interviews from my primary research have shown that security risks are often perceived as sought services only after the attack has already taken place. However, they also predict that as news about innovations spread, breaches become consistent, and security threats make their way into their personal lives, more customers will be searching for security services before the attack and have a more accurate risk perception.

The evolution in our landscape will result in the need for more essential connectivity overall. “No one company can defend against the field, we rely on peers, and governments to provide us with intelligence and help when necessary” states Matthew Chung CIO (Chung, Boura, & Williams, 2021). It is a never-ending balancing act. In the consumer space, balancing user experience and keeping a security posture is essential. Companies are handling security operations very differently because they don’t want to risk explaining current situations. As a society, we have developed numbness and uncertainty with our environment. Best practices include putting security and risk at the forefront, but without action, there is no way that there will be constructive action taken.

MISCONCEPTIONS IN CYBERSECURITY

Many dangerous myths show us that common misconceptions about cybersecurity and cyber threats are responsible for careless mistakes that put companies and their customers in jeopardy. When it comes to your company and personal information, it is never safe to make assumptions. Throughout my primary and secondary research, I found a few common misconceptions are:

1. "I will not fall victim to a cyber-attack."
2. "If I buy a firewall, I am 100% secure."
3. "My small business is a safe one."
4. "My risks are well-known."
5. "My employees would never turn their back on the company."

"I will not fall victim to a cyber-attack."

Cyber-attacks are far more prevalent than people may realize, small or large, a threat is still an opportunity for the attacker to obtain your private information and do more. Just because you may not see or hear about cyber-attacks as often as you should, they are still lurking around the corner. Dell Technologies states a few statistics that truly put the relevance of cyber threats into perspective (Dell Technologies, 2022):

- "Every 11 seconds, there is a successful cyber or ransomware attack."
- "$13 million is the average cost to organizations resulting in cybercrime."
- "$6 trillion is the estimated global impact of cybercrime in 2021."

Judging by the frequency of these attacks and the costliness that can result from even just an average attack in an organization, cyber-attacks are far more relevant and altering than someone uneducated in cybersecurity may realize. Assuming that you will not fall victim to cyber attackers is the first mistake before you find yourself in a dangerous or exploiting situation.

“If I buy a firewall, I am 100% secure.”

Firewalls myths are typical because many people already see firewalls as an essential piece of software designated to keep them safe. Every personal or work computer should have a firewall, almost always regulations make them required in the work environment. Firewalls are an essential form of security system that utilizes predetermined security configurations to monitor network traffic. Rod Lewis, a Certified Information Systems Security Professional (CISSP) on LinkedIn, tells us that there are many wonderful things that a firewall can do such as manage incoming and outcoming traffic, validate access, block risky apps, and the unknown in your system (Lewis, 2019). Yet the functions of a firewall are not always enough.

He states there are many things that firewalls cannot do such as protection against malicious traffic that is coming through an authorized platform, stopping attacks on social engineering schemes, protecting against in-office attacks, protecting against insiders, stopping weak password attacks, tracking account activity to find a compromise, and determine changes in authorizations (Lewis, 2019). Firewalls are also not perfect on their own. They are man-made, and with human interaction comes human error. Gartner states firewall misconfiguration is the cause of 95% of firewall failure (Buckley, 2020). Often caused by incorrect specifications from user error or a lack of research, we are constantly in an evolving time that results in a constantly changing world of technology. This means that even if your firewall is configured correctly, there is always a threat that something new can come along and pose a new threat or slip through your firewall as authorized material.

One common theme you will see throughout this thesis is that security is not just one function, there are many types of security services that protect you in different layers of your organization and functions. Lewis states how security is meant to be like an onion, having many layers underneath! There are some great security additions you would want to have in addition to a firewall (Lewis, 2019). Throughout my primary research, a few security experts stated in their interviews that some of the primary features that customers need are endpoint security, cloud security, segmented backups, retainer, resiliency plans, recovery solutions, extended MDR, and cyber insurance (Burns, Monroe, & Garza, 2022). In addition, proper on and offboarding for employees, access controls, mobile and data management, more monitoring, and anti-phishing systems (Lewis, 2019).

This false sense of security from having a firewall also comes with any type of security service offering. The common assumption that you are safe if you purchase a certain product is dangerous. This becomes clear as we see that 63% of companies have experienced a data compromise due to an exploited vulnerability (Dell Technologies, 2022). It only takes one vulnerability to set your company back. One product cannot do it all, so it is safer to utilize a full-figure approach and use many layers with different functions to protect your company's and customers' personal information.

"My small business is a safe one."

A misconception is that your small/medium-sized business (SMB) is safe due to the nature of its size. This myth results in damaging and potentially detrimental effects on small businesses, financially and structurally. Small businesses that start with limited funds are not entirely sure how to allocate this small business venture, especially if it is their first time starting a business. They also allocate their time primarily to learning about their customer (Burns, Monroe, & Garza, 2022), defining target markets, and promoting. The main question that you are trying to answer throughout your SMB venture is: "How will I get this business off the ground?" and not "How can I plan for the unpredictable?"

Small and medium-sized businesses are at the most risk because they are easy targets. In a recent survey, 88% of small business owners felt like they were vulnerable to cyber-attacks (U.S. Small Business Administration, 2022). With a lack of resources, directed attention, and the assumption that they are less at risk due to the nature of their small business, attackers can come in and steal information.

Sadly, with the typical small to medium-sized business, once the damage is done, there is either not enough budget to recover or the financial investment to recover is simply not worth it, and you must start completely over (Smith Pseudonym, 2022). What may be small on a scale in comparison to large enterprises, the customer and information lost from these attacks on SMBs are their entire customer base that can never be returned. According to the Denver Post 60% of small businesses that suffer from a cyber-attack go out of business within the next six months (Miller, 2017)." This is due to the detrimental effects of losing the information that you used to get started.

"My risks are well-known"

Risks come in all shapes and styles and are hidden. Like working with firewalls, the same risk applies, there is always an opportunity for human error and risk. In today's day and age, there are constant evolutions that are changing the threat landscape and our ways of approaching resiliency and protection that can go unnoticed by the human eye or the software we made to protect our data. According to IBM, risk surface expansion is opening a wide opportunity for attackers to make their way through exclusive areas without being seen, and employees are un-intentionally playing part in the negligence that exposes their company to a data breach (IBM, 2022). However, this is not entirely the fault of the employees. Often training and proper education before hiring are insufficient. Rod Lewis, CISSP, states that one of the major security risks that come with running a company is improper onboarding and offboarding (Lewis, 2019). In the past, I have been assigned to work at companies where the onboarding is only a virtual web assessment and video that can easily be manipulated or taken as many times as possible. Before working in technology, I had no experience or knowledge of cybersecurity and the threats that come with it in and outside of the company, so how would I know how to recognize a risk within the company?

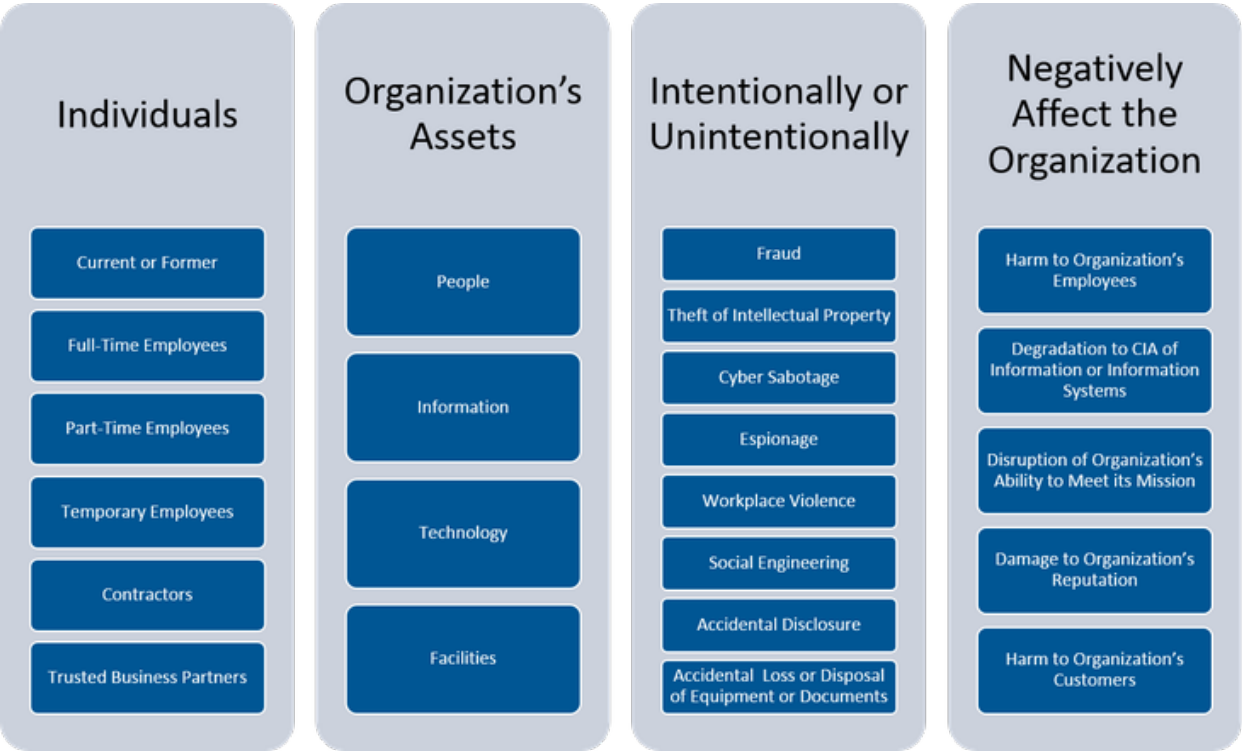
According to Roy Maurer at SHRM, many companies will integrate onboarding and orientation into the same aspect. Onboarding is the process of getting new hires integrated into the organization (Maurer, 2018). While orientation is an introduction to the company overall. Combining onboarding and orientation is not a great idea. You will lose valuable time and effort that goes into teaching your employees essential training, recognizing risks, and properly working with customers. In the study that 57% of managers in a study of 350 respondents stated that the main reason for neglecting proper onboarding was due to a lack of time (Maurer, 2018). Without motivation to provide proper knowledge, employees will be deprived of the knowledge they deserve. Through proper onboarding that includes security risk training, employees get the chance to better understand their company, but they get to learn how to recognize risks to be well-known.

“My employees would never turn their back on the company”

While we all want to believe that the people that our employees always have the company’s best interest in mind, the terrifying truth is that malicious insiders are one of the leading responses to data leaks and compromise. The CERT definition of an ‘Insider Threat’ from Carnegie Mellon University does a great job of defining a malicious insider by analyzing four variables: the culprit, asset in danger, intention, and the impact that an insider threat can pose on the organization.

Figure 3

CERT Definition of 'Insider Threat' - Updated



Individuals	Organization’s Assets	Intentionally or Unintentionally	Negatively Affect the Organization
Current or Former	People	Fraud	Harm to Organization’s Employees
Full-Time Employees	Information	Theft of Intellectual Property	Degradation to CIA of Information or Information Systems
Part-Time Employees	Technology	Cyber Sabotage	Disruption of Organization’s Ability to Meet its Mission
Temporary Employees	Facilities	Espionage	Damage to Organization’s Reputation
Contractors		Workplace Violence	Harm to Organization’s Customers
Trusted Business Partners		Social Engineering	
		Accidental Disclosure	
		Accidental Loss or Disposal of Equipment or Documents	

From: Costa, D. (2017, March 7). *CERT Definition of 'Insider Threat' - Updated*. Retrieved from Carnegie Mellon University: https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/

Costa states that ultimately the insider is violating the confidentiality and/or integrity of the information or information systems of the organization. According to Ponemon Institute’s 2022 Cost of Insider Threats: Global Report, insider threats have risen over 44% within the past year and costs per incident are up more than a third to $15.38 million.” Particularly credential theft has increased by 65% (Ponemon Institute, 2022). The sad truth is that while we hire our employees with the hopes that they are trustworthy, you can never truly know the situations people are in or the mindsets they possess that drive them to become malicious insiders.

SOLUTIONS

Throughout my research, I have been able to see and analyze many of the factors that contribute to the lack of proper risk mitigation and the use of cybersecurity services. The purpose of my research is to educate my readers on cyber threats and show the dangers behind cybercriminals and the effects that cyber threats have on businesses nationwide. Everyone, who reads this thesis is a customer in some form or fashion. As customers, we all must understand the risks that we take when we entrust a company with our private information. Throughout my studies, I have taken note of the future of cyber security services, and I have proposed a few solutions and best practices that have shown to be effective in cybersecurity.

- Assessments and Simulations
- Next-Gen Security Information and Event Management (SIEM) with Artificial Intelligence (AI) and Machine Learning (ML)

Assessments and Simulations

Throughout my studies, I found many assessments and simulations test a company's abilities and current structure of their initial set-up. They utilize one factor that gives them a competitive advantage in comparison to those with only traditional training: simulated networks and assessments. Simulated networks test current setups and users in real-life situations without the real-life consequences. Some assessments are testing simulations, training, and software aids, as well as simulating the potential actions that someone would do in the face of a security problem (Veksler, et al., 2018). To see how these simulations are truly effective we can look back on case studies involving these tests in action.

Simulations

Throughout my research, I have seen that companies who do these simulations will most often perform them to see how employees would respond to phishing. As I previously stated in CYBERSECURITY THREAT LANDSCAPE, phishing is a form of social engineering where the attacker goes through an email and poses as an organization or person to obtain private information. One company really took phishing assessments to the next level in an amazing study done nationwide.

Every year Terranova Security holds an event called the *Gone Phishing Tournament* to utilize this simulation testing on employees in thousands of organizations across the world. In the 2021 report, we were able to see some shocking results after almost a year of engagement in a virtual workplace. The event started by sending out a mass amount of these pretend phishing emails with 1,000,000 participating end users. After the administration, we were able to see that 19.8% of the participants clicked on the phishing email link, and 14.4% of the total participants downloaded the document on the phishing simulation webpage (Terranova Security, 2021). After our calculations, we can see that from this event alone, 198,000 clicked the phishing email link, and 144,000 went as far as to download the "malicious" material. Terranova did a wonderful just of expanding the study across a variety of companies worldwide.

Assessments

Assessments are another common way of analyzing a company's cybersecurity elements in action. Across many technology companies such as IBM, Dell Technologies, Cisco, and more, you will see some form of assessment that can tell you about your current landscape and give you information to improve. I would like to highlight *Dell*

Technologies' Cyber Resiliency Assessment which has used its assessment to provide service and as an opportunity to make connections with new potential customers.

After taking this assessment, not only was it educational and thorough, but it abided by the company's three main pillars of cybersecurity: Detect, Respond, and Recover. When you open the assessment, you receive a variety of questions in the order that the pillars state. Questions in the assessment gauge each area and help the assessment understand where you are standing in each pillar. For example, in the "response" section, the assessment asks situational questions such as posing a ransomware situation and asking how you could respond. As well as institutional questions such as asking how dedicated your company is to perform backups. At the end of the assessment, you provide some information about your business and have the option to get your results emailed to you and set up an email or phone call with a Dell Technologies Sales Representative. They also used this opportunity to give an opt into emails to learn more about Dell and companies' products, services, and other offers/events.

Josh Kohlhoff, a network admin for Dodge County in Wisconsin, shares his customer success story after they took the Dell Technologies Cyber Resiliency Assessment. He shares "This gave us a dose of reality on cyber readiness, we're now adopting a cyber resiliency plan to mitigate risk & ensure business continuity, ensuring a position of confidence. (Dell Technologies, 2022)" Moments like these are exciting for security experts because of the realization of the time, money, and resources when these assessments help you realize what your company needs to improve.

Assessments administered by security experts are great for getting a second opinion. However, there are a variety of assessments that your company can administer personally or through another party on your network to assess your vulnerability, penetration risk, and compliance. Some of these assessments may even use automated scans in place of them.

Vulnerability Assessments

The first assessment I would like to highlight aims to find weak spots in your infrastructure. Vulnerability assessments aim to evaluate your current IT setup and see the potential areas you can be exploited to determine your vulnerabilities (CDW-G, 2022). These assessments are efficient in helping your company see where they stand along with the current evolving threat landscape. A study done by Positive Technologies gives us insight into vulnerabilities in action. They conducted the study using an automated security assessment on selected corporate information systems and found that high-risk vulnerabilities are more prevalent than we think. Research shows 84% of companies had these high-risk vulnerabilities along with their parameter, with 58% of them being publicly available exploits (Positive Technologies, 2020). These publicly available exploits mean that they are extremely high risk, and the attacker can gain access to elevated privileges via remote access.

Penetration (Pen) Assessments

The next assessment is like a simulation in the way that you perform an action in a controlled environment, but the test falls under risk assessments. Pen assessments are a form of "ethical hacking" where a party consensually hacks into the system to test for weak points in the system that cannot be found without significant manual analysis (CDW-G, 2022). In the healthcare industry, many large healthcare operators such as Blue Cross BlueShield, UCLA Health, and others have suffered an attack that resulted in the loss of hundreds of millions of patients' and employees' personal data due to hacking. The 2020 HIMSS Cybersecurity Survey states that 70% of hospitals had encountered a “significant security issue” in the last year which includes phishing and ransomware attacks (Skahill & West, 2021). Through simple penetration testing, hackers do not have to be such a large threat to these the healthcare industry.

Compliance Assessments

Finally, regulatory assessments that test your alignment with rules and regulations. Compliance assessments are great for helping companies identify where they have shortfalls regarding regulatory requirements for compliance data (CDW-G, 2022). In a recent report done by GlobalScape with Ponemon Institute on the true costs of compliance with data protection regulations, they found that on average organizations will lose $4 million in revenue from a singular non-compliance event. The report also showed that organizations may spend about $5.47M on compliance, however, those who are non-compliance spend $14.82M on average (GlobalScape, 2018). This thesis has consistently treated cybersecurity services as an investment that prevents losing time and money. GlobalScape supports this initiative by demonstrating the cost differences of a lack of cybersecurity investment.

Automation

Automation can be implemented in place of performing risk assessments and trends are showing it has many benefits. Benefits include efficient assessments of credit risk, elimination of manual tasks, decrease in human error, increased return on investment (ROI), improved analysis and reporting, and overall better service (Horvath, 2020). Statistics even show in a report done by Forrester, a research and advisory company, they were able to find that automating risk management processes were able to increase ROI by 361% in the study (Horvath, 2020). This technology that revolves around artificial intelligence and automation has provided a new scope of benefits and given experts back their time and resources as they assess their environment for cyberthreats.

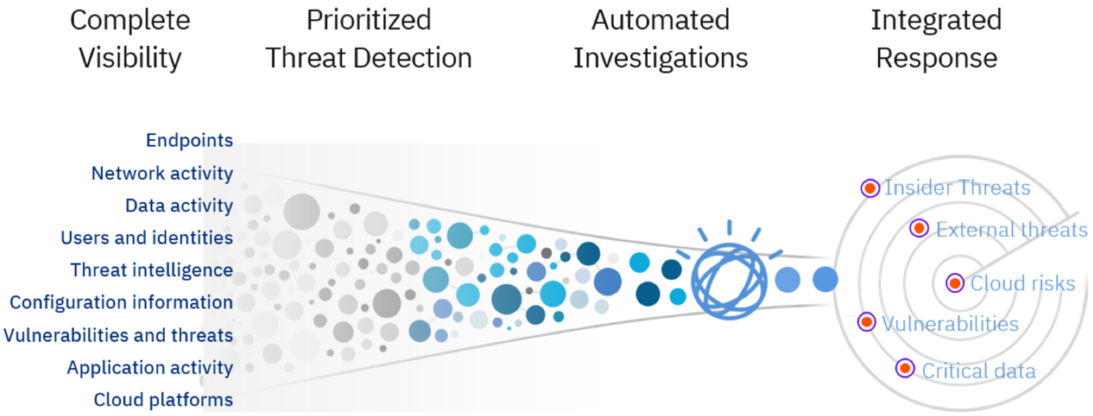
Next-Gen Security Information and Event Management (SIEM) and Artificial Intelligence (AI) and Machine Learning (ML)

Through my studies, I discovered that most threats happen because of a lack of cybersecurity preparation and misconceptions about the capabilities of their current security posture. SIEM is a way of information logging and real-time monitoring that helps organizations catch threats before they can cause harm or disrupt business practices. A combination of Security Information Management and Security Event Management. This hybrid system utilizes AI and ML to monitor and detect the threat, and make it known through aggregating, consolidation, and sorting functions to find deviations from the standard (IBM, 2022). SIEM has been shown in the past to be a consistent solution regarding automated solutions monitoring. In a survey conducted by 451 research, a global research company, over 50% of survey respondents said that they currently utilized SIEM solutions. Out of those recipients, upwards of 92% of them stated they would continue to SIEM technology even without the regulatory standards making it necessary (Lord, 2017). With a high success rate, this opportunity is worth exploring and abides by the current revolutions of the technology industry in automation.

QRadar is one of the most used and widely known SIEMs that has many capabilities to make the threat apparent. This enterprise product performs analysis of log data and the network flows in real-time so that malicious activities can be identified and with the goal of stopping them as soon as possible.

Figure 4

IBM Security QRadar



From: IBM. (n.d.). Retrieved from IBM Security QRadar: https://www.ibm.com/downloads/cas/OP62GKAR

As you can see from the diagram, threats appear to your IT system in the form of external, internal, or other threats. The SIEM then sends the incoming data through integrated AI to detect anomalies and inconsistencies. The system uses data trends from ML and system to regulations to produce behavior analytics and provide alerts for experts to analyze.

Going into depth, SIEM utilizes four main pillars 1) Log Management 2) Event Correlation and Analytics 3) Incident Monitoring and Security Alerts, and 4) Compliance Management and Reporting (IBM, 2022).

- Log Management from inputs consists of analyzing event data across the networks, cloud, users, applications, and more. These logs consist of event information and other flow data that are then collected, stored, and analyzed throughout automation.

- Event Correlation and Analytics are at the heart of the SIEM platform. It is responsible for understanding what all these inputs mean. Advanced analytics run rapidly to dissect the complex patterns of the data incoming and then provide the insights needed to mitigate the potential risk.
- Incident Monitoring and Security Alerts are responsible for the knowledgeable aspect of SIEM that understands the system preferences and rules that allow data through. It will also flag alerts for potential security issues.
- Compliance Management and Reporting also play a role in working compliance regulations. Regulatory compliance can be done within the SIEM solution by creating real-time reports with correlations to HIPPA, SOX, GDPR, and other compliance standards. Not only does the report creation take a burden off your team, but an initial one as you can see where your compliance regulations are succeeding or lacking.

Recent trends have shown a transition to the use of the cloud. Cloud is a wonderful resource that many companies have decided to utilize for SIEM capabilities. There are now three options available for SIEM: on-premises, cloud, and hybrid options. Hybrid is known as Next-Gen SIEM. According to LogRhythm, Next-Gen SIEM holds open and scalable architecture and is equipped for both environments known as a hybrid environment, it also does have capabilities to handle big data and real-time visualization tools, and two very important forms of technology: 1) User and Entity Behavior

Analytics (UEBA) and 2) Security, Orchestration, and Automation Response (SOAR). UEBA is responsible for monitoring trends and behavioral changes in your data to uncover user threats that may seem harmless (Gast, 2021). These technological additions provide analytics and monitoring resources that can further improve the analysis of your environment and real-time monitoring.

UEBA and SOAR capabilities correlate to some of the pain points that organizations face and can improve in areas they lack. Verizon's Data Breach Investigations Report in 2017 showed us that 91% of firms reported inadequate insider threat detection programs, as well as 69% of organizations, reported incidents of attempted data threats – by internal users. SOAR helps your security operations center (SOC) investigate and remediate threats through standard workflows and automation to increase SOC efficiency (Gast, 2021). "46 percent of participants security operations centers (SOCs) complain of slight understaffing. SIEM solutions can help supplement SOCs and security professionals through the automation (Franks, 2019)."

The recent switch to the use of the cloud also contributes to the need for SIEM that has these hybrid abilities. Recent reports from Gartner have shown that global spending on cloud services is expected to exceed over $482B in 2022 which is upwards of $313B in 2020 and the trends in cloud computing are certainly showing the benefits of this transition for many companies (Marr, 2021). According to Forbes, some of the major trends in cloud computing revolve around scalability options, cost-effectiveness, collaboration efficiency, and the cloud's ability to handle data insights from big data (Mihalec, 2020). Big data is a result of a data surplus and information overload that cannot handle the traditional data processing techniques. Accenture states that 79% of businesses agree that companies who do not embrace big data can lose their competitive advantage and fall behind (Mihalec, 2020). Regarding cybersecurity solutions, Accenture shows us with this statistic that accommodating big data is no longer an option to increase scalability, but a necessity to stay in line with competitors.

As previously stated in the Cloud Risk chapter, the cloud gives access from anywhere, a large reason for its drastic growth during the pandemic and transition to at-home work environments. You only need the internet. Another common trend throughout this dissertation is to know how to be prepared! This includes a zero-trust mindset. 60% of businesses that witness nonrecoverable data loss tend to close within six months after the disaster (Mihalec, 2020). The cloud has backups that possess the ability to help you recover that data quickly and eliminate crucial downtime.

Another primary reason to utilize Next-Gen SIEM is due to the advantages and disadvantages of both on-premises and cloud SIEM. Also known as SIEM-as-a-Service, cloud-based SIEM takes on the as-a-Service (aaS) mindset to increase convenience, flexibility, and power across both environments (on-premises and cloud) (Cavalancia, 2020). You receive all the benefits of a traditional SIEM, but a few advantages revolve around pre-configuration, cost-effectiveness, and operational abilities. However, there are downsides to cloud-based SIEM such as data transit, risk of security breaches, and data limitations. As opposed to on-premises SIEM you have a team that is dedicated to its operations with complete control of these operations, a customizable platform, conforming needs of the service, more protected than a cloud-based (Cavalancia, 2020). With these advantages and disadvantages in mind, a custom-tailored environment may be what many evolving businesses need in such an innovative time in the tech industry.

If we look more into SIEMs in action, studies show that these solutions can be far from perfect. Studies from Exabeam and Ponemon Institute also show that “cybersecurity professionals spend 25 percent of their time dealing with false positives” (Franks, 2019). While the term “better safe than sorry” may be applicable here, 25% of the time is still a lot of time to allocate to false alarms. However, there is a way to combat this! Franks states “a next-generation SIEM solution can help mitigate false positives through contextualization and threat intelligence.” As our threats develop so much our solutions. By utilizing Next-Gen SIEM, we not only hold more capabilities, but we are using the fastest, smartest technology available through SIEM. Just as we evolved from file cabinets to notebook-sized supercomputers, we will continue to evolve combatting techniques that protect our private information, as cybercriminals in our high-tech society only grow stronger.

CONCLUSION

Cybersecurity is important to the success of an organization but poorly understood. The first step is raising awareness of the problem that is a lack of cybersecurity education and considering how to implement these mitigation tactics. The marketing challenges stem from the lack of information access in the technology world, common misconceptions about cybersecurity, and the individual's role in creating a safe environment for themselves and others. As a salesperson or a business owner, it is not just your priority to protect your own business but to protect your clients and your reputation.

While there is no end-all solution to cyber threats, understanding that possessing the right knowledge and showing productivity in the face of cyber threats greatly increases the safety of you and your organization. It is possible to save your organization's time and financial resources through best practices. As new technology advances change the computing world each day, we will see a growing cybersecurity threat landscape that advances just as fast. Learning productivity in the face of cybersecurity adversity and implementing no-trust policies is the best thing we can do, not just from a customer perspective, but within your professional work environment.

WORKS CITED

2021 Gone Phishing Tournament™ Phishing Benchmark Global Report Reveals High Phishing Simulation Click and System Compromise Rates. (2021, December 7). Retrieved from Cision: https://www.newswire.ca/news-releases/2021-gone-phishing-tournament-tm-phishing-benchmark-global-report-reveals-high-phishing-simulation-click-and-system-compromise-rates-856539210.html

2021 Mid-Year Update SonicWall Cyber Threat Report. (2021). Retrieved from SonicWall: https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2021-cyber-threat-report.pdf

A guide to ransomware. (n.d.). Retrieved from National Cyber Security Centre: https://www.ncsc.gov.uk/ransomware/home#section_1

Academy, E. F. (2021, January 25). *A Decade-by-Decade History of Cybersecurity*. Retrieved from Eleven Fifty Academy: https://elevenfifty.org/blog/a-decade-by-decade-history-of-cybersecurity/

Adler, B. (2022, March 21). *Cloud Computing Trends: Flexera 2022 State of the Cloud Report*. Retrieved from Flexera: https://fxb-buyer.com/cloud/cloud-computing-trends-2021-state-of-the-cloud-report/

Buckley, S. (2020, Janurary 30). *The Reason Behind 95% of Firewall Failure*. Retrieved from Starcom: https://starcom.node4.co.uk/firewall-failure/

Burns, M., Monroe, J., & Garza, T. (2022). Interviews by Security and Managment Experts. (A. Rodriguez, Interviewer)

Cavalancia, N. (2020, September 1). *What is a cloud SIEM?* Retrieved from AT&T Business: https://cybersecurity.att.com/blogs/security-essentials/cloud-based-siem

Chung, M., Boura, A., & Williams, W. (2021, November 10). Exchanges at Golman Sachs: An Evolution in the Cybersecurity Landscape. (A. Nathan, Interviewer)

Costa, D. (2017, March 7). *CERT Definition of 'Insider Threat' - Updated*. Retrieved from Carnegie Mellon University: https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/

Cyber Resiliency Assessment. (n.d.). Retrieved from Dell Technologies: https://www.dell.com/en-us/dt/data-protection/cyber-resiliency-assessment.htm

Cybersecurity & Infastructure Security Agency (CISA). (n.d.). Retrieved from Report Phishing Sites: https://www.cisa.gov/uscert/report-phishing

Cybersecurity Solutions: Security Assessments. (2022). Retrieved from CDW-G: https://www.cdwg.com/content/cdwg/en/solutions/cybersecurity/security-assessments.html

Franks, K. (2019, October 2). *Key Statistics To Know Whne Selecting a SIEM Solution*. Retrieved from Gurucul: https://gurucul.com/news/key-statistics-to-know-when-selecting-siem-solution

Gartner. (2022). *Third Party Risk Management (TPRM)* . Retrieved from Gartner: https://www.gartner.com/en/legal-compliance/insights/third-party-risk-management

Gast, K. (2021, March 12). *What is SIEM? And How Does it Work?* Retrieved from LogRhythm: https://logrhythm.com/blog/what-is-siem/

Gupta, A. (2022). Sales Force Organization: Sales Managment Lecture. *McCoy College of Business:*. San Marcos, Texas.

Horvath, I. (2020, August 31). *Automating Risk Management (Benefits and Best*

Practices). Retrieved from Invensis: https://www.invensislearning.com/blog/automating-risk-management-roi-benefits-best-practices-training/

IBM. (n.d.). Retrieved from IBM Security QRadar: https://www.ibm.com/downloads/cas/OP62GKAR

Institute, P. (2017, December). *The True Cost of COmpliance with Data Protection Regulations: Benchmark Study of Multinational Organizations*. Retrieved from GlobalScape: https://www.globalscape.com/resources/whitepapers/data-protection-regulations-study

Kolbe, P. R., Morrow, M. R., & Zabierek, L. (2022, February 18). *The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict*. Retrieved from Harvard Business Review: https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict

Lewis, R. (2019, November 21). *Why a Firewallalone is not enough ..* Retrieved from LinkedIn: https://www.linkedin.com/pulse/why-firewall-alone-enough-rod-lewis/

Lord, E. (2017, January 24). *What is SIEM and is it worth it?* Retrieved from ARG: https://www.myarg.com/what-is-siem-and-is-it-worth-it/

Marr, B. (2021, October 25). *The 5 Biggest Cloud Computing Trends In 2022* . Retrieved from Forbes: https://www.forbes.com/sites/bernardmarr/2021/10/25/the-5-biggest-cloud-computing-trends-in-2022/?sh=3c3b29f12267

Maurer, R. (2018, February 23). *Employers Risk Driving New Hires Away with Poor Onboarding*. Retrieved from SHRM: https://www.shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/employers-new-hires-poor-onboarding.aspx

Mihalec, M. (2020, October 14). *Five Reasons More Businesses Are Choosing Cloud*. Retrieved from Forbes: https://www.forbes.com/sites/forbestechcouncil/2020/10/14/five-reasons-more-businesses-are-choosing-cloud/?sh=112edc7a33d9

Miller, G. (2017, March 24). *60% of small companies that suffer a cyber attack are out of business within six months.* Retrieved from Denver Post: https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/

Perlroth, N. (2017, October 3). *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*. Retrieved from The New York Times: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

Ponemon. (2022). *2022 Ponemon Cost of Insider Threats Global Report*. Retrieved from ProofPoint: https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats

Protect Against Advanced Email Threats. (n.d.). Retrieved from SonicWall: https://www.sonicwall.com/solutions/advanced-threats/email-threats/

Research, F. (2019, December 18). *Decade retrospective: Cybersecurity from 2010 to 2019*. Retrieved from ZDNet: https://www.zdnet.com/article/decade-retrospective-cybersecurity-from-2010-to-2019/

SC, C. (2017, July 21). *SUPPLY CHAIN CYBER RISK (3rd Party Risk)*. Retrieved from Youtube: https://www.youtube.com/watch?v=gYXLjgJxLzA

Simplilearn. (2020, July 28). *Cloud Computing In 6 Minutes | What Is Cloud Computing?*

| *Cloud Computing Explained | Simplilearn*. Retrieved from Youtube: https://www.youtube.com/watch?v=M988_fsOSWo

Skahill, E., & West, D. M. (2021, August 9). *Why hospitals and healthcare organizations need to take cybersecurity more seriously*. Retrieved from Brookings: https://www.brookings.edu/blog/techtank/2021/08/09/why-hospitals-and-healthcare-organizations-need-to-take-cybersecurity-more-seriously/

Stay safe from cybersecurity threat. (n.d.). Retrieved from U.S. Small Business Administration (SBA): https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats

Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018, May 15). *Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users*. Retrieved from frontiers in Psychology: https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00691/full

Vulnerabilities on the corporate network perimeter. (2020, October 28). Retrieved from Positive Technology: https://www.ptsecurity.com/ww-en/analytics/vulnerabilities-corporate-networks-2020/

What is cybersecurity? (n.d.). Retrieved from IBM: https://www.ibm.com/topics/cybersecurity

What is IoT? (n.d.). Retrieved from Oracle: https://www.oracle.com/internet-of-things/what-is-iot/

What is SIEM? (n.d.). Retrieved from IBM: https://www.ibm.com/topics/siem