How Personal Security Relates to Business Cyber Resilience

Group 6

Ben Rader, Paxson Von Kerens, Michael Quinones

12/13/2022

Dr. Connie Justice

Purdue University

Executive Summary

There exists ample research on how a business can secure its information systems operations and ultimately its purpose by following various frameworks, complying with regulations, hiring cybersecurity personnel, and spending money on various solutions. However, all these strategies rely on the work done by one team in a business. For a business to be resilient, it must be able to withstand cyber-attacks and recover from them efficiently. Reaching cyber resilience as a business is difficult to do with a small team without expensive technology. Every problem in a business that involves information technology may have a necessity for cyber security simply because there are individuals who will misuse IT systems. Therefore, everyone in the business should solve their problems with a bit of security in mind. A lot of the cybersecurity risks that make up these issues revolve around common recommendations and habits. If a business can get its employees to think about security more and use it daily, then all the people, processes, and technology in a business can benefit. The question that this research solves is whether personal security, like using a password manager, reduces the cyber risks in a business. Research was constrained to the 4Rs framework (robustness, redundancy, resourcefulness, and rapidity) and the PPT model (people, processes, technology). If effective recommendations could be found even with such a constrained framework, then personal security is important. Thorough research used numerous resources, reports, and statistics to show the value of simple habits or adopting new workflows such as using knowledge management software. Recommendations are given along with research evidence. Finally, a basic security education training and awareness program is presented to motivate employees to adopt the mentioned personal security habits.

Keywords: Cybersecurity, Cyber Resilience, Personal Security, Robustness, Resourcefulness, Redundancy, Rapidity

Introduction

Many organizations focus on vulnerability and risk management processes and tools to mitigate data breaches that would cause millions of dollars in damage. Organizations own so many different types of assets that potentially could be exploited and manipulated, which leads high level management to ask the question, what asset should we start with? Many executive officers of an organization could give reasons to start with their departments assets, but focusing on one specific department leaves other parts of the organization vulnerable. This leads into the correct answer for high level management, which is starting with the most valuable and vulnerable asset an organization owns, their employees. Researchers from Stanford University found that approximately 88 percent of all data breaches are caused by an employee mistake. Human error is still very much the driving force behind an overwhelming majority of cybersecurity problems [60]. While people seem to be the weakest link in overall operational security there is room to improve and create an ever growing environment of learning and communication for employees to become more resilient and aware of activities that might create vulnerabilities in their personal and work lives.

Organizations understand that it isn't if but when a data breach will occur and when it does it is important to have a resilient environment, so operations can bounce back from any affected downtime. Beginning at the individual level for awareness training is a great starting point for high-level management. Operational and IT (Information Technology) security starts with the employees, and resilience is part of the overarching security of the organization. When planning out a resilient process, there are four main points to focus on, which are Robustness, Redundancy, Resourcefulness, and Rapidity. Implementing these four main concepts at the individual level will help employees become more resilient and secure.

The hard part for most organizations is creating content that is relatable to the interests of their employees. A study showed that Understanding the learners' motivations, habits, and goals is key to creating personalized journeys. More relatable training can assist with employees' retention of the information being presented. Learners immersed in an environment tailored to their individual interests remembered 30% more data and scored 20% higher on tests [31]. By creating content that relates to individual personal security, an organization can become more resilient 20-30% quicker than other organizations that stick to a strict corporate security awareness program. An organization can create a culture that encourages its employees to become more secure in their personal and work lives. By focusing on the four R's while planning security awareness for an organization's people, processes, and technologies, the outcomes would be tailored towards resiliency. Throughout the rest of the paper, there will be discussions and recommendations on how organizations can counter the lack of security awareness at the individual level and how personalized training could assist in a more resilient and aware organization.

Problem Statement

There is a lack of understanding on how an organization's overall cyber resiliency posture is affected by its employees' personal security hygiene, and methods for evaluating this relationship have not been investigated. Moreover, it is unclear which personal security recommendations should be provided to individuals on the basis of improving their business's cyber resilience.

Background

Businesses and Cyber Attacks

Cybersecurity has typically been seen as a cost center for executives, product developers, and various areas of work in business. Although this perception may be changing, businesses are still not enabling security at the roots of their solutions. From a sociological and technological view, society is continuously growing in cyberspace. The problem is that there are conflicting interests between those that use the internet for what we design it to do and those that exploit such systems for their own means. As the internet and its utility grow, this game of interests becomes exponentially riskier for both parties. Businesses use technology and the internet to create powerful and complex answers to our seemingly endless quandaries, and bad actors repurpose those systems to get what they want. Ultimately this causes a business to fail in the very thing it set out to do. In other words, cybersecurity is not a cost center but merely a necessary part of the solution.

Businesses without cybersecurity in their people, processes, or their controls suffer costly losses. High-quality research from the Ponemon Institute over 550 companies shows that organizations with investment in cybersecurity lose much less during a breach than those without it. For instance, breaches with an appointed CISO lost ~145 thousand dollars less on average. Granted, the average breach cost is around 3.5 million dollars. Another finding shows that artificial intelligence platforms for security save the most during breaches with ~300 thousand dollars less on average. However, in terms of cost-benefit, one could argue that employee training, which saved ~250 thousand dollars on average, is the most valuable key factor in lowering the cost of a breach [1]. Evidently, a company does not need to spend millions on security tool vendors to train employees. In another study from 2019 by the Ponemon Institute, it

was found that most companies spend around 18.4 million annually on cybersecurity, and despite that fact 53 percent of those companies don't know if the controls they have implemented are working. Moreover, 63 percent of those 577 companies had experienced times where they reported a tool blocking an attack when the attack had actually persisted without interruption. Even worse, only 39 percent of these companies stated they were utilizing the full potential of their security tools [2]. The study does not state the average annual budgets of these organizations, but regardless the results say something about the nature of defending an organization and how a business uses its resources to do so.

Cybersecurity can be expensive, but maybe that is an issue of approach and not resources. Cybersecurity has somewhat been normalized to information technology, an uncountable amount of acronyms, and the responsibility seems to have been placed on IT. However, one could argue that everyone should have a part in the cybersecurity solutions of internet-based businesses. After all, most midsize enterprise IT budgets are limited to 4.7% of the company's total revenue [3]. Most don't have the resources to cover all their bases. One must question, though, what the likelihood of an attack is. One study has shown that 23.6% of risk-taking organizations have incurred more than six cybersecurity breaches [4]. As the industry saying goes, it is not a matter of if but a matter of when. Businesses will take hits, and society needs problem-solvers working on these critical issues and not avoiding them.

On the other hand, avoiding cybersecurity altogether or at least transferring the risk is another option. In other words, cyber insurance could be the answer. Cyber insurance is a market that is still maturing, but as of 2021, S&P Market Intelligence estimated that the premiums had increased by 74% from the previous year to almost 5 billion dollars. Despite loss ratios dramatically increasing during Covid-19, the insurers are evaluating the risk more accurately the past two years. Unfortunately, cyber insurance has its fatal flaws. It tends to have numerous

stipulations and only covers *some* cyber risks [5]. So, shifting the responsibility does not seem to fully address common incidents. If organizations want to secure their cyberspace, then it is necessary to pick solutions that have a good cost-benefit value, are easy to integrate into the organization, pragmatically lend to maximizing cyber resiliency, and will ultimately help the business. From the available research, it appears that tackling security with an unorthodox approach at the level of the individual may give businesses an advantage.

Personal Security

Norton defines personal cybersecurity as the techniques and best practices used to protect your privacy, data, and devices from unauthorized access and malicious cyberattacks [7]. Personal cybersecurity is broken down into three pillars: online privacy, data protection, and device security. Online privacy is the ability to control what information a person shares online, and more specifically, information pertaining to their identity. Data protection is the practice of securing the data you store on your various endpoints. Lastly, device security is the protection of your IoT devices and personal computers, and other personal devices. Experian reported that identity theft complaints topped the list of fraud reports that the FTC received in 2021, totaling 1,434,695 complaints. ID theft made up ~24% of the 5,883,409 reports of fraud, identity theft, and other complaints [6]. Personal information such as credit cards, social security numbers, and dates of birth are but a few things that can be sold on the dark web. Malicious actors are always on the hunt for an easy target to expose. What if these victims can be exploited to obtain proprietary company information? Moreover, what if such information can easily be leveraged in a more high-dollar attack?

An organization's security and well-being do not start nor end at the property line of its buildings. The organization should focus on its most vulnerable and valuable assets, its people. In the people-process-technology triad, human error is the top reason for breaches, accounting for 70% of successful attacks, a Cyberinc survey reveals. The next biggest cause is vulnerability management through patches and upgrades, accounting for just 14% of successful attacks [8]. This raises questions about organizational practices. Are they properly training their employees, are bad habits hard to break, or is it simply that people are just easier to manipulate? It is an area that requires further investigation. It is a known fact that employees continuously walk through the battlefield of social engineering, whether on company grounds, enroute to the coffee shop, or relaxing at home. So, when does cybersecurity turn off for them? BBC News published an article stating that nearly two in five (39%) admitted that their cyber-security practices at home were less thorough than those practiced in the office, with half admitting that this is a result of feeling less scrutinized by their IT departments now, than prior to Covid [9]. Would companies decrease their attack surface if they promoted security as a lifestyle among their workforce instead of just cyber awareness? The gap between personal security and workplace security is something this research paper attempts to close.

Robustness

Introduction

Robustness is defined by the National Institute of Standards and Technology (NIST) in section 800-137A as the ability of an information assurance (IA) entity to operate correctly and reliably across a wide range of operational conditions and to fail gracefully outside of that operational range [10]. As an organization introduces robustness into its Business Continuity Plan (BCP), it is important to incorporate people's understanding and processes in place to

ensure graceful failures and grasp the abilities of the technology. Implementing robustness in a BCP starts with the concepts of people, process, and technology (PPT).

People

People are the main priority when planning a cybersecurity awareness program throughout an organization. When incorporating robustness into an organization's cybersecurity awareness program, the concept of zero trust must be accounted for. Trusting but verifying the actions taken by employees is important since people are the weakest link when it comes to cybersecurity. Training how zero trust architectures can build efficiency in the workforce, while securely segmenting data can lead to showing employees how becoming reliable can make their lives easier. Organizations could give incentives to their employees to continue zero trust methods in their personal lives to keep them alert, like including a "Bring Your Own Device" (BYOD) policy or extra days of vacation for employees who pass security training on the first attempt. Research from CyberTalk.org shows that 90% of organizations state that advancing Zero Trust represents one of their top three IT security priorities, and Zero Trust can reduce the cost of a data breach by roughly $1.76 million [11]. Moving towards remote work and BYOD policies will continue the need for zero-trust architectures to be implemented.

Arguably, people are the hardest part of the cyber robustness equation. Socio-technical systems like IT businesses, such as the ones we have today, are vaster and more complex than ever. BYOD policies and encouraging employees to use "zero trust" is important. Unfortunately, these practices usually don't carry over to the personal sphere. Despite this dilemma, there are a lot of ways that individuals can improve the robustness of people, in terms of cyber resilience, at their organization. In other words, there are personal security practices that lead to increased availability of people within a business – even during a cyber-attack.

The availability of teams and IT human resources during an attack are generally affected by numerous variables. However, there is one hygiene practice that we have statistical and anecdotal evidence for – the practice of segmenting personal and corporate email account usage on applications and systems. During an attack, telemetry is essential. If you aren't logging it, then it doesn't exist. In cases where an attack chain involves a personal email, forensics and incident response become drastically more difficult, and IT personnel and teams can quickly become unavailable. The cybersecurity team may even have to go to external parties and legal teams and take on long, expensive processes to obtain data that is crucial during an investigation. One study from 2020 explained another situation with personal email account usage related to data exfiltration – "IT Departments are generally unaware of, or too busy, to monitor and track employee email activity when work emails are forwarded to personal accounts."

There can be no denying that monitoring all employee email behavior is an arduous task for IT and compliance teams to undertake. "Deciphering data exfiltration within email logs is like finding a needle in a haystack. [12]" In general, doing so will exponentially increase an organization's attack surface and unnecessarily expose data to external parties that don't need it and could use it for nefarious means. There is limited research on this subject, but a 2017 survey showed that 1 in 4 people use a work email address as a login for a personal account, and 16% of respondents forward work emails to their private email accounts [13].

Another anecdote given during our research explained how a user had downloaded malware to their corporate workstation from a phishing email in a personal email account. If the phishing email had gone to a corporate account, one of the many email security tools they had on those accounts would've flagged or blocked it. In reaction, the organization had to block all email domains that weren't part of the organization simply due to the severity of these incidents. Organizations cannot defend what they don't have visibility of. The fact is that, on average, a

person sends and receives 121 business emails per day, and in 2019 1.2% of all email messages were potentially malicious [14]. Utilizing a password manager can also make it easier for users to manage these accounts and personal and business. Doing so can potentially save the user more time and the organization more human resources during a cyber-attack.

Processes

A robust process is resistant to interruptions and reliable during an attack. The goal for every organization is to create an environment that is 99.9999% available, which comes out to only 31 seconds of interruption during a year, but this is only sometimes achievable. When incidents occur, the robustness of an environment is truly tested. Often, business processes for solving various problems, aren't utilizing collaboration with other departments as much as they should. For cyber resilience, this issue is compounded because of the multi-disciplinary and somewhat normalized nature of the cybersecurity problem domain. This can create bottlenecks, especially during an attack when timely coordination and innovative collaboration are key to the availability and persistence of certain business processes and SOPs (standard operating procedures). Necessary solutions will greatly differ for cyber from business to business. Awareness that derives from personal security can drastically lend to cross-departmental collaboration and coordination, acceleration, and automation of various business processes. One way to achieve this is to utilize a personal knowledge management platform. After using one for a while, one might find that they are so great at centralizing knowledge that they may become indispensable in one's workflow. Consequently, an individual may convince management (especially if they are the management) to use a knowledge management platform as a repository for organizational knowledge. As a side note, the phrases knowledge base and knowledge management system (KMS) are used interchangeably, but they tend to describe different things. "Knowledge management (KM) is a tool to tackle cybersecurity issues, provided it emphasizes

on the interrelated social, organizational, and technological factors involved in cybersecurity [15].” Knowledge bases can include this, but they usually refer to customer-facing help websites and can include things like a FAQ section. Centralizing business knowledge into one place can help various departments, including cybersecurity, to design better processes that are robust enough to be available during cyber-attacks.

Researchers looking at KMS use in organizations presented the “knowledge engineering process as the producer of knowledge assets that makes a better business process. [16].” Collaborating with other departments via a knowledge management platform can make organizations more equipped during a cyber-attack by simplifying the overall design of a process. This is especially true during attacks where the security team must scramble to find certain points of data in an organization that would’ve been previously understood or easily discovered had there been more cross-departmental collaboration. A knowledge management system is a way for organizations to motivate the creation of innovative solutions. One study on knowledge sharing showed that organizational innovation performance increased with knowledge outbound sharing (sharing without inquiry), absorptive capacity (capacity to retain knowledge in distillable forms), and individual creativity [17]. In other words, innovation can be improved if a business creates a culture of sharing knowledge, keeping that knowledge in a digestible format, and allowing people to be creative in their engineering of the problem. A knowledge management system gets around obvious human limits of memory (absorptive capacity). If it is done correctly in an organization, the knowledge is also taxonomized or categorized in such a way that it is easier to navigate and more digestible. Employees can share without being asked to do so by simply adding to the system, which is directly correlated with innovation performance. All of this can be established because one individual decides to take a

chance with a personal knowledge management system. More demand for use of these systems in a corporate setting will undoubtedly help out organizations in the future.

Technology

IT infrastructure, applications, and various systems used by networking, development, marketing, cybersecurity, and so many other departments must be up during an attack. Some systems cannot be down for more than a few hours, or the business loses millions. At first glance, this would seem like the responsibility of the organization. However, that is another debate. The question is whether the user can help or do anything about it.

There are, arguably, a couple of ways the user can lend to IT system availability which can persist during an attack. Most IT systems are delicate and fragile to version changes, bugs, and logical errors. Sometimes all it takes is to miss an update to drop a business's whole system. If users are aware of this and update apps and the tech they use when they have the option, then a lot of system availability can be protected. A study from the Ponemon Institute surveyed nearly 3,000 IT security professionals over the question of whether an attack they experienced occurred because of an unpatched vulnerability that could've been prevented. Around 60% of the 3,000 respondents from 2018 and 2019 said that one or more of their breaches could've prevented with an available patch for the known vulnerability. Additionally, 74% of companies cannot patch faster because they need more staff to do so [18, 19]. Statistics from Automox showed that 81% of the 560 IT and security professionals which they surveyed were breached in the past 2 years, with root causes of the breach being missing OS patches (30%), missing application patches (28%), and OS misconfiguration (27%). Phishing was the most common with 36% [20]. The point is that most of them could've been fixed with updates or patches, which means that cyber needs a behavioral change across the organization. The obvious recommendation would be to

update your apps, devices, and systems whenever possible and automate this if it is doable. Unfortunately, this can quickly become a burden. The superior recommendation for personal security hygiene would be to do a hard, factory, or complete reset of your systems once or twice a year. This will not only automatically put security updates into your systems, but it will also make those IT systems more available. Doing so with your devices tends to speed up their operation too. In terms of cyber resilience and robustness, updating, patching, or simply resetting your systems here and there will greatly increase the availability of the systems you need when you need them in a cyber-attack.

Secondly, users often need to be made aware of the settings and configurations of the applications and systems they use, IT staff cannot account for all the caveats of these configurations, and companies need to predict how users will utilize their applications. In one survey relating to checking security and privacy settings, out of 1,391 respondents, 9% check security or privacy settings after every usage, 32% multiple times per year, 12% once per year, 11% after registration, and the rest do not at all. That means that about half never check the privacy or security settings of apps. 5% of the respondents didn't know what security settings even were, and this study was based in Germany where citizens are familiar with the GDPR (General Data Protection Regulation) [21]. Another study on online social networks (OSNs) showed that "80% of users neither check their OSNs nor know about the privacy of their profile whether they have been offered default privacy settings or adequate privacy that meets the expected level" [22]. Social network settings usually won't create an availability issue for IT applications in a business. However, this sort of behavior goes to show that users have too much trust in the applications which they use daily. Most people likely think that these applications are plug'n'play or that the time to go through settings outweighs the benefits. This is a much harder behavior to change because it requires that the user exercises prudence. Therefore, motivating

users to read documentation, look for certain sections (especially IAM, users, and accounts settings), and research configurations and settings for things they use can reduce the chance of apps causing business-wide system issues that are the result of settings choices or from accidentally locking out important users from a system during an attack. In general, users can do a lot by putting in the effort to understand the apps and systems that they use daily and by knowing when to put in the time and when not to. Our recommendation would be to use the "break things", hacker mentality with personal applications and apply what you learn about apps to the systems you use at work.

Redundancy

Introduction

Redundancy refers to the extent to which systems, system elements, or other units are substitutable, that is, capable of satisfying functional requirements if significant degradation or loss of functionality occurs [34]. This idea can apply to engineering and physical design, but it very much applies to cyber resilience. Whereas robustness refers to the ability of systems to withstand disasters, redundancy is all about if that system can be substituted for another. In an IT or cyber socio-technical component of a business, we will look at the degree to which a business can substitute people, processes, and technologies around a cyber-attack and how the personal security hygiene of an individual can create conditions for better redundancy.

People

The redundancy of an organization's people may seem unrelated to personal security hygiene. However, personal security involves more than methods, strategy, and tactics normalized to the cybersecurity industry. As has been mentioned already in this paper,

cybersecurity is a multi-disciplinary practice. Therefore, individuals need more than cybersecurity knowledge and behavior to help our business resilience.

In the ‘Robustness’ section, we showed how knowledge management can make processes more robust and resistant during cyber-attacks. Truthfully, knowledge management is a powerful skill to have, and its benefits reach into many areas of business security and resilience posture. In this case, developing a personal knowledge management workflow can also make it easier to substitute people in a business during a cyber-attack. In other words, documentation, note-taking, and categorization or building a taxonomy of that knowledge can increase the redundancy of people in an organization. It gives the business the ability to mobilize the workforce during an attack and the ability to divvy out processes to the people that need them. For example, a SOC analyst may need someone to watch the SIEM (security information and event management system) while they do some digital forensics. Only 21% of people in a business communicate without using copious amounts of jargon and terminology that is too specific [23]. On top of that, data from Panopto shows that "42% of valuable company knowledge is unique to the individual employee [27]." If an employee needs to quickly hand off a process to someone else and everyone’s hair is already on fire because there’s a cyber-attack, then it will be a chaotic situation. Moreover, if an employee that handles work that is crucial during an attack recently left, then 42% of their work will have practically gone into the ether. It’s no coincidence that NIST’s Workforce Framework for Cybersecurity (NICE) has a section about knowledge management and this very issue [24, 25]. Knowledge management saves the organization time and puts people’s efforts where they need them the most during a cyber-attack.

Processes

Process redundancy starts with individuals who play a role in the process. Before a process is created, it is thought of and created by people. Intangible ideas and thoughts are added

to a knowledge base for an organization to use. When ransomware or another type of attack that justifies a need for a disaster recovery process arises, properly initiating the processes to mitigate the attack will be crucial for a successful recovery. Redundant processes for the same or similar event will help people choose from multiple courses of action. Sometimes software that is used by customers can be improperly designed and lack redundant processes to fix vulnerabilities that get exploited due to insecure programming practices. The inner platform effect is an event that can occur in an organization when software that is used by a customer is too customizable. Over time this inner platform effect slowly builds until it is too late to correct the customizable site. The inner platform effect is defined by Alex Papadimoulis on his blog The Daily WTF in 2006 as a result of designing a system to be so customizable that it ends up becoming a poor replica of the platform it was designed with. This "customization" of this dynamic inner platform becomes so complicated that only a programmer (and not the end-user) is able to modify it [26]. When an organization falls into an inner platform effect situation, the individual employee and customer cannot use the data being shared with them. Training at an individual level on how to organize and navigate problem and knowledge domains would be of interest to an organization to help the redundancy of their processes and mitigate the possibilities of inner platform effect. In doing so, an individual would be able to groom their own personal security hygiene by being aware of the issues that can occur when processes are not properly documented and tools that are too customizable continue to grow without being audited.

Technology

Redundancy is crucial with technology in businesses these days. It isn't obvious how applying personal security to one's life can improve the ability of a business to substitute its technologies. However, technology also includes data within it. Consequently, the idea of data recovery and disaster recovery and how that relates to personal backups comes into play.

Although the adoption rate has decreased since 2008, personal backup usage is at 11% as of 2021 [28]. People still see the value of backing up their data, whether family photos or a computer hard drive. This can sometimes take some getting used to if you're using a more advanced cloud service, a NAS (network-attached storage) device, or another self-hosted option. However, the general mentality remains to back up and save your data and technology. This can even apply more basically to "ctrl-s'ing" your documents or other media when you are editing the files for a prolonged period. In cybersecurity, backups refer to disaster recovery and business continuity. More than ever, this threat manifests itself as ransomware. Ransomware is some form of malware that encrypts your data and holds it for ransom till the money is given to the attackers. The average cost of such an attack sits at $4.54 million as of 2022 with the Ponemon Institute study. Not to mention, 8% of the attacks they found data on were ransomware attacks [1]. The problem shows itself when you look at the data restoration rates of these ransomware attacks. It seems that only 33% of companies avoid ransoms by restoring from backups [29]. This happens even when companies have backups because sometimes it is too expensive to mobilize those backups in a short time and cheaper to pay the ransom. We hypothesize that utilizing personal backups will give individuals the right perspective on backup processes, and it will allow them to utilize them or at least go to the right people to have them setup when they are necessary to the organization's resilience.

Resourcefulness

Introduction

Resourcefulness refers to "the ability to diagnose and prioritize problems and to initiate solutions by identifying and mobilizing material, monetary, informational, technological, and human resources [34]." Many will see this attribute as related to management and human

resources processes, and it is. However, all problems are affected by the resourcefulness of various components of the business. To improve business decision-making, an organization must think about how it can give more flexibility and utility to its people, processes, and technologies, and this goes for all parts of the business. Such an undertaking can paradoxically have the issue of lacking resources. Therefore, the next place to look would be at the individual level, and in this case, personal security hygiene and practices can improve the resourcefulness of these business components.

People

Most people understand that the social aspects of businesses are quite complex, and it can be hard to quantify and calculate interactions between various groups, departments, and individuals in an organization. During an attack, the issue of not knowing whom to contact or what to do becomes very apparent, and common bureaucratic bottlenecks exist in every business. For2fi a company that specializes in cybersecurity training states “Having workers know what to do to prevent or mitigate an attack is essential” [47]. Business communication and visibility are number one in cyber. If you don’t know what resources you have or how to get them, the business might as well get cyber-ransomed for all it is worth.

Typing up “chain of command” for a search query will show results like “Respect for chain-of-command is essential for the smooth growth, prosperity and effective management of an organization. If it works in the Army, it will prove invaluable in your business structure. [36]” The idea of a chain of command is a somewhat controversial topic in business. This debate exists because not all businesses need a chain of command, but many benefit from the hierarchical structure it offers, like in the case of the army. On the other hand, certain domains of the software industry work better with an open communication structure [35]. As explained in

previous sections, a knowledge management system or simple policies can greatly improve communication, but such a system assumes adoption and development across departments. Alternatively, there are personal security-related practices on the individual level that can aid this communication and resourcefulness issue for people during incidents like cyber-attacks. Specifically, OSINT, or "Open-Source Intelligence," can be a tool for individuals in an organization.

Literature, popular opinion, common sense, and general intuition suggest that people could do better at keeping their information private [21, 22]. Luckily, this can be an opportunity for resilience and resource visibility and not just a tool for hackers. In layman's terms, "OSINT is publicly produced and publicly available data that can be collected and shared without breaking laws or policies. [37]" Personal security is more than the normalized topic of cybersecurity, and that is why OSINT should be included as a piece of it. Part of securing one's personal life is having the ability and motivation to investigate entities that affect their goals. Most OSINT practitioners haven't received training in OSINT techniques or the risks involved with conducting investigations, so personally doing OSINT should require some effort. After all, OSINT, again, is NOT just a security thing. Investigation and research are a part of every problem-solving journey. Outside the workplace, personal security-focused OSINT should prioritize risk reduction and maximize resource visibility.

Pragmatically, this means using more than simple Google searches to figure out what your threats are. OSINT increases the resourcefulness of people in a business setting by expanding employee visibility within an organization. Studies including OSINT in education show that participants gain ample awareness about the accessibility of public information and malicious uses with such information [38]. Google "dorking" is one way to use Google for

OSINT purposes, but there is a myriad of unorthodox and unconsidered techniques for obtaining publicly available information.

Regardless of how public information about people, places, or things is obtained, there are two immediate benefits for a business when individuals conduct personal OSINT investigations. For one, OSINT increases awareness about public exposure of personal information for people. Secondly, OSINT reinforces habits and techniques that can be leveraged for resource visibility in an organization. In one study with 852 respondents and 1,947 instances of security and privacy behavior changes, 39% of the behavioral triggers were social. Moreover, socially triggered behaviors were 4 times more likely to be shared with other people. The motivation for this sharing was, by far, one of concern for others' security and privacy welfare [39]. In other words, if people are concerned enough about public exposure of their data, then doing OSINT should create a social domino effect that increases not only resource visibility during incidents but also general awareness. A 2022 Public Affairs study of over 4,000 adults from various U.S. states shows that 84% of people are somewhat concerned about the safety and privacy of the personal data that they provide on the internet [40]. In terms of resource visibility during an incident, employees are more likely to use techniques learned from OSINT investigations to figure out the organization hierarchy, roles, and general information necessary for their problem. Therefore, personal OSINT habits and behaviors are a great benefit to the modern user, and such habits positively impact the resourcefulness of people within an organization.

Processes

Creating an environment that encourages problem-solving can be developed into an organizational process for all employees. By teaching individuals how to use resources and

troubleshoot issues, an organization can mature their security awareness along with teaching individuals skills that they can use in their personal lives to make educated decisions and find a solution to their problems. An individual would be able to gain a fundamental understanding of security through training and webinars and then move onto a logical thought process to step-by-step troubleshoot work-related or personal-related issues [30]. When an individual is given the right training, they can become more resourceful in their personal lives. A resourceful person knows how to reach out for help and time manage, which is a skill that can always be improved. Good starting points for individuals to problem solve is to ask questions like what the actual problem is or who is experiencing this problem. Put simply, asking the 5 W's (When, Where, Why, What, Who) can be the beginning steps to helping an individual practice logical thought processes when problem-solving an issue, which in turn helps them become more resourceful and aware of something that might be a security vulnerability [30].

Possible ways to help employees learn and exercise logical problem-solving processes on their own would be to send out short daily or weekly security blogs that explain questions that anyone can think of to help start their problem-solving process or interesting podcasts to listen to while driving or simple trivia about best practices for being secure while using social media platforms. An effective way to deliver short, targeted pieces of content to learners without overwhelming them is known as microlearning [31]. This approach to learning has caught traction in the workforce. Through more research, the practice of microlearning through mind maps or short training is positively impacting the way people retain information and ultimately helping individuals become more resourceful. A study from the Multimedia Tools and Applications International Journal concluded that short-term memory could only manage around four elements at a time. The same study surveyed learning professionals about their experience of microlearning and found that 71% see its potential to increase knowledge retention, and nearly

68% believe it can drive engagement [32]. Another term for these sorts of personal security-related activities would be personal threat intelligence. Cybersecurity media, podcasts, news, and micro-learning sessions are effective ways to get prioritized information about the modern threat environment which can be retained and utilized for the resourcefulness of various processes in a business. The common user can execute these simple tasks once every couple of weeks, and the business can benefit. This comes down to knowing what's going on and what threats or opportunities exist.

Technology

An individual's resourcefulness depends on the person's awareness and understanding of how to spot vulnerabilities and what they might look like. Hardening a device at the individual's level helps secure an environment and allows individuals to better understand why certain settings should be selected on their devices. Organizations can send guidelines or recommendations to employees to help harden their personal devices to better secure them from external threats. By doing this, individuals can become aware of the tools to safely secure their personal information. Usually, these tools are free or not tools at all, like deactivating Bluetooth capabilities when it is not needed, using antivirus, host intrusion detection systems, and data loss prevention. This leads to a more resourceful person and ultimately helps the organization's security posture [33]. These hardening practices are great for organizations, but how can individuals change personal practices to have the same impact?

During an attack, incident, or breach, time is vital. As of 2022, the average data breach takes around 277 days to identify and contain [19]. By every metric and according to most, if not all, of the major security reports, two security practices reduce the possibility, cost, and time of a data breach – password management and multi-factor authentication [19, 43, 44, 45]. Some of

the most frequent and costly attacks of business email compromise and stolen or compromised credentials can be avoided using a combination of multi-factor authentication (MFA) and password management. Additionally, both attacks take the longest average time to identify and contain [19,42]. According to another popular study, 99.9% of incidents involved times where multi-factor authentication was not being utilized with the attacked component [41]. Data from IBM's X-Force Intelligence team also suggested that attackers were pivoting to new targets during 2021 because more U.S. companies started using MFA in their operations [43]. Verizon's top recommendation for companies to not become targets of an attack is to use two-factor authentication, their second is to not reuse or share passwords, and their third is to use a password manager! Verizon's top 3 recommendations to avoid attacks were around the idea of authentication methods and credential management [44]. Password management and MFA are quite cost-effective in avoiding losses from data breaches, so why not start with the individual?

Credential management is something that anyone can do. Most password managers are quite easy to install, and MFA is also straightforward to set up. Another survey from the Ponemon Institute, which partnered with Yubico (a 2FA physical key vendor), showed that only 36% of IT security respondents say their organizations use a password manager, and 46% said that email accounts are secured with 2FA. Only 29% of individual respondents said that they changed how they manage passwords by using a password manager. Most respondents said they use "stronger passwords." Lack of password manager usage is a slippery slope to credential and account compromise, and such data only refers to issues with password manager adoption. When looking solely at personal account usage with 2FA (two-factor authentication), only 40% of IT users and 36% of regular users are utilizing 2FA on any of their personal accounts. Of these same users, 50% and 54%, respectively, are reusing passwords across those personal accounts. To top it off, at best, only around 50% of the users who use 2FA are securing their email

accounts. So, only about 18% of the ~2,500 surveyed IT users had their email accounts secured with 2FA [46]. Combine this with the relevance of business email compromise and credential compromise, and we are left to wonder why people aren't using password managers and 2FA daily.

Security.org surveyed individuals about password manager adoption. Findings show that most people who use password managers do so because they cannot remember their passwords. It also showed that most don't use password managers because they are not secure (71%) or they are not sure that they need one (51%) [45]. In terms of 2FA adoption, the Ponemon study found that most organizations don't use 2FA because "usernames and passwords provide enough security" (60%) or two-factor authentication has not been requested (39%) [46]. The evidence shows that password managers and 2FA usage for accounts, especially email, improve the overall security of the business at a low cost. Additionally, using password managers ironically makes people more productive and speeds up workflows. Credential management and multi-factor authentication should be a part of everyone's personal security hygiene.

With individuals that utilize these techniques, a business can rule out certain attack vectors during an attack or incident. For example, a security operations team may be deciding to put effort during an investigation towards email account logs or endpoints logs. If the team knows that the applicable users were utilizing 2FA and password managers, it is much easier to rule out credential and account compromise-based attacks. Consequently, they will focus on the endpoint and look for evidence or IOCs (indicators of compromise) of malware. Therefore, credential management should be a part of every individual's personal security arsenal. It is a low-cost, high-reward method to increase the resourcefulness of technology, such as logging systems, IDR, EDR, and other monitoring tools during an attack. In other words, it makes it easier for people and technology to work together during an incident and bounce back from it.

Rapidity

Introduction

Rapidity is referred to as “the capacity to restore functionality in a timely way, containing losses and avoiding disruptions [48].” Organizations are concerned with operational Return on Investment (ROI) and system uptime for customers. Many see rapidity as an attribute that will define how quickly an organization can recover with minimal impact on the overall ROI and system uptime. Not only can technical tools and processes help an organization’s rapidity, but employees can as well. Training people to be well-rounded and prepared to implement recovery procedures will assist an organization’s rapidity rate. It doesn’t stop by only training and implementing tools to improve rapidity but by using metrics with qualitative and quantitative data that help manage and identify uptime improvements [49]. With this broad range of available metrics, it can be hard for an organization to identify a starting point to focus on. Therefore, it is recommended to start at the individual level and furthermore emphasize how the personal security hygiene of an individual can improve overall rapidity.

People

A recommended resource to bridge the gap between cybersecurity in personal and work life at the individual level is Security Education Training and Awareness (SETA), which Living Labs hosts. It is a platform that allows college students to apply networking, security, database, website and application development concepts and techniques learned from prior CIT courses. SETA is a program designed to help organizations mitigate the number of security breaches caused by human error. This is accomplished by increasing awareness of information security policies and helping people apply them during their daily activities to prevent security incidents

[52]. Utilizing SETA can enhance an organization's rapidity by positively influencing the lives of its employees, allowing them to bridge the risk awareness gap between life at home and work. When it comes to incidents and people, awareness is everything.

Security awareness training doesn't have to come from formal initiatives. For instance, one could introduce password managers and explain how they are not only convenient but also add to the security of the organization. Simply naming off some statistics and making it personal could persuade them to utilize them and improve their personal security. Statistically, people enjoy password managers because most people can't remember their passwords [54]. They start to understand why their inherent memory capacity problem creates a weakness with all their passwords. Subsequently, during an incident, they are more familiar with the risks around improper password hygiene. This sort of dynamic goes for all sorts of business security practices. However, teaching security is only a job for the security people, so it does not do much for the average person. What one may not notice is that all these problems with the rapidity of people during an incident revolve around business communication, so attacking that problem may be the answer.

Communication can sometimes become the true limiter in the success of businesses, and it slows response to incidents. As mentioned, people use too much jargon [23]. "Kaspersky research has found that over two-fifths (42 percent) of UK C-level specialists believe that jargon around cybersecurity is the biggest reason for lack of risk understanding at the top of organizations [55]." Nonetheless, jargon can sometimes be the only way to describe incidents, especially when the business is metaphorically on fire. With more awareness, though, jargon isn't an issue. For the individual, there are many ways to increase awareness, decrease misunderstandings of cyber incident jargon, and increase recovery speed during an incident. One of the most common terminology misunderstandings are around computer network terms. This

brings up an obvious solution. Individuals need to secure their home networks, and by doing so, they will learn not only the terminology of networking but also some of the difficult concepts that are the foundation of most cyber-attacks.

Home networks tend to be insecure on a large scale. It would not be unreasonable to say that most nation-states are using these large-scale weaknesses to their advantage. Moreover, although there isn't data to show that the average Joe is taking losses from home router attacks, espionage could be an issue, and there are not many statistics on such issues. A 2020 study from a German research group on home router security showed that even some of the more secure routers have around 20 critical CVEs (common vulnerability enumeration) and around 350 high-rated CVEs [56]. In layman's terms, almost all home routers probably have an easy weakness to exploit. Moreover, IoT (Internet of Things) is becoming very common, yet only 98 percent of these devices encrypt their traffic [57]. The home user can fix these issues.

Individuals have various ways to start doing network security, and these methods go from dead simple to advanced. We will go over advice that one of the top pentesting firms gives. If you aren't familiar with security at all, then get a device like a "Firewalla" or any firewall device with Pfsense on it. This is what we call network monitoring. This is how one can see into their home network and have a HUD (heads-up display) of all the network security information, alerts, and even some terminology. If you are more confident with information technology, then set up Pfsense with some other intrusion detection tools like RITA (Real Intelligence Threat Analytics), Suricata, Snort, Zeek, or other tools that can ingest data from Pfsense. Some routers don't allow this sort of setup, though. In that case, one can get fancy and redirect all of the network traffic through a personal computer running Linux by following their webcast and setting up security alerts that way, or one can simply utilize a "network tap [58]." The gist is that anyone can do home network security if they put in an hour of work about once a year. The result is that people

will have better communication during incidents because they are willing to put in a minimal amount of work at home to understand the main issue of infrastructure cyber security…networks. The next time they hear the word “malware,” they aren’t at all confused because they have security alerts for it on their firewall app for their device at home.

Process

The ability to recover in an efficient and timely manner in daily activities is often one fo the most important and most valuable tasks to organizations and people. During hurricane season or winter snow storms, people prepare for electrical outages by buying generators and stocking up on the necessities in order to recover from the affects as quickly as possible. “In the preparation and aftermath of a major natural disaster – the opportunity for fraud exists from multiple angles," said Susan Koski, Director and Head of Security & Enterprise Response with PNC Bank. While fraud can occur in many ways, two of the most common scams related to natural disasters including phishing attacks and counterfeit charities.” [59] Natural or man-made disasters occur across the world, and they affect individuals. Personal security and preparation to recover from these types of disasters can help individuals understand the processes and practices used in the workforce to recover in a rapid state. By linking the importance of a timely recovery at an individual level, people might show more awareness and alertness to possible incidents at work. 66 percent of Americans don’t feel fully prepared for natural disasters, which is 221.3 million US (United States) citizens. Educating and assisting individuals in their personal preparation for disasters and teaching them signs to look for, so disasters can be avoided will give organizations better rapidity during any incident, whether natural or unnatural [50].

It is recommended that a key process in the organization’s Business Continuity Plan (BCP) elaborate on the importance of personal security training at the individual level alongside the disaster recovery process. The human error factor is the largest security threat to an

organization while recovering from a natural or man-made disaster. This human error factor explains that the threat posed by the likelihood of mistakes made by an organization's own staff could result in the catastrophic loss of all crucial data during normal operations or from a recovery point. Rapidly recovering and restoring functionality to all systems is important, but it should also come with accuracy. A system that comes back up in a timely manner but holds a vulnerability made by an untrained or unaware employee can cause future data loss and system downtime [51]. Connecting daily activities that require rapid recovery, in a personal way, to procedures in the workforce can utilize personal habits and actions to better equip a company's rapidity.

The bottom line is that something as simple as disaster preparedness at home can extend to good business resilience during a cyber-attack. These habits help more than just cyber workers. Disaster preparedness helps human resources, other IT jobs, legal teams, and anyone who has a part in the business. A 2017 American Housing Survey showed that only 6 percent of Texas households without basements or multiunit structures had a tornado saferoom. This was lower than the 11 percent national average. In Florida, 70 percent of households reported having an emergency preparedness kit. In California, 30 percent of households with two or more people had a communication plan if cellular stopped working, 38 percent had a meeting location, and, luckily, 94 percent had emergency vehicles [54]. Some of these states are very prone to natural disasters, and yet a lot of households are unprepared in that regard. Risk analysis at home and work should be done, which accounts for incidents like these.

Technology

Most small businesses, in fact, 40 to 60 percent of them never reopen after a disaster, whether from natural or man-made causes. That is one of FEMA's most startling disaster recovery statistics and is important for organizations to consider when evaluating the technical

tools that help them rebound rapidly from an incident [53]. A good personal security practice to keep in mind is to always be aware of the location of vital data or systems. Something as simple as redundancy with personal valuables can be vital to rapid recovery after a personal incident. If a house is lost, then you shouldn't lose everything along with that house. Utilizing the cloud and creating hard copy backups are daily tools that people use for personal reasons. However, these same technologies can be used in disaster recovery programs in an organization. As shown earlier in this paper with research at Splunk, most organizations aren't prepared for ransomware, and ransomware is the epitome of a cyber disaster. 71 percent of companies only developed a ransomware playbook after an incident, and 66 percent reported paying the criminals, most of which did so out-of-pocket and some via cyber insurance [29]. At home, there will be times when insurance can cover something, but usually, the benefits of simply preparing properly for the incident will vastly outweigh the costs. This all comes down to doing the research, working on the problem, and doing due diligence. This is not as easy as some other recommendations for cyber resilience, but it is the hard truth. When it comes to technology, people must learn to utilize search queries, documentation, knowledge management, and communication in innovative ways. In cases where a potential disaster can mess up the technology that runs our lives, we need a backup plan. Do this planning annually and bring those planning habits to work anytime you work on a problem or make a decision that can affect the overall business.

SETA Program Design

Security Training and Awareness Programs are essential to creating a business model that includes security. Our background research revealed that the most cost-effective way to reduce the cost of a breach is to train employees [1]. Additionally, as shown in the "Resourcefulness-People" section, socially triggered efforts in security are the ones that are most likely to be adopted across the organization [39]. A training and awareness program that is properly

conducted should be cost-effective and motivate contemplation and social sharing of cybersecurity concepts and threats. If employees are more concerned for the security and privacy welfare of others, then the program is doing a good job. This is the hardest part of employee training, that is, making it not seem like an inconvenience and more of a necessity. Three methods are defined in research: superficial triggers of sparks (ads or social proof notifications), facilitators (make it look easier), and signals (reminders and calls to action) [39]. We will utilize these three tactics to create an effective SETA program.

People

To improve people in an organization, we should use a mix of the methods mentioned above and general strategies for building habits. For people, our research shows that we should make the training personal or more applicable to what they do. It is crucial for the individual to realize the importance of good personal security and how it affects their well-being and the operation of the business. Getting leadership involved is the first step in the process. After that, social proof notifications and reminders that everyone on a team has done some training should be shown. To keep growth and cultivation consistent, training should be in short bursts, personal, and memorable. The participants should also walk away with a tool they will be persuaded to utilize.

Process

Improving processes in an organization is much more difficult than conducting traditional training. To improve processes through SETA, training must be personalized to a team's operations. One easy way to do this is to supply departments or teams with personalized recommendations and tools for personal security hygiene, and then tabletop exercises could be conducted using these. This may or may not be facilitated by a security professional. This sort of

training could take place for half an hour. Alternatively, personalized training videos should be made that require the participant to install certain tools and upload proof of completion. Such training should be intermittent and utilize calls to action, and the process should be straightforward to complete.

Technology

To improve the use of technologies in an organization, from personal security habits, the organization should use the framework to educate and motivate participants. Firstly, show users the value of certain personal security habits when it comes to improving technology utilization in the business. Then, show the user resources, techniques, workflows, and skills to not only improve personal security but improve how technology is viewed, managed, and found on the internet. In a nutshell, show people how to solve problems better with technology, and that includes using search engine technology and research technologies to find technological solutions.

SETA Program Implementation

Leadership Buy-in

This was briefly stated above. However, it cannot be overstated. In a corporate setting, leadership buy-in is practically required to have effective training. Employees will only be able to put in the work or properly contemplate cybersecurity with the support of their supervisors and managers. Roles and responsibilities should be established before starting a SETA program.

Tabletop Exercises

Tabletop exercises can be more personalized than other sorts of training. A game like “Backdoors and Breaches” or a customized game that is personalized to certain departments or personal security situation can be fun and memorable ways to highlight certain personal security

practices. These take a bit more involvement and devotion. Therefore, this should require a security SME (subject matter expert) facilitator to discuss security alongside employees.

Interactive Training

Interactive training would be video-based and have users complete certain tasks. Security teams could design virtual machines to let users try out certain tools and workflows where it is necessary. These would be guided tutorials on certain skills, habits, or tools.

Team/Department Produced Security Demos (Video or In-Person)

These could involve various teams in videos to "put a face to the team" and make it more personal. For instance, the network and security team could work together to show users how to set up home network monitoring, or they could show hacking POCs (proof of concepts) to users on why they should use better passwords and a password manager. This could also be done in-person maybe in the lobby or as a sort of seminar where people outside of the organization are also invited.

Conclusion

Overview

Personal security is not seen as an important practice to uphold at home, because people fail to see the value of it. It is reasonable to think that the costs of putting up personal security protections and consistently reducing one's personal risk surface is higher than the benefits of doing so. Most people say, "no one wants my data" or "I'm not a target." On the contrary, everyone is a target, and this is especially true when it comes to businesses and corporate assets. More importantly, businesses are the primary target. If personal security can cost-effectively add resilience to a business's people, processes, and technology, then such personal security habits

should be integrated into people's lives. Additionally, there should be systems that make this integration easier and motivate individuals by making it personalized to their innate goals.

Outcome 1

Thorough research was conducted to find evidence of connections between personal security habits and business cyber resilience in various areas of operations. A framework was developed by combining the 4Rs resilience framework and the PPT model of people, processes, and technology. Our research was applied to this constrained framework to curate innovative recommendations and personal-to-business connections based on the uncovered evidence.

Outcome 2

A general program design and approach was hypothesized for implementing the developed personal-to-business framework in a corporate setting. The most promising part of such a program involves demos that are facilitated by an enthusiastic security team.

Future Work

A more exhaustive framework less constrained to the 4Rs and PPT (people, process, technology) would be more effective at covering all areas of personal security. Constraints are beneficial because they force ideas to be a bit more innovative. However, numerous personal security habits should have been mentioned that benefit organizations more than some of the unorthodox recommendations given in this research. Covering areas of privacy and talking about business cybersecurity from the perspective of risk reduction could allow for more coverage of the cybersecurity and personal security domains.

Developing a program framework to implement a wider variety of personal security habits should be a consequence of this research. Figuring out personal security recommendations and integrating them into societal habits are two very different problems. Research, statistical

studies with surveys, and pragmatic approaches to large-scale implementation should be a focus of subsequent research.

References

[1] Ponemon Institute LLC, “Cost of a Data Breach 2022,” ibm.com, 2022. https://www.ibm.com/sg-en/security/data-breach

[2] Ponemon Institute LLC, “The Cybersecurity Illusion: The Emperor Has No Clothes,” Ponemon Institute LLC, 2019. [Online]. Available: https://go.attackiq.com/rs/041-FSQ-281/images/REPORT-Ponemon1_vF2.pdf

[3] C. Stamford, “Gartner Says Cybersecurity, Application & Integration Strategies and Cloud Are Top Technology Priorities for Midsize Enterprises,” Gartner, Inc., Sep. 26, 2022. https://www.gartner.com/en/newsroom/press-releases/2022-09-26-gartner-says-cybersecurity-application-and-integration-strategies-and-cloud-are-top-technology-priorities-for-midsize-enterprises

[4] S. Kissoon, “Optimum Spending on Cybersecurity Measures: Part II,” Journal of Information Security, vol. 12, pp. 137–161, Jan. 2021, doi: 10.4236/jis.2021.121007.

[5] Fitch Solutions, Inc., “US Cyber Insurance Sees Rapid Premium Growth, Declining Loss Ratios,” Fitchratings.com, 2022. https://www.fitchratings.com/research/insurance/us-cyber-insurance-sees-rapid-premium-growth-declining-loss-ratios-13-04-2022

[6] J. Akin, Ed., “Identity Theft Statistics: Fraud Is on the Rise - Experian,” www.experian.com, Oct. 11, 2022. https://www.experian.com/blogs/ask-experian/identity-theft-statistics/#:~:text=to

[7] C. Stouffer, “Personal cybersecurity resolutions for 2022: A month-to-month guide,”

us.norton.com, Jan. 23, 2022. https://us.norton.com/blog/privacy/personal-cybersecurity (accessed Nov. 15, 2022).

[8] S. L, “Phishing attack statistics 2022,” CyberTalk, Mar. 30, 2022. https://www.cybertalk.org/2022/03/30/top-15-phishing-attack-statistics-and-they-might-scare-you/

[9] B. Debusmann, “Why remote working leaves us vulnerable to cyber-attacks,” BBC News, Jul. 25, 2021. [Online]. Available: https://www.bbc.com/news/business-57847652

[10] National Institute of Standards and Technology, “robustness - Glossary | CSRC,” csrc.nist.gov. https://csrc.nist.gov/glossary/term/

[11] Slandau, “12 illuminating Zero Trust statistics and trends in 2022,” CyberTalk, Aug. 05, 2022. https://www.cybertalk.org/2022/08/05/12-zero-trust-statistics-and-trends-in-2022/

[12] D. Borkovich and R. Skovira, “Working From Home: Cybersecurity in the Age of Covid19,” Information Systems, vol. 21, pp. 234–236, Sep. 2020, doi: 10.48009/4_iis_2020_234246.

[13] N. Cicchitto, “Emailing Behaviors: Do Business and Personal Email Accounts Overlap?,” The Identity and Access Management Blog, Aug. 24, 2017. https://www.avatier.com/blog/personal-vs-work-email/

[14] Financesonline.com, “56 Email Statistics You Must Learn: 2022 Data on User Behaviour & Best Practices,” Financesonline.com, Jun. 09, 2021. https://financesonline.com/email-statistics/

[15] S. Wang and H. Wang, “A Sociotechnical Systems Analysis of Knowledge Management for Cybersecurity,” International Journal of Sociotechnology and Knowledge Development (IJSKD), vol. 13, no. 3, pp. 77–94, 2021, doi: 10.4018/IJSKD.2021070105.

[16] L. Dobrica, “KNOWLEDGE IN ACTION TOWARDS BETTER KNOWLEDGE MANAGEMENT IN ORGANIZATIONS,” Management Research and Practice, vol. 13, no. 2, pp. 26–35, 2021.

[17] S. Zhao, Y. Jiang, P. Xiaobao, and J. Hong, “Knowledge sharing direction and innovation performance in organizations: Do absorptive capacity and individual creativity matter?,” European Journal of Innovation Management, vol. aheadofprint, Mar. 2020, doi: 10.1108/EJIM0920190244.

[18] E. Georgescu, “Software Patching Statistics for 2019: Common Practices and Vulnerabilities,” Heimdal Security Blog, Dec. 03, 2019. https://heimdalsecurity.com/blog/software-patching-statistics-practices-vulnerabilities/

[19] Ponemon Institute LLC, “COSTS AND CONSEQUENCES OF GAPS IN VULNERABILITY RESPONSE.” [Online]. Available: https://media.bitpipe.com/io_15x/io_152272/item_2184126/ponemon-state-of-vulnerability-response-.pdf

[20] K. Sheridan, “Missing Patches, Misconfiguration Top Technical Breach Causes,” Dark Reading, Mar. 25, 2020. https://www.darkreading.com/vulnerabilities-threats/missing-patches-misconfiguration-top-technical-breach-causes

[21] M. Rudolph, D. Feth, and S. Polst, “Why Users Ignore Privacy Policies – A Survey and Intention Model for Explaining User Privacy Behavior,” in HumanComputer Interaction. Theories, Methods, and Human Issues, 2018, pp. 587–598.

[22] U. Din, N. Islam, J. Rodrigues, and M. Guizani, “Privacy and Security Issues in Online Social Networks,” Future Internet, vol. 10, Nov. 2018, doi: 10.3390/fi10120114.

[23] K. Wojda, “7 Surprising Internal Communications Statistics,” Spectrio, May 01, 2020. https://www.spectrio.com/internal-communications/7-surprising-internal-communications-stats/ (accessed Nov. 15, 2022).

[24] NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES, “Knowledge Management | NICCS,” niccs.cisa.gov. https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/knowledge-management (accessed Nov. 15, 2022).

[25] “NICE Cybersecurity Workforce Framework | CISA,” www.cisa.gov. https://www.cisa.gov/nice-cybersecurity-workforce-framework

[26] M. Jones, “The Inner-Platform Effect - The Daily Software Anti-Pattern,” Exception Not Found, Aug. 15, 2018. https://exceptionnotfound.net/the-inner-platform-effect-the-daily-software-anti-pattern/ (accessed 2022).

[27] J. Chan, “Why Not Sharing Institutional Knowledge is Costing Your Company Money,” 360Learning. https://360learning.com/blog/institutional-knowledge/

[28] Yev, “How Often Do People Backup Their Computers?,” backblaze.com, Jun. 08, 2021. https://www.backblaze.com/blog/the-state-of-backups-whos-most-at-risk/

[29] Splunk Inc., “The State of Security 2022,” Splunk, 2022. https://www.splunk.com/en_us/campaigns/state-of-security.html (accessed Nov. 15, 2022).

[30] “An Effective Problem Solving Process for IT Professionals,” *Source One Technology*, Jan. 04, 2017. https://www.sourceonetechnology.com/problem-solving-process/

[31] “10 Facts and Stats About Learning Retention | Bridge,” *www.getbridge.com*, Jul. 12, 2022. https://www.getbridge.com/blog/learning-analytics/10-stats-about-learning-retention-youll-want-forget/ (accessed Nov. 22, 2022).

[32] R. P. Díaz Redondo, M. Caeiro Rodríguez, J. J. López Escobar, and A. Fernández Vilas, "Integrating micro-learning content in traditional e-learning platforms," *Multimedia Tools and Applications*, vol. 80, no. 2, pp. 3121–3151, Sep. 2020, doi: 10.1007/s11042-020-09523-z.

[33] "What Does It Mean to Harden a Device?," *CBT Nuggets*. https://www.cbtnuggets.com/blog/technology/system-admin/what-does-it-mean-to-harden-a-device

[34] K. Tierney and M. Bruneau, "Conceptualizing and measuring resilience a key to disaster loss reduction," May 2007.

[35] R. Adner, P. Puranam, and F. Zhu, "What Is Different About Digital Strategy? From Quantitative to Qualitative Change," Strategy Science, vol. 4, no. 4, pp. 253–261, 2019, doi: 10.1287/stsc.2019.0099.

[36] Second Wind Consultants, "Teach Your Employees To Respect The Chain-of-Command - Second Wind Consultants," Second Wind Consultants, 2019. https://secondwindconsultants.com/resources/teach-your-employees-to-respect-the-chain-of-command/

[37] Media Sonar, "Is OSINT Legal?," Media Sonar Technologies, 2020. https://mediasonar.com/2020/04/30/legal-ethical-osint/

[38] A. Mendlein, T. Nguyen, and A. Rege, "Cybersecurity Awareness and Training through a Multidisciplinary OSINT Course Project." doi: 10.18260/1234367.

[39] S. Das, L. A. Dabbish, and J. I. Hong, "A typology of perceived triggers for End-User security and privacy behaviors," Aug. 2019, pp. 97–115. [Online]. Available: https://www.usenix.org/conference/soups2019/presentation/das

[40] M. Newall and J. Sawyer, “A majority of Americans are concerned about the safety and privacy of their personal data,” IPSOS.com, May 05, 2022. https://www.ipsos.com/en-us/news-polls/majority-americans-are-concerned-about-safety-and-privacy-their-personal-data

[41] A. Weinert, “Your Pa$$word doesn’t matter,” microsoft.com, Jul. 09, 2019. https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/your-pa-word-doesn-t-matter/ba-p/731984

[42] K. Thomas and A. Moscicki, “New research: How effective is basic account hygiene at preventing hijacking,” Google Online Security Blog, May 17, 2019. https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

[43] IBM X-Force IR Team, “X-Force Threat Intelligence Index 2022,” ibm.com, 2022. https://www.ibm.com/downloads/cas/ADLMYLAZ (accessed Nov. 22, 2022). [44] Verizon Report

[44] G. Bassett, C. D. Hylender, P. Langlois, A. Pinto, and S. Widup, “DBIR Data Breach Investigations Report,” verizon.com, 2022. https://www.verizon.com/business/resources/reports/dbir/ (accessed Nov. 22, 2022).

[45] G. Turner, “Password Manager and Vault 2021 Annual Report: Usage, Awareness, and Market Size,” Security.org, Dec. 06, 2021. https://www.security.org/digital-safety/password-manager-annual-report/

[46] Ponemon Institute LLC, “The 2020 State of Password and Authentication Security Behaviors Report,” Ponemon Institute LLC, 2020. Accessed: Nov. 22, 2022. [Online]. Available: https://www.nass.org/sites/default/files/2020-04/Yubico%20Report%20Ponemon%202020%20State%20of%20Password%20and%20Authentication%20Security%20Behaviors.pdf

[47] Clikcloud. (n.d.). *Role of your employees in Cybersecurity*. For2Fi. Retrieved November 22, 2022, from https://www.for2fi.com/role-of-your-employees-in-cybersecurity/

[48] M. Bishop, M. Carvalho, R. Ford, and L. Mayron, "Resilience is More than Availability," in *New Security Paradigms Workshop*, 2011, p. 98.

[49] "The Qualitative and Quantitative Metrics You Should Measure for Your Inbound Marketing Strategy," *BenchmarkONE*, Mar. 10, 2021. https://www.benchmarkone.com/blog/qualitative-quantitative-metrics-inbound-marketing-strategy/

[50] "66% of Americans Don't Feel Fully Prepared for Natural Disasters, and 45% Don't Know if Their Insurance Covers Related Claims," *ValuePenguin*. https://www.valuepenguin.com/natural-disaster-preparedness-survey

[51] "The human error factor in disaster recovery. - Kinetek," *www.kinetek.co.uk*. https://www.kinetek.co.uk/insights/the-human-error-factor-in-disaster-recovery_37.html (accessed Nov. 29, 2022).

[52] "Security Education Training and Awareness (SETA) – IT Living Lab." https://livlab.org/seta/

[53] T. Rock, "23 Disaster Recovery Statistics You Should Know," *Invenio IT*, 2015. https://invenioit.com/continuity/disaster-recovery-statistics/

[54] S. Bucholtz, "Measuring Disaster Preparedness with 2017 AHS Data | HUD USER," www.huduser.gov, Mar. 23, 2020. https://www.huduser.gov/portal/pdredge/pdr-edge-frm-asst-sec-032320.html (accessed Dec. 06, 2022).

[55] A. Hurst, “Cybersecurity jargon between C-suite and specialists a key barrier,” Information Age, Nov. 22, 2022. https://www.information-age.com/cybersecurity-jargon-impacting-communication-between-c-suite-specialists-123500747/ (accessed Dec. 06, 2022).

[56] P. Weidenbach and J. Vom Dorp, “Home Router Security Report 2020,” FRAUNHOFER-INSTITUT FÜR KOMMUNIKATION, INFORMATIONSVERARBEITUNG UND ERGONOMIE, FKIE, 2020. [Online]. Available: https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf

[57] Palo Alto Networks | Unit 42, “2020 Unit 42 IoT Threat Report,” paloaltonetworks.com, 2020. https://unit42.paloaltonetworks.com/iot-threat-report-2020/

[58] BHIS and J. Strand, “Webcast: No SPAN Port? No Tap? No Problem!,” Black Hills Information Security, Jul. 23, 2021. https://www.blackhillsinfosec.com/webcast-no-span-port-no-tap-no-problem/ (accessed Dec. 06, 2022).

[59] “Natural Disasters Bring Increased Fraud – How to Beware of Scammers.” Natural Disasters Bring Increased Fraud – How to Beware of Scammers | PNC Insights, 21 Jan. 2022, www.pnc.com/insights/personal-finance/protect/natural-disasters-bring-increased-fraud.html.

[60] S. Sjouwerman, “Stanford Research: 88% Of Data Breaches Are Caused By Human Error,” *blog.knowbe4.com*. https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error#:~:text=Researchers%20from%20Stanford%20University%20and