The Effects of COVID-19 on Cybersecurity and Securing a Post-COVID World

Ryan Pizzo

A Senior Thesis submitted in partial fulfillment
of the requirements for graduation
in the Honors Program
Liberty University
Spring 2023

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial
fulfillment of the requirements for graduation from the
Honors Program of Liberty University.

_____
Melesa Poole, Ph.D.
Thesis Chair

_____
James McNicholas III, Ph.D.
Committee Member

_____
David Schweitzer, Ph.D.
Assistant Honors Director

_____
Date

Abstract

The world became hardly recognizable throughout the COVID-19 pandemic as the normal state of the world was disrupted. In addition to affecting everyday life, the pandemic touched every industry, especially that of cybersecurity. To properly remediate for the future of cybersecurity, the trends in cybercrime seen throughout the pandemic warrant further investigation. An overall increase in cybercrime was clearly observed with no signs of plateauing. This trend was paired with developing sophistication of cybercrime means and methods. In response to this, a defense-in-depth strategy focusing on a layered defense approach strengthens an organization's security posture. Focusing on every policy and technology implementation to limit attacker impact is the path to security in this post-COVID era. A proactive focus on how to leverage future technologies and methodologies will pave the way to securing the future.

Keywords: Cybersecurity, COVID-19, Cloud Security, Ransomware, Work-From-Home

The Effects of COVID-19 on Cybersecurity and Securing a Post-COVID World

COVID-19 disparaged the known normality of the world at its height and left no industry untouched, including that of cybersecurity. Although the majority of focus gravitated toward the most well-known industries such as healthcare and business during the pandemic, the cybersecurity industry also suffered a heavy loss while undergoing a drastic reshaping of the overall landscape. To fully quantify the reaching effects that COVID-19 had on the world of cybersecurity, several variables must be considered. The first is the trend of cybercrime committed pre-COVID and post-COVID and whether any possible conclusions can be drawn from these figures. In the pursuit of gaining an overall picture of the effect of COVID-19, an analysis of how cybercrime has evolved since the emergence of the pandemic is necessary. The primary focus is on certain categorizations of cybercrime and what vectors of attack fluctuated, if any.

Pivoting from a purely analytical approach to the study of the reach of COVID-19, the next key to understanding its effect is comprehending the rapid terraforming in the field of cybersecurity. Grasping how these changes will continue to shift the threat landscape of cybersecurity is crucial to assessing threats in the post-COVID modern era. Once threats have been assessed, proactive remediation is the key to securing the future period of this industry. Many common-place best practices need to be retrofitted to best combat the ever-evolving threats in this post-COVID age. In addition to these practices, the implementation of "future" technology must be thoroughly investigated in order to stay ahead of the curve. COVID-19 was a catalyst to evolve the cybersecurity world; whether the industry adapts and acknowledges the effects of that catalyst will provide insight to the security of the future.

Literature Review

Foundational Studies

The Evolution of Cybercrime due to COVID-19

COVID-19 had a significant impact on cybercrime; however, examining how cybercrime has evolved is imperative to comprehending the analysis of the data. There is a myriad of unique ways the internet can be exploited to achieve criminal ends. A society at the brink of the digital era was quickly forced into a fully digital reality seemingly overnight (Buil-Gil et al., 2020). This shift applied to every industry (aside from critical sectors), and employees who potentially had never had to rely on telework technologies were required to engrain them into their daily routine. The consequences of this transition are yet to be fully realized; however, certain effects were seen even in the immediate years following (FBI IC3, 2015, 2016, 2017, 2018, 2019, 2020, 2021). In the criminal world, this shift was no different. While society transitioned online, the "opportunities for crime appear to have shifted towards cyber-dependent or cyber-enabled crime" (Buil-Gil et al., 2020, p. 1) and criminals who relied on strictly physical operations were required to adapt to the societal changes that overthrew the norms known for so long.

In general, fear and the ability of the criminal to force a victim to act in response to fear, is one of an attacker's greatest strengths. During the pandemic, public fear was at a higher level even without criminal intervention, therefore victims could be coerced into taking actions that pre-pandemic would not have been a viable attack vector (Furnell & Shah, 2020). Therefore, crime was inevitably up due to the increased probability of success for even the most average cybercriminal. This is especially true when paired with tightening economic pressure, as desperation increased among the average citizen simply looking to pay rent. These factors can be

theorized to have pushed the standard victim to be increasingly targeted along with the everyday technical citizen pushed towards crime.

How COVID-19 Has Shifted the Cybersecurity Threat Landscape

Transition to an "At-Home Workplace". The ramifications of COVID-19 and how the cyber threat landscape was reshaped must be scrutinized. Seemingly overnight, the entire world shifted from a primarily in-person office setting to an at-home workplace. These changes were severely accelerated due to the immediate health concerns, and when change is rushed, holes in security are exposed. This was the case during the aggressive change to a stay-at-home work environment during COVID-19 as "employees were transferred from companies or offices to their homes without adequate protection for performing tasks over the Internet" (Machado & Gouveia, 2021, p. 4). Working from home was already an option for some employees in various industries; however, in most cases, specific procedures and policies guided the employees on how to remain secure. In the case of the mass transition to a work-from-home environment, these policies and procedures, assuming they existed, did not account for a large number of employees under them or the potential technological ineptitude of those employees (Borkovich & Skovira, 2020).

In a state of emergency, such as the COVID-19 pandemic, the procurement of devices able to be brought home from the office securely was nearly impossible unless already possessed (Eiza et al., 2021). Supply chain failure during the pandemic restricted procurement of a variety of equipment (Borkovich & Skovira, 2020). Therefore, most industries took a *bring your own device* (BYOD) approach that leveraged tools such as virtual private networks (VPNs) to connect foreign hosts to a company-specific network (Borkovich & Skovira, 2020). Without mentioning

the many other consequences of pivoting to a work-from-home approach, from a strictly cybersecurity perspective, a BYOD approach with ill-equipped employees is a recipe for disaster, which was confirmed through cybercrime reports (FBI IC3, 2019, 2020, 2021). A large part of the strength of an information technology team when defending against cybersecurity threats is the ability to control exactly what software and versions are used on any given device on the network. However, when a BYOD policy is implemented, that ability can be lost completely. An employee's computer can be extremely vulnerable to compromise and allow an attacker an easy route to accessing a private corporate network that houses very sensitive information (Borkovich & Skovira, 2020).

Another large threat for a cybersecurity team that was presented with the emergence of COVID-19 is the exfiltration and insecure transfer of sensitive industry or customer information. Average employees are not cybersecurity conscious and, therefore, will often sacrifice security for ease of work. This sacrifice takes the form of "downloading sensitive information onto thumb drives, forwarding work emails to their personal computers, or sharing documents that they should not" (Borkovich & Skovira, 2020, p. 3), all of which pose a larger cyber threat landscape for any company. In the current age, the average employee tests their security consciousness daily by providing easy shortcuts without any foreseeable downsides aside from compromising security (Borkovich & Skovira, 2020). In an office setting, this opportunity to take shortcuts is less heightened as personal computers and accounts are not easily accessible except through company-monitored means (Vadlamudi & De, 2021). In addition, there is a social factor to integrity that the office breeds by maintaining an environment where anyone could walk into any employee's office space at any moment, which deters compromising behaviors. Accordingly,

when integrity is suddenly tested for a myriad of employees, there will always be those who value efficiency over integrity.

In a 2020 study of teleworking professionals, this idea was thoroughly put to the test (Borkovich & Skovira, 2020). The study interviewed several professionals working remotely due to COVID-19, and responses were consistent in lacking a cybersecurity-conscious mindset. One such response highlights the efficiency over integrity mindset when an engineer at a small business states, “Don’t tell my IT guy, but I have discovered interesting workarounds to get my job done more efficiently” (Borkovich & Skovira, 2020, p. 8). Another employee interviewed states, “Yeah, I do forward work emails with attachments to my home email address…it’s just more convenient” (Borkovich & Skovira, 2020, p. 8). Additionally, this employee was self-identified as a payroll supervisor, highlighting the level of sensitive information this employee handles. Employee mindsets that follow this trend are dangerous in any work environment due to that very mindset being one of the leading causes of breaches in even the largest businesses.

Furthermore, the rapid adoption of many public applications not previously used, such as video conferencing, VPN, and other tools, opened the attack surface for many organizations. Moreover, the technologies employed to allow regular business practice to continue may be inherently vulnerable and open up an organization to a breach. The abrupt move to an almost solely at-home work environment left companies ill-prepared to combat the challenges that resulted from this change.

Shift to Cloud-Based Computing. A further change to the overall cybersecurity threat landscape is the shift to cloud computing that was catalyzed by the COVID-19 pandemic. Cloud computing “is aimed to provide hosted services over the internet” (Alouffi et al., 2021, p. 1) that

are not managed by the client but rather by the provider. This newer trend in IT infrastructure has been in use for a number of years with the leaders in this industry being Amazon's AWS and Microsoft's Azure. These providers take care of all physical and virtual infrastructure needs at varying levels coined Infrastructure as a Service (IaaS) and Software as a Service (SaaS), along with other services. The pandemic and the rise in the need for flexibility have pushed many organizations towards the cloud rather than in-house (on-premises) infrastructure solutions. This conversion has positive and negative implications; however, at a general level this change is positive in a security aspect (Alouffi et al., 2021). This mass migration to cloud computing options "is anticipated to increase at a significant compound annual growth rate (CAGR) of 22.59% during the years of 2019 to 2022" (Alashhab et al., 2021, p. 2). Many factors contribute to that number; however, a highly theorized reasoning is that the pandemic and the need for managed infrastructure, along with access to corporate resources through the internet, enable a work-from-home environment better than an on-premises solution (Alashhab et al., 2021).

From an attacker's perspective, targets remain consistent in a post-COVID world, exploiting people rather than systems. Although a shift to the cloud does pivot the vectors that attackers take in more technical attacks, in the ordinary attack, the same methods persist. There is an expression in the cybersecurity community that people are the weakest link in cybersecurity. Accordingly, although a migration to the cloud shifts where the infrastructure is hosted and even potentially who is the manager, the primary vector for cybercrime and intrusion remains unchanged. In light of this, pivoting remediation efforts towards cloud-specific tactics while not neglecting the overlooked methods that secure the people rather than the organization is important.

FBI Crime Report

When performing analytics on any event and determining the breadth of impact, a holistic review of all existing data sources is required. To begin discussing the various points of data utilized in this analysis, the largest dataset will be examined first: the FBI Internet Crime Report. An FBI subdivision called the Internet Crime Complaint Center (IC3) maintains a record of all internet-based crime (FBI IC3, 2016). Individual filings create an annual report detailing the specifics trends and breakdown the number of cybercrimes for that year by age of victim and type of crime. The IC3 has publicly released these reports all the way back to 2001. These reports provide a wealth of data from which to analyze and elicit trends.

The pursuit of a clear picture of the effects COVID-19 had on cybercrime requires a defining of terms. Due to the lack of a clear definition of cybercrime in the FBI report, an agreed upon definition must be determined. The European Commission attempted to define the broad category of cybercrime. The threefold definition can be condensed into the following: traditional and internet specific crimes "committed over the electronic communication networks and information systems" (Anderson, 2013, para. 10). An important note regarding this definition is that the victim does not need to be the user of a computer to be targeted; simply, the perpetrator needs computer or internet access. Although individuals with regular computer access may provide a larger attack surface for a cybercriminal, anyone can be a victim of cybercrime. Additionally, this definition captures a wide range of technical expertise required to carry out these crimes. The criminal can be regarded a cybercriminal whether they committed identity theft over the phone or carried out a sophisticated ransomware operation against a Fortune 500

company. Now that an authoritative definition of cybercrime has been established for this study, the supporting research will be examined.

US Census Data

To supplement the vast amount of data provided in the IC3 annual reports, the US Census is utilized as a means to further analyze the impact of COVID-19 per pre-defined age strata. Since the IC3 report provides data on the counts and losses of cybercrime based on the age of the victim, analysis can only be done well if the total population of each age strata is known. This fact is due to the potential that although one age group could have a larger count of cybercrime, this may be the result of a larger population to target. The US Census Bureau publishes an annual breakdown of the population based on age which allows for the population of each defined FBI age strata to be determined (US Census Bureau, 2015, 2016, 2017, 2018, 2019, 2020, 2021). Possession of the population sizes of each age strata allows for an analysis that focuses on percentage affected and average losses per thousand people instead of totals from each of those categories.

Hypothesis

Determining a baseline prediction of the trends to be analyzed will guide the examination of the data. Due to the large number of rapid changes that COVID-19 brought about, the expectation for the research is that the losses and count of cybercrime increased throughout and after the pandemic. The initial anticipated spike in cybercrime numbers would be expected to continue to rise even after the pandemic. The reason for this prediction is due to the transition of business operations that took place during the pandemic paired with an increase in overall fear and desperation. Continuing this line of reasoning, it is suspected that the age group that would

be most highly targeted is also the group most effected by the pandemic. This would include those who are 60 years old and older. This demographic was isolated due to the raging pandemic which expectedly would make them easier targets for cybercrime supporting the above hypothesis.

Methodology

Data Compilation

The nature of research conducted for this study consisted of compilation of years of publicly accessible data in the form of the FBI Internet Crime Report and the US Census. Both of these sources provide annual reports that can be combined with previous years to provide a look at the trends over a period of time. The designated period for this research was 2011-2021, in order to provide ample data preceding the events of COVID-19 to establish the baseline. In regard to the means of data collection for each dataset utilized, the FBI crime report is created from the complaints that FBI IC3 receives each year. Data based on the nature of the complaint and the victim are recorded and presented in the annual report.

Although the US Census Bureau formulates a census every ten years to be used in political apportionment, the government office also publishes yearly reports, one of which is a population breakdown based on age groups. This report was utilized to properly calculate the population for each of the age strata used in the FBI Internet Crime Report. Therefore, the US Census data from 2011-2021 was extracted and paired with the data from the FBI crime report to provide a more statistically accurate representation of the data. The assembling of this amount of data results in a combined dataset to perform further analysis on from a number of differing angles rather than simply in a vacuum.

Data Categorization

An understanding of how the data was categorized and parsed is crucial to the analysis stage of research. In regard to the primary dataset of the FBI Internet Crime report the creation of age strata was done internally by the IC3. The age strata are under 20, 20-29, 30-39, 40-49, 50-59, and over 60. This breakdown of age ranges is not representative of an equal population distribution which required the additional data source from the US Census. The US Census provides population data based on five-year age ranges beginning with under 5 all the way to 85 and above. This grouping of data allowed for multiple of these five-year age groups to be combined to match the age breakdown of the FBI Internet Crime Report. The combination of these allowed for more accurate analysis to take place.

The second categorization of data presented in the FBI Internet Crime Report was the type of cybercrime. In the most recent publication of the report, there was a breakdown of thirty categories outlining the types of cybercrime (FBI IC3, 2021). In order to amply focus on the most significant trends in the data, a subset of the entire dataset will be examined (Jahankhani et al., 2014). The subset to be analyzed can be identified as *sophisticated attacks*, this subset includes the FBI defined categories of hacktivism, ransomware, malware/scareware/virus, and denial of service/TDoS. To begin defining these categories, hacktivism is hacking for the purpose of furthering a social or political cause. Ransomware is a specific type of malicious software that traditionally encrypts a user's files and asks for a ransom payment to reclaim their files.

The category of malware/scareware/virus is a broader category that encompasses general types of malicious software that don't fall into the more specific categories of ransomware and

denial of service. The final category examined is denial of service/TDoS, which encompasses cybercrime with the intent of disrupting services of a victim, potentially causing lost revenue or other repercussions. The reasoning behind choosing these specific categories is due to the need for a more technically savvy criminal to use these attack vectors as opposed to a social engineering-based attack vector such as scamming or vishing (Jahankhani et al., 2014). The overall reasoning for making deliberate categorization choices was to provide a clear and accurate view of the specific trends observed in this research.

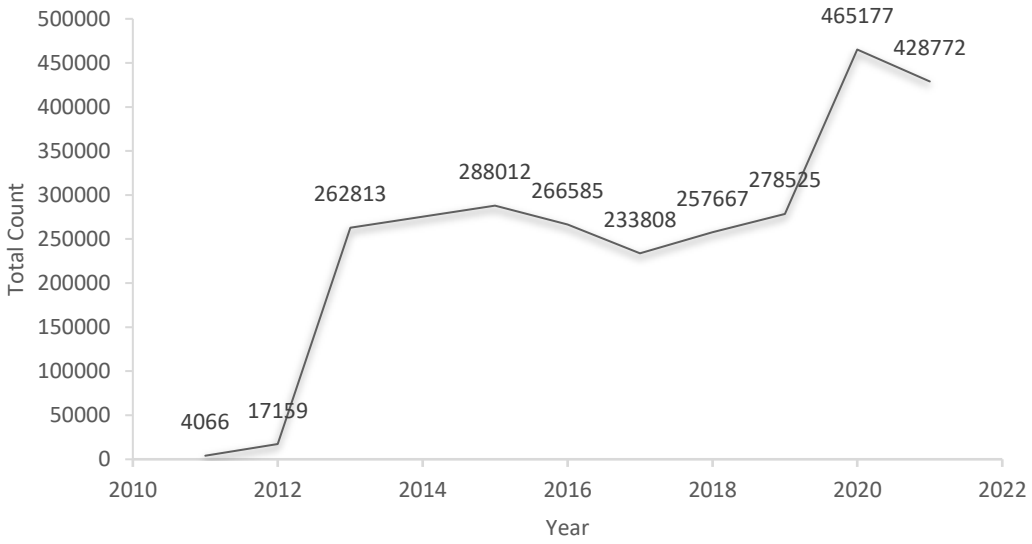
Analysis

Cybercrime Statistics Before, During, and After COVID-19

Before delving into the more granular statistics broken down by specific factors of cybercrime, gaining a total picture of cybercriminal trends is crucial. A clear and obvious trend can be seen from a simple glance at the data in Figure 1 and 2. There was a sudden increase in cybercrime during the 2019-2020 period, which coincides with the proposed date range for the events of COVID-19. There has been a steady upward trend through the specified years regarding the number of cybercrimes and their related losses. However, there is a sharper increase from 2019-2020 in both losses and count that accelerates this trend. In contrast, during the years 2020-2021, there was a drop-off in the count of cybercrimes yet a still increasing amount of money lost to cybercrimes. There are some potential reasons for this trend; however, the most prominent is the sophistication and incorporation of cybercrime that some theorize took place during the period of COVID-19 (Alghamdi, 2020). This trend will be investigated when the types of cybercrimes are further scrutinized. This data can be analyzed when investigating the next set of data from the annual FBI Internet Crime Report paired with the US Census which

Figure 1

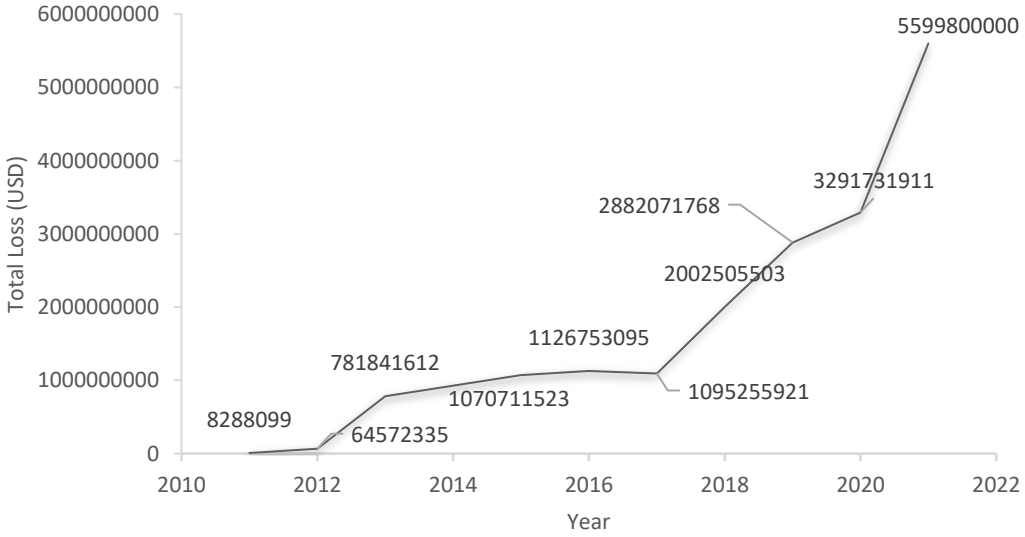
Total Number of Reported Cybercrimes



Note: The data for count comes from *FBI Internet Crime Report* by FBI IC3, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021

Figure 2

Money Lost to Cybercrime



Note: The data for losses comes from *FBI Internet Crime Report* by FBI IC3, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021

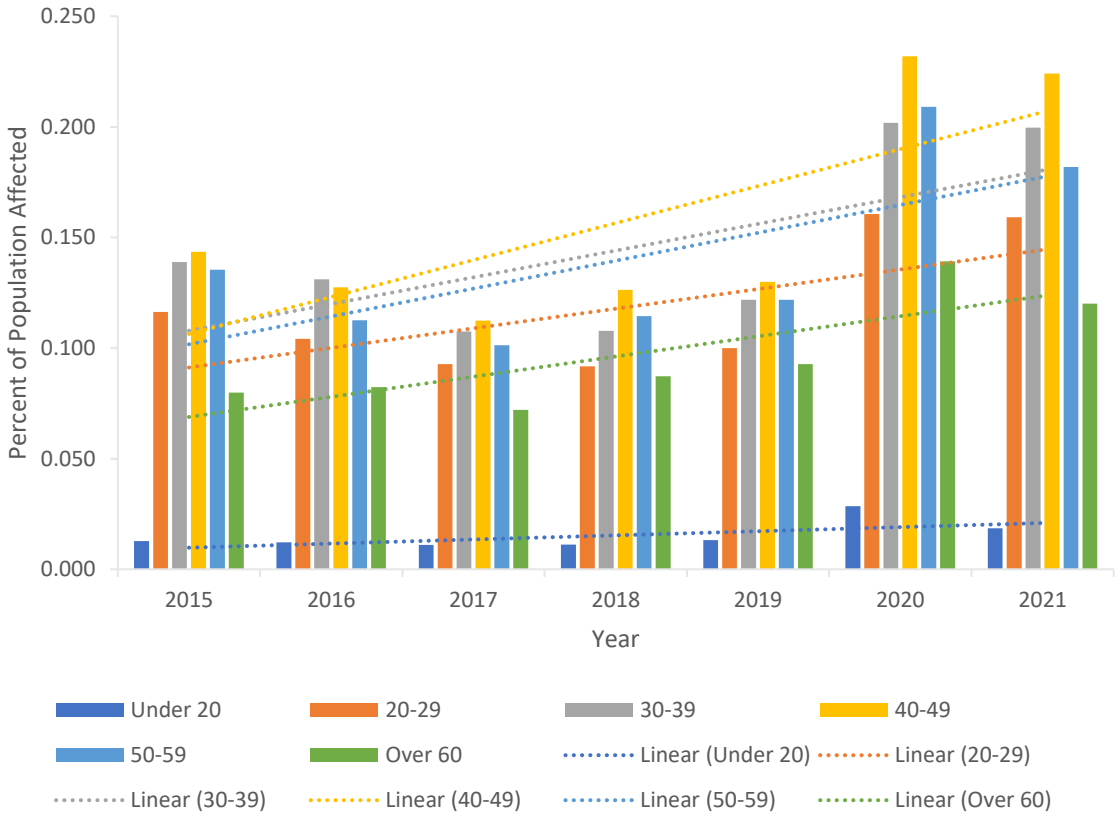
focuses on the age group breakdown of the victims of cybercrimes.

Breaking down the data by age group of the victim helps bring added clarity to the overall picture of cybercrime provided by the previous sets of data in Figure 1 and 2. The combination of the US Census data and the FBI Internet Crime report allows research to observe the trends while being unaffected by a skewing of the data a population misrepresentation can cause. The clear trend seen in Figures 3 and 4 follows the previously discussed movement where both cybercrime count and losses increased considerably from 2019 to 2020. In addition, the count decreased from 2020 to 2021 while the losses continued a sharp upward climb. Every age range even when adjusted for population size saw a decrease in the number of cybercrimes committed; conversely, all age strata saw an increase in losses. For example, the total losses sustained by the 20 to 29 age strata from 2019 to 2020, jumped from $4,477.66 to $9,884.44 and the age strata sustaining the most losses, 50 to 59, spiked from $20,626.82 to $30,765.47, a staggering 49% increase. In contrast, the percentage of population affected by cybercrime for the age range of over 60 decreased from .139% to .12% and the strata of 40 to 49 that was most affected declined from .232% to .224%. Although these are small percentage changes when regarding the entire population, this is a larger shift than first conceived. A holistic picture of the data must be presented which leaves the breakdown of the data based on the type of cybercrime to be analyzed.

The ability to track the overall trends allows for a high-level analysis of cybercrime trends in conjunction with providing a more granular look. Concentrating on Figures 5 and 6, a different trend is observed when compared with previously discussed data. Focusing on the designated cybercrime subtypes highlights a secondary trend, the rise of ransomware. In the

Figure 3

Percentage of Victim Age Group Population Affected by Cybercrime Count

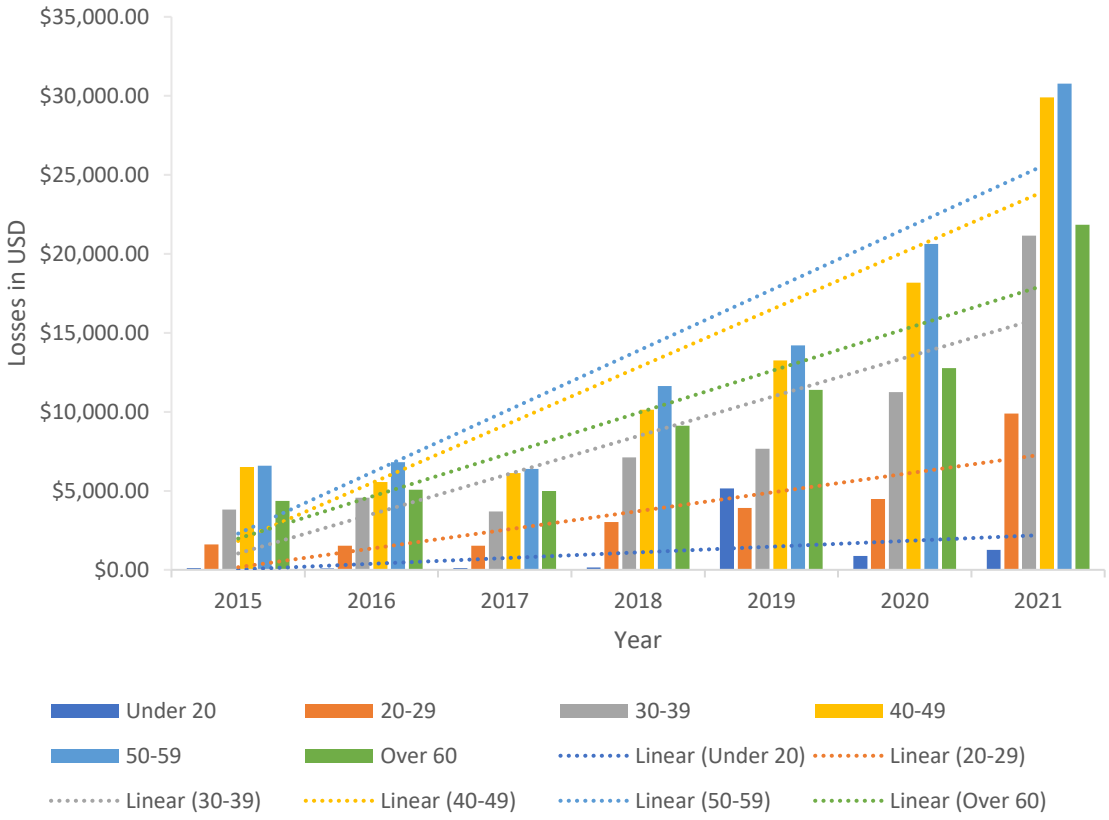


Note: The data for count comes from *FBI Internet Crime Report* by FBI IC3, 2015, 2016, 2017, 2018, 2019, 2020, 2021. The data for population comes from *Age and sex composition in the United States* by the US Census Bureau 2015, 2016, 2017, 2018, 2019, 2020, 2021. The count and population were used to determine the percent of population affected.

years of 2015 to 2018, the chosen subtypes declined in overall count and remained reasonably consistent regarding the losses inflicted. In the years of the pandemic, previously defined as 2019 to 2020, ransomware significantly increased in count and losses inflicted while the other three categories declined. Ransomware is malware that "is designed to disable the victim's computer or access to their data" (O'Kane et al., 2018, p. 1) usually through the use of encryption. The

Figure 4

Cybercrime Losses per Thousand People by Age Group



Note: The data for losses in USD comes from FBI Internet Crime Report 2015, 2016, 2017, 2018, 2019, 2020, 2021 by FBI IC3. The data for population comes from *Age and sex composition in the United States* by the US Census Bureau 2015, 2016, 2017, 2018, 2019, 2020, 2021. The losses in USD and population were used to determine the losses per thousand people by age group.

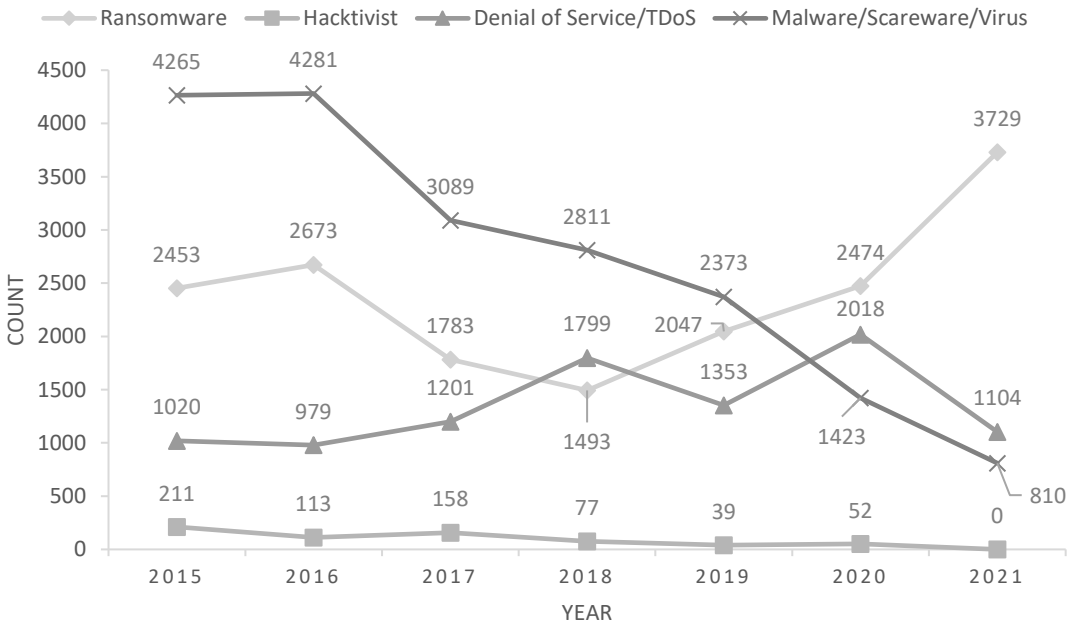
explosion of monetary loss caused by ransomware is seen most vividly in the comparison of the losses caused in 2018 and after the pandemic in 2021. In 2018, ransomware caused $8,965,847 in losses, and just three years later in 2021, it inflicted $49,207,908, a 448.8% increase. No other chosen categories increased from 2018 to 2021. The category of malware/scareware/virus inflicted the second highest amount of losses being reported as $5,596,889 in damages in 2021

compared to the previously reported as $7,411,651 in 2018. These numbers demonstrate a distinct movement in the data that cannot be denied.

The ability to execute a ransomware operation requires a higher understanding of encryption and other cybersecurity concepts and tradecrafts, therefore making it a more sophisticated attack path for cybercriminals. Even if the perpetrator is simply a script kiddie or one who executes complex scripts without understanding the inner workings, there has to be a point in the ransomware operation where someone understands and crafts the program. The rise in this form of cybercrime, beginning during the height of COVID-19 in 2019, suggests a pattern regarding the business of cybercrime (O'Kane et al., 2018).

Figure 5

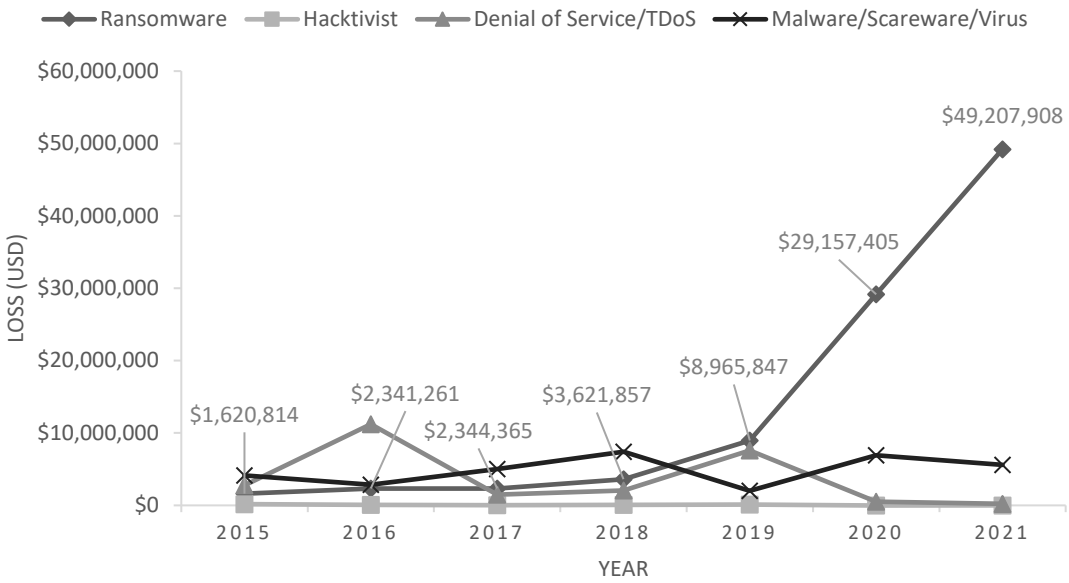
Cybercrime Counts by Subtypes



Note: The data for count comes from *FBI Internet Crime Report* by FBI IC3 2015, 2016, 2017, 2018, 2019, 2020, 2021

Figure 6

Cybercrime Loss by Subtypes



Note: The data for losses comes from *FBI Internet Crime Report* by FBI IC3 2015, 2016, 2017, 2018, 2019, 2020, 2021.

Implications

Potential Conclusions Drawn from FBI Crime Reports

Due to the wealth of data provided by the annual FBI Internet Crime Report, many trends can be observed; however, a proven conclusion may be harder to deduce. When dealing with statistical analysis, correlation does not always imply causation. Therefore, several possible conclusions taking their most informed hypothesis will be discussed. While these deductions only have the capacity to postulate reality as best as possible, one conclusion is undeniable based on the data: cybercrime accelerated and remains on a path to continue pace. As seen in Figure 2, cybercrime cost the world two billion dollars in 2018 before the pandemic, which was still a one billion dollar increase from three years prior in 2015 (FBI IC3, 2015, 2018). However, in 2021 it cost the world 5.5 billion dollars. The count of cybercrimes committed from 2019 to 2020 nearly doubled, highlighting this trend.

The potential factors that led to this surge during this period may be attributed to the fact that the average cybercriminals "were provided with a much richer landscape for exploitation" (Furnell & Shah, 2020, para. 21) along with the fact that "individuals were a more vulnerable and easily exploitable target" (Furnell & Shah, 2020, para. 22). COVID-19 provided a large attack surface for cybercriminals. In addition to the overall increase in cybercrime, a more specific, however equally concerning trend, was seen among the data: an increase in particular sophisticated attack vectors.

The trend of an overall increase in total money lost to cybercrime, yet a corresponding decrease and plateau in the amount of cybercrime seen during the pandemic, infers sophistication or more directed targeting. As previously discussed in the rise of ransomware, during the COVID-19 pandemic, widespread lockdowns occurred which forced criminals to spend more time in their homes. It is theorized that due to the longer period of lockdown than expected, cybercriminals honed their toolsets and tradecraft which resulted in an outward data trend, suggesting an increase in crime complexity (Ahmad, 2020). In addition to this, cybercrime operations that potentially relied on physical interaction had to be digitized, which opened up a criminal operation to the opportunity to reach a wider audience (Buil-Gil et al., 2020). This increase in reach can lead to the formalization of cybercriminal operations, where instead of a local scam operation, there is a nationwide ransomware broker. Although this relationship can only be theorized, there is at least backing for cybercriminals targeting larger and more profitable targets (Alghamdi, 2020). These trends must be further investigated because the incorporation of cybercrime could pose a grim reality where ransomware attacks are as common as scam calls.

Remediation for the Next Era of Cybersecurity

A firm foundation has been set for the discussion of remediation strategies moving forward from the pandemic to discuss security strategies for the future. Drawn from the conclusions of the previous section, the world has shifted from on-premises infrastructure to the cloud and from a primarily office-based setting to a work-from-home environment. This shift in business practices means that an equal shift in security must follow suit. In addition, even before COVID-19, an estimated "42% of endpoints are unprotected at any given time" (Ahmad, 2020, p. 1), and in the United Kingdom "46% of all UK businesses…experienced a breach or attack in [2019]" (Mandal & Khan, 2020, p. 2). These are staggering figures stressing the importance of working with security in mind, but tangibly how is that achievable?

A number of approaches need to be implemented in order to achieve a cybersecurity concept called defense-in-depth, where there is no single point of failure but rather redundancy and security controls past the first line of defense (Rahman et al., 2020). This concept recently became a buzzword in the cybersecurity community, but how does an organization achieve this golden standard of layered defense? The answer is simply by assuming a breach and taking steps to remediate at every level rather than only externally. Consequently, several general best practices, along with more specific and complex security implementations, will be examined to provide a standard for securing the future. In addition to these, future technologies that are being developed must be analyzed to determine how they can be leveraged from a cybersecurity perspective to aid in security efforts.

General Best Practices

To begin implementing defense-in-depth, a basis for security must be established, and in cybersecurity, that starts with best practices. The idea of best practices is a frequent motif in

cybersecurity discussions; however, they are rarely explicitly defined. This lack of definition can be due to the varying needs of organizations around the globe. For example, Apple does not have the same security needs as a local bakery. However, many security implementations are universally beneficial to organizations, small and large alike.

Password Policy. The first and potentially most unpopular is implementing a strong password policy (Eiza et al., 2021). For some time in the cybersecurity industry, password policy was a point of frustration for the average employee and IT manager. There was a recent shift in the ideology of password policy by many large corporations such as Microsoft. This change focuses on length, with the recommended minimum being 14 characters while not requiring "mandatory periodic password resets for user accounts" (Microsoft, 2022, para. 8). A strong password policy also limits the usage of common passwords along with requiring some level of complexity within the password (numbers, symbols, etc). With a password not able to be brute forced by a potential attacker, malicious actors are limited from taking advantage of this.

Multi-Factor Authentication (**MFA).** Continuing on the topic of general account security best practices, the enabling of MFA is another step toward organizational security. The overarching idea of MFA is that it requires a user to prove their identity using a variety of methods, not just one, such as a password. This can be achieved through the use of SMS, email, or a physical token acting as a secondary test proving the user asking for access is authenticated. Multi-factor authentication severely impedes an attacker's progress, as instead of intending to exploit a single point of failure, namely one password, the attacker must breach the secondary authentication method as well. The use of multi-factor authentication hinders any attacking force

and, according to the defense-in-depth methodology, helps develop a layered defensive strategy without any single points of failure (Rahman et al., 2020).

Patch Management. A commonly missed security measure that is among the most crucial is the management of software and system updates. Software vendors regularly push software patches that are released to fix certain vulnerabilities in the code that an attacker can potentially leverage (Dissanayake et al., 2021). If there are a rampant number of systems that are unpatched and running antiquated software, then that gives attackers yet another avenue for an easy means of unauthorized access (Dissanayake et al., 2021). Thus, a security team must take responsibility for managing the patching of systems and software on a corporate network. This task is made more difficult when a BYOD policy has been pushed due to COVID-19; however, this policy can be utilized to best protect organizations.

Employee Training. As the outer walls of an organization are secured through these general best practices, the people and practices must also be secured. The people of an organization are among the highest targets of any attacker to exploit via one of many avenues whether through kindness, compassion, or simply laziness (Borkovich & Skovira, 2020). In order to combat this, employees must be thoroughly trained on the importance of cybersecurity and what good cyber etiquette includes. Employees can be made to understand the why behind cybersecurity and what potential outcomes look like when best practices are neglected in favor of laziness (Vadlamudi & De, 2021). Phishing is a popular form of attack; therefore, training on how to properly identify phishing attempts and also how to properly elevate an incident through the proper channels can increase an organization’s security posture immensely.

Principle of Least Privileges. As the people of the organization are secured, the processes of the business must be secured as well. A baseline standard in cybersecurity is the principle of least privileges, which states that the only privileges given to any user should be the lowest level to get their jobs done (Eiza et al., 2021). An example of such an implementation is not giving access to the command terminal or PowerShell to the finance team or not allowing access to HR documents to anyone except those authorized on the HR team. This security implementation assumes a breach, which is a key aspect of defense-in-depth. The ability to assume the worst case and develop hurdles for the attackers to endure to achieve their goals is at the heart of this methodology. Therefore, providing each user with the least amount of privileges possible means that if an attacker gains access to a user account, then they have siloed privileges that limit the amount of lateral and horizontal pivoting they can achieve in a network. The danger of not implementing this methodology is allowing an attacker to gain access to one "low-level" employee with privilege misconfigurations, giving them an easy vector to escalate privileges and move vertically in the network. The implementation of these general security practices helps eliminate a number of easy wins that will deter a full breach in an organizational network.

Specialized Remediation Tactics

Virtual Private Networks. The need for more specialized and technical methods must be employed along with more developed tactics to proactively respond to the trends seen through COVID-19. One of the most prominent switches seen in COVID-19 is the work-from-home environment. The ability to work from home and still leverage resources on a corporate network is enabled by the use of a virtual private network (VPN). However, all VPNs are not the same (Eiza et al., 2021). In order to remain secure while using a VPN the level of encryption must be

to the recommended standard: 256-bit encryption. Along with the bit-length of the encryption used, the type of encryption used must be secure. Protocols such as point-to-point tunneling (PPTP) are an example of an insecure protocols whereas IKEv2 using AES is a very secure protocol (Abhijith & Senthilvadivu, 2020). If a VPN connection is not properly configured, then an attacker can have an easy foothold into a corporate network, usually requiring physical access. VPNs brought large benefits to organizations navigating the unknown waters of a work-from-home environment, but from a security perspective, moving forward managing and securing this technology is vital.

Data Exfiltration. Another added challenge faced by organizations during COVID-19 was the rampant exfiltration of data from the business environment into personal devices. This extraction of data opens up many legal ramifications, especially if that data involves customer or employee information. Therefore, security controls must be leveraged to prevent the misuse of this data, which comes in the form of data loss prevention (DLP). There are two primary forms of DLPs: network and endpoint. A network DLP "monitors and protects all data in use, in motion or at rest on the company's network" (Crowdstrike, 2022, para. 5) whereas an endpoint monitors the data on a variety of endpoints rather than in the network. The overall goal of a DLP is to leverage a variety of means (regular expressions, hash validation, etc.) to track classified documents and information and be able to prevent unauthorized movement of these resources. When there is a lack of in-office accountability, a DLP protects companies from negligent or lazy employees that attempt to exfiltrate information from the private network.

Security Information and Event Management. The ability to have an accurate real-time understanding of the state of one's network and where potential incidents are occurring is

invaluable to an organization. The primary technologies that allow these capabilities are security information and event management (SIEM) and security orchestration, automation, and response (SOAR) technologies. SIEM and SOAR technologies centralize the vast amount of information a network makes available to a security team. The key difference is an alteration in the use of automation which a SOAR utilizes, whereas a SIEM does not and focuses on log correlation and centralization (Bridges et al., 2022). Both SOARs and SIEMs, when properly configured, alleviate a considerable amount of the security workload from a security team. Though this is the case, during COVID-19 and immediately following, the amount of manpower and expendable budget for the average business fell (Borkovich & Skovira, 2020). The ability to lean on the automation of a SOAR is advantageous for smaller or tight-budgeted organizations (Bridges et al., 2022). The implementation of these capabilities adds another layer to the defense in depth model, where attackers must now tread carefully on an internal network in order to avoid SIEM alerts that if properly configured will severely limit them by reporting actions through proper channels.

Intrusion Detection/Prevention System. In addition to SIEM and SOAR resources, the use of intrusion detection and prevention systems (IDS/IPS) are crucial for limiting the activity an intruder can do toward an organization. The proper configuration of these technologies will result in yet another layer added to the defenses of an organization following the defense-in-depth methodology. The overall goal of using an IDS is “detecting malicious behavior that can compromise the security and trust of a network” (Pranggono & Abdullahi, 2020, p. 5) and setting up proper alerts for the security team so they can properly diagnose and remediate the alert. The key difference in goal for an IPS is that detection turns into prevention and alerts turn into steps

of remediation. An IPS, when properly configured, is more advantageous to set up for an organization; however, an IDS still can provide an organization a valuable asset in the journey towards layered defense (Rahman et al., 2020).

Cloud Access Security Broker. Pivoting towards the protection of cloud computing resources due to the rise in usage that COVID-19 provided, employing the use of a cloud access security broker (CASB) is an important step toward security. Overall, a CASB aims to "ensure the security of data and also the workability of the services of clouds" (Ahmad et al., 2021, p. 1) and give security professionals visibility into their cloud environment. With the previously discussed rush towards cloud solutions, adhering to the shared responsibility model most providers use is central to security. The added functionality a CASB provides is a platform to protect one's data while in the cloud and in transit from the cloud (Ahmad et al., 2021). The implementation of all of these more specific and technical resources in any corporate environment does not guarantee the lack of a breach; however, the security posture increases and the chance of an attack going undetected and unremedied decreases.

Implementation of Future Technology and Concepts

Zero Trust. The future of cybersecurity is dependent on a proactive mindset, but where does that leave the current security community? Two themes have already been distinguished as focal points that will determine the security of the future: artificial intelligence/machine learning (AI/ML) and zero trust (Rose et al., 2020). Starting with the concept of zero trust, the idea that encapsulates this concept is assuming "there is no implicit trust granted to assets or user accounts based solely on their physical or network location…or based on asset ownership" (Rose et al., 2020, p. 7). The overall focus of implementing this methodology is "protecting resources…not

network segments" (Rose et al., 2020, p. 5) which is a keen switch from the modern methodology. The current status of zero trust is that a shift has begun in large corporations and government entities to this model; however, this strategy remains largely unused at this current juncture. For that reason, the aim of the current cybersecurity community should be to make the leap from the current environment to a zero-trust model in the majority of their environments. This change strengthens the overall security posture of small and large organizations alike and also provides a standard of security across all sectors of business.

AI/ML. Transitioning from zero-trust methodology to the expanding field of AI/ML, will launch the cybersecurity field into the era past the post-COVID age. AI/ML solutions are already being leveraged mostly in the field of data science. They have started being used in security; however, the applications for this level of technology are expansive in the realm of cybersecurity. Possible applications are operating AI/ML capabilities in unison with a SIEM and automatically detecting and applying remediations to dynamic threats that may arise. The determination of future security will be based on how the globe adapts and incorporates waves of new technologies. The opposition is keen to gain an edge through new means, and, thus, the defense should follow suit.

Limitations of Study

In order to confidently draw conclusions from this analysis, potential blind spots need to determined. The first limitation of this study is the lack of secondary authoritative sources due to the FBI and US Census Bureau being the primary authority on the statistics compiled. There are a number of secondary sources that support conclusions drawn, yet no other entity publicly records this information. In addition to this constraint, the FBI IC3 notes in their report "some

complainants may have filed more than once" (FBI IC3, 2021, p. 33). Paired with this, the research done only covers the numbers of cybercrime where a complaint was filed which may not be the complete picture. In spite of these limitations, there is still strong support for the conclusions drawn due to the vast amount of data analyzed that spanned multiple years with consistent strata. Regarding future research, these limitations must be considered and addressed to provide more definite conclusions on the state of cybercrime.

Future Research

Future Outlook of Cybercrime

When a trend in data can be determined, then proper remediation or counterbalance can be applied. However, purely reactive security will pave the way for an increasingly insecure future. Therefore, in order to shift from reactive to proactive security, the cybersecurity industry must understand the previous trends in cybercrime and be able to utilize that knowledge to deduce the impending evolutions of security. Therefore, a proposed area of further research is to compare the number of cybercrime victims who utilize a proactive versus a reactive approach. There is an increasing need to focus efforts to critical sectors so the push from reactive to proactive could help limit the loss caused by cybercrime annually.

The constraining factors for this push towards proactive security are time and resources. Consequently, the need to properly perceive the ebbs and flows of the cybercrime world is paramount. When the trends can be predicted with general accuracy, then the resulting reality is one where limited time and resources are allocated to the most vital sectors. As seen in this research, specific forms of cybercrime such as ransomware are on the rise. Research focused on

the effectiveness of specific security controls targeting distinct attack paths would provide a beneficial resource to organizations looking to increase their security posture.

The future of the technology industry as a whole is artificial intelligence and machine learning (AI/ML). The ability to harness technologies already being used for big-data analysis would propel the current cybercrime remediation landscape well into a more proactive stance. Additionally, AI/ML, "must be included in threat detection and response capabilities" (Baz et al., 2021, p. 10) to maintain a strong security posture. However, further research into new remediation tactics to keep pace with the ever-evolving industry is another area of vast benefit for the cybersecurity community as a whole.

Balance between Security Fatigue and Secure Working

Security solutions and technologies can be implemented day in and day out; however, at the heart of security are the people and processes of an organization. Security fatigue is the concept of security becoming exhausting to the average employee, causing the employee to resent security policies, eventually leading to the undermining of those very policies (Furnell et al., 2021). A crucial discussion can take place in every organization to determine where the balance between secure working and security fatigue lies.

Consistency and consciousness have been identified as points of focus for security teams creating policy (Furnell et al., 2021). The notion of consistency in security policy implementation means not changing security advisement frequently because a "change of guidance causes some people to question the validity of the advice and the credibility of the source" (Furnell et al., 2021, p. 3). This has been compared with the changing of guidance that people experienced during COVID-19, which saw this exact outcome of questioning of

credibility. Paired with consistency, consciousness captures the idea that the security team must be aware of the impact of their policies. An over-burdened employee very easily becomes apathetic toward security in general, which can be dangerous for any organization. On the other side, a security team that finds ways to unburden employees, yet still increases the overall security posture, will foster a security-positive environment. Therefore, a concerted effort to research the prevalence of security fatigue related incidents pre- and post-COVID would prove beneficial. Future research into this area can help determine the relevance of security fatigue and how much of a role it played in the findings of this research. At the very least, a discussion across the cybersecurity community as a whole needs to take place to combat growing security fatigue in the workplace.

Conclusion

The COVID-19 pandemic ravaged the known world in a variety of areas; however, one overlooked area has been the cybersecurity industry. Crime statistics show a clear uptick in the amount of crime, along with the total losses experienced by cybercrime, with no signs of slowing down. Along with these trends, more advanced trends such as the incorporation and sophistication of cybercrime, are clearly seen in rapid increases in ransomware along with other more specific and targeted types of crime. Moving away from a statistical approach, the threat landscape drastically shifted when a primarily office-bound workforce transitioned to a remote workspace. This shift created a large number of security threats, and the speed at which this took place increased the number of vulnerabilities that opened up. A clear transition to cloud infrastructure was seen as a result of COVID-19 as well, which further disrupted the previous cyber threat landscape.

In spite of this reshaping, the general best practices remain for organizations striving for security. Focusing on implementing a layered approach is among the most effective methodologies to follow, especially in the new territory known as the post-COVID landscape. The golden triad of people, processes, and technology is at the center of modern security. Properly training employees on how to engage securely with their various jobs and focusing on the *why* can aid in the overall security posture of any organization. Security policies and processes simply focusing on this layered approach and securing the easily exploitable vulnerabilities such as patch mismanagement, weak password policies, or a lack of MFA can launch an organization into a higher echelon of security maturity. Implementing secure technologies and devices on a network such as a DLP, SIEM/SOAR, or IDS/IPS can significantly limit an attacker's ability to compromise a network. Future technologies and methodologies must also be proactively implemented to keep pace with this ever-evolving field of security. Organizations that simply keep up with the ever-changing landscape may be far more vulnerable than ones who set the trend; therefore, continually aiming to set the pace of cybersecurity is the key to a strong security posture

References

Abhijith, M., & Senthilvadivu, K. (2020). Impact of VPN technology on IT industry during COVID-19 pandemic. *International Journal of Engineering Applied Sciences and Technology*, *5*(5), 152–157. https://doi.org/10.33564/ijeast.2020.v05i05.027

Ahmad, S., Mehfuz, S., & Beg, J. (2021). Enhancing security of cloud platform with cloud access security broker. *Information and Communication Technology for Competitive Strategies (ICTCS 2020)*, 325–335. https://doi.org/10.1007/978-981-16-0882-7_27

Ahmad, T. (2020, April 6). *Corona virus (COVID-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity*. SSRN. Retrieved March 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3568830

Alashhab, Z. R., Anbar, M., Singh, M. M., Leau, Y.-B., Al-Sai, Z. A., & Abu Alhayja'a, S. (2021). Impact of coronavirus pandemic crisis on technologies and cloud computing applications. *Journal of Electronic Science and Technology*, *19*(1), 100059. https://doi.org/10.1016/j.jnlest.2020.100059

Alghamdi, M. I. (2020). A descriptive study on the impact of cybercrime and possible measures to curtail its spread worldwide. *International Journal of Engineering Research & Technology (IJERT)*, *9*(6). https://www.ijert.org/a-descriptive-study-on-the-impact-of-cybercrime-and-possible-measures-to-curtail-its-spread-worldwide

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: Threats and mitigation strategies. *IEEE Access*, *9*, 57792–57807. https://doi.org/10.1109/access.2021.3073203

Anderson, R., Barton, C., Böhme, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2013). Measuring the Cost of Cybercrime. In: Böhme, R. (eds) *The economics of information security and privacy*. Springer. https://doi.org/10.1007/978-3-642-39498-0_12

Baz, M., Alhakami, H., Agrawal, A., Baz, A., & Khan, R. A. (2021). *Impact of COVID-19 pandemic: A cybersecurity perspective*. Intelligent Automation and Soft Computing. Retrieved March 25, 2022, from https://pesquisa.bvsalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/pt/COVIDwho-1155091

Borkovich, D. J., & Skovira, R. J. (2020, September). *Working from home: Cybersecurity in the age of COVID-19*. ResearchGate. Retrieved January 24, 2023, from https://www.researchgate.net/profile/Debra-Borkovich/publication/354694505_Working_From_Home_Cybersecurity_in_the_Age_of_COVID-19/links/614819b43c6cb310697e0f54/Working-From-Home-Cybersecurity-in-the-Age-of-COVID-19.pdf?origin=publication_detail

Bridges, R. A., Rice, A. E., Oesch, S., Nichols, J. A., Watson, C., Spakes, K., Norem, S., Huettel, M., Jewell, B., Weber, B., Gannon, C., Bizovi, O., Hollifield, S. C., & Erwin, S. (2022, August 12). *Testing soar tools in use*. arXiv.org. Retrieved January 24, 2023, from https://arxiv.org/abs/2208.06075

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020, August 11). *Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK*. Taylor & Francis. Retrieved March 25, 2022, from https://www.tandfonline.com/doi/full/10.1080/14616696.2020.1804973

Crowdstrike. (2022, September 27). *What is data loss prevention (DLP)? [beginners guide]: Crowdstrike*. crowdstrike.com. Retrieved January 6, 2023, from https://www.crowdstrike.com/cybersecurity-101/data-loss-prevention-dlp/

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2021, December 2). Software security patch management - *A systematic literature review of challenges, approaches, tools and practices*. Retrieved February 14, 2023, from https://www.sciencedirect.com/science/article/pii/S0950584921002147

Eiza, M., Okeke, R., Dempsey, J., & Ta, V. (2021, January). *Keep calm and carry on with cybersecurity @home: A framework for securing homeworking IT environment*. Researchgate., from https://www.researchgate.net/profile/Max-Eiza/publication/348553003_Keep_Calm_and_Carry_on_with_Cybersecurity_Home_A_Framework_for_Securing_Homeworking_IT_Environment/links/617d3e57eef53e51e1090232/Keep-Calm-and-Carry-on-with-Cybersecurity-Home-A-Framework-for-Securing-Homeworking-IT-Environment.pdf

FBI IC3. (2016, May 3). *Cyber crime*. FBI. Retrieved December 28, 2022, from https://www.fbi.gov/investigate/cyber

FBI IC3. (2011). *FBI Internet Crime Report*. FBI. Retrieved December 28, 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2011_IC3Report.pdf

FBI IC3. (2012). *FBI Internet Crime Report*. FBI. Retrieved December 28, 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2012_IC3Report.pdf

FBI IC3. (2013). *FBI Internet Crime Report*. FBI. Retrieved December 28, 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2013_IC3Report.pdf

FBI IC3. (2014). *FBI Internet Crime Report*. FBI. Retrieved December 28, 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2014_IC3Report.pdf

FBI IC3. (2015). *FBI Internet Crime Report*. FBI. Retrieved December 28, 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2015_IC3Report.pdf

FBI IC3. (2016). *FBI Internet Crime Report*. FBI. Retrieved December 28, 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2016_IC3Report.pdf

FBI IC3. (2017). *FBI Internet Crime Report 2017*. FBI. Retrieved December 28, 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2017_IC3Report.pdf

FBI IC3. (2018). *FBI Internet Crime Report 2018*. FBI. Retrieved December 28, 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2018_IC3Report.pdf

FBI IC3. (2019). *FBI Internet Crime Report 2019*. FBI. Retrieved December 28, 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf

FBI IC3. (2020). *FBI Internet Crime Report 2020*. FBI. Retrieved December 28, 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

FBI IC3. (2021). *FBI Internet Crime Report 2021*. FBI. Retrieved December 28, 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Furnell, S., & Shah, J. N. (2020, August 18). *Home working and cyber security – an outbreak of unpreparedness?* Computer Fraud & Security. Retrieved March 2022, from https://www.sciencedirect.com/science/article/pii/S1361372320300841

Furnell, S., Haney, J., & Theofanos, M. (2021, March). *Pandemic parallels: What can cybersecurity learn from COVID-19?* Computer. Retrieved March 25, 2022, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8356203/

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014, July 25). *Cybercrime classification and characteristics*. Cyber Crime and Cyber Terrorism Investigator's Handbook. Retrieved February 10, 2023, from https://www.sciencedirect.com/science/article/pii/B9780128007433000128

Machado, T. J., & Gouveia, L. B. (2021). COVID-19 effects on cybersecurity issues. *International Journal of Advanced Engineering Research and Science, 8(8)*, 222–229. https://doi.org/10.22161/ijaers.88.27

Mandal, S., & Khan, D. A. (2020, September). *A study of security threats in cloud: Passive impact of COVID-19 pandemic*. IEEE Xplore. Retrieved March 25, 2022, from https://ieeexplore.ieee.org/abstract/document/9215374

Microsoft. (2022). *Password policy recommendations - Microsoft 365 admin*. Password policy recommendations - Microsoft 365 admin | Microsoft Learn. Retrieved January 4, 2023, from https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *IET Networks*, *7*(5), 321–327.

Pranggono, B., & Abdullahi, A. (2020, October). *COVID-19 pandemic cybersecurity issues*. Wiley Online Library. Retrieved March 2022, from https://onlinelibrary.wiley.com/doi/full/10.1002/itl2.247

Rahman, M. T., Rahman, M. S., Wang, H., Tajik, S., Khalil, W., Farahmandi, F., Forte, D., Asadizanjani, N., & Tehranipoor, M. (2020). Defense-in-depth: A recipe for logic locking to prevail. *Integration*, *72*, 39–57. https://doi.org/10.1016/j.vlsi.2019.12.007

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. *NIST Special Publication 800-207*. https://doi.org/10.6028/nist.sp.800-207-draft2

US Census Bureau. (2021, December 16). *Age and sex composition in the United States: 2011*. Census.gov. Retrieved February 8, 2023, from

https://www.census.gov/data/tables/2011/demo/age-and-sex/2011-age-sex-composition.html

US Census Bureau. (2021, December 16). *Age and sex composition in the United States: 2012*. Census.gov. Retrieved February 8, 2023, from https://www.census.gov/data/tables/2012/demo/age-and-sex/2012-age-sex-composition.html

US Census Bureau. (2021, December 16). *Age and sex composition in the United States: 2013*. Census.gov. Retrieved February 8, 2023, from https://www.census.gov/data/tables/2013/demo/age-and-sex/2013-age-sex-composition.html

US Census Bureau. (2021, December 16). *Age and sex composition in the United States: 2014*. Census.gov. Retrieved February 8, 2023, from https://www.census.gov/data/tables/2014/demo/age-and-sex/2014-age-sex-composition.html

US Census Bureau. (2021, December 16). *Age and sex composition in the United States: 2015*. Census.gov. Retrieved February 8, 2023, from https://www.census.gov/data/tables/2015/demo/age-and-sex/2015-age-sex-composition.html

US Census Bureau. (2021, December 16). *Age and sex composition in the United States: 2016*. Census.gov. Retrieved February 8, 2023, from

https://www.census.gov/data/tables/2016/demo/age-and-sex/2016-age-sex-composition.html

US Census Bureau. (2021, December 16). *Age and sex composition in the United States: 2017*. Census.gov. Retrieved February 8, 2023, from https://www.census.gov/data/tables/2017/demo/age-and-sex/2017-age-sex-composition.html

US Census Bureau. (2021, December 16). *Age and sex composition in the United States: 2018*. Census.gov. Retrieved February 8, 2023, from https://www.census.gov/data/tables/2018/demo/age-and-sex/2018-age-sex-composition.html

US Census Bureau. (2021, December 16). *Age and sex composition in the United States: 2019.* Census.gov. Retrieved February 8, 2023, from https://www.census.gov/data/tables/2019/demo/age-and-sex/2019-age-sex-composition.html

US Census Bureau. (2021, December 16). *Age and sex composition in the United States: 2020*. Census.gov. Retrieved February 8, 2023, from https://www.census.gov/data/tables/2020/demo/age-and-sex/2020-age-sex-composition.html

US Census Bureau. (2021, December 16). *Age and sex composition in the United States: 2021*. Census.gov. Retrieved February 8, 2023, from

https://www.census.gov/data/tables/2021/demo/age-and-sex/2021-age-sex-composition.html

Vadlamudi, S., & De, S. (2021, June). *A novel approach in cyber security for securing the workplace of the future in large industry setups*. IEEE Xplore. Retrieved March 2022, from https://ieeexplore.ieee.org/abstract/document/9498468