Spring 2021

The Evolution of Cyber Risk and the Cyber Insurance Market

Abigail Chase
University of South Carolina - Columbia

Director of Thesis: Robert Hartwig

Second Reader: Gregory Niehaus

Table of Contents

THESIS SUMMARY

Insurance and hedging instruments can help corporations manage many of the operational and financial risks they face. Yet, additional complexities are introduced now that many risks are increasingly interdependent and thus strongly correlated, making them more challenging to manage. Few risks illustrate this challenge better than cyber risk.

This thesis will focus on the increasing attention that the management of cyber risks receives in corporations, institutions and industries, and the role that insurance and risk management strategies play in mitigating this risk. The decision to focus on cyber risks—and the financing and management of those risks—is directly related to the exponential increase in cyber threats throughout the global economy. Thirty years ago, few would have predicted the magnitude of damage that cyber-attacks would routinely inflict upon organizations of all sizes—with the potential for far more severe losses looming ever larger. The rapid evolution and escalation of cyber threats—along with their ubiquitous nature—has led to a comprehensive reassessment of how organizations manage risks of all types. Insurers have been meeting the changing risk management needs of these organizations through innovations in product design, which now commonly include elements of loss control and post-event mitigation—in addition to traditional loss financing.

This thesis begins with a historical review of cyber threats and proceeds to examine the varied nature of cyber threats impacting several key industries. Data on major attacks for each industry examined in this thesis were researched, collected and analyzed, and are displayed in the database included in the appendix to this paper. For the discussion of early-stage cyber threats, I will trace the evolution of cyber threats from relatively simplistic denial-of-service attacks, to early computer viruses, to phishing emails, and to the multiplicity of sophisticated threats seen

today, such as ransomware. The objective is to provide those who are unfamiliar with cyber risk (i.e., students or other professionals) with an increased awareness of the threats, as well as an understanding of how organizations can mitigate such threats.

INTRODUCTION

Cyber-attacks can have long lasting impacts for organizations and companies. The financial consequences are potentially substantial—both in terms of direct costs to manage the consequences of the attack as well as a company's share price. Cyber-attacks can also negatively impact a company's reputation with the public and customers. In the case of healthcare, for example, individuals want assurance that their personal and private information is protected; any actual or perceived cyber threat against a healthcare institution will jeopardize the presumption of privacy and may lead clients to seek healthcare elsewhere.

Vulnerability to cyber risks is increasing exponentially. Digitization and interconnectedness are proceeding at a pace that is faster than what can be realistically managed. The rapid progression and evolution of cyber risks are central themes of this thesis. Specifically, I will analyze past examples of cyber-attacks for trends in each of three significantly impacted industries: healthcare, transportation, and electoral systems. The research will examine vulnerabilities among organizations affected by these attacks. Cyber risk management protocols in place at the time of the attacks will be assessed to ascertain the degree and nature of vulnerabilities. Opportunities for enhancing cyber risk management will also be identified.

HISTORY OF CYBERSECURITY AND CYBER RISK

The rapid evolution, spread, and dependence on digital technologies over the past 25 years has resulted in an exponential increase in cyber risk. Management of cyber risks is now a C-suite and board level issue, with an increasingly sophisticated portfolio of cyber insurance products playing a key role in managing that risk. Cyber insurance has been available since the late 1970s, though few organizations took advantage of it. “Following Y2K, the dotcom crash and the 9/11 attacks, interest in cyber insurance grew. There was a growing realization that the virtual world did not necessarily fit within the scope of many traditional covers/classes of insurance” [1].

How Y2K Changed Cyber Risk

In the late 1990s, Y2K and the dotcom boom were the primary drivers of increasing awareness of cyber risk and the dangers of interconnectivity of networks. In the article, “The Y2K Problem: Social Chaos or Social Transformation?”, explicit fear was expressed by the author, John L. Peterson, a futurist specializing in long-range security implications of a rapidly changing world. Writing in 1998, Peterson’s article examines societal apprehensions near the turn of the millennium. Peterson describes the panic that ensued in the population over the perception that the year 2000 might cause chaos for computer systems, despite the seemingly innocuous root of the problem. Since the dawn of the computer age in the mid-twentieth century and for decades thereafter, computer algorithms created by software engineers utilized a two-digit (rather than four digit) date format (i.e., 1960 was denoted as “60”), and many feared the systems would not have the ability to properly interpret the year 2000 [2]. Peterson further asserted at the time that “the year 2000 computer problem could create chaos on an order of magnitude we have never seen. Without a spirit of cooperation, we may all suffer” [3].

The turn of the millennium was an important time in history, because while cyber risks were clearly in existence prior to Y2K, mounting concerns over Y2K beginning in the late 1990s represent a reasonable historical starting point for the analysis of cyber risks. This is because the Y2K period was when this risk first became universally recognized as a societal and economic threat. It is also important to point out that there was increasing recognition that the world had become interdependent on technology. “It is that interconnectedness that threatens us if we do not match it with the deeper interconnectedness of human beings and communities” [3]. The interconnectivity of systems created a terrifying scenario, because no single system could protect itself. In the past, many companies operated their own proprietary networks; if one company was hacked, then that became an isolated issue which needed to be resolved. Y2K revealed that cyber risks are a systemic risk, potentially leading to cascading failures capable of crippling basic infrastructure and threatening the economy in general.

The Interconnectivity of Systems

Today, most companies are connected—directly or indirectly— to their suppliers, vendors, customers, and many other entities and organizations—including some with poor cyber risk management protocols or worse, actual malicious intent. Connectivity brings convenience to users, but with that convenience comes an elevated risk. This interconnectivity—frequently referred to as the “Internet of Things” or IoT—has led to risk management issues so large that it has become increasingly necessary and prudent for companies to purchase a separate cyber insurance policy to cover the losses that can arise [4].

The Rise of Cyber Insurance

Early cyber insurance policies began to gain traction with businesses as a stand-alone product in response to Y2K concerns. Such insurance was needed to fill gaps in traditional property and casualty products [1]. Cyber insurance generally covers business’ liability for data breaches involving sensitive customer information, such as credit card numbers, social security numbers, and health records. Cyber insurance also helps with repairing damaged computer systems, recovering compromised data, and notifying clients of the data breach [5]. Privacy regulation in the U.S. in the early 2000s served as an additional catalyst fueling increased demand for cyber insurance. Increasingly frequent mass data breaches—coupled with greater media attention and public concern to the issue resulted in pressure for regulation. A flurry of legislative actions ensued. California was at the vanguard of this regulatory movement with the passage of one of the nation's first breach notification laws, which became effective on July 1, 2003. "Other states followed, mandating that companies had to immediately disclose a breach to customers, usually in writing in addition to the regulatory authorities" [1]. Cyber insurance products shifted in response to these new notification requirements toward compensating the costs associated with major data breaches, including the costs of notifying customers and regulators. The market quickly gained momentum in the U.S. as notification rules expanded across multiple sectors and states. As major breaches began to make headlines with ever increasing frequency, the demand for cyber insurance grew and the market took off [1]. And as cyber-attacks become more damaging, institutions were searching for cyber coverage to protect themselves from these risks.

The increase in frequency and severity of cyber-attacks underscores the important role of insurance in managing and mitigating risks. High-profile cases, such as the 2013 Target data breach, 2017 Equifax data breach, and the leak of Democratic National Committee emails during the 2016 election made national headlines [6]. Indeed, organizations across all industries are extremely likely to be the victim of a cyber-attack. Willis Towers Watson, one of the world's largest insurance brokers, in its 2019 Cyber Security Breaches Survey 2 reported that over 32% of businesses experienced a cyber-attack within the past year [7]. Cyber insurance can help companies by providing teams with expertise in responding to cyber incidents. According to Willis Towers Watson, cyber insurance can also help foster a dialogue within an organization:

"The application, underwriting, and renewal process can help open up needed conversation among an organization's key leaders about how to best mitigate cyber vulnerabilities. This process — which involves questions, advice, and input from a company's broker and underwriter(s) — quickly highlights critical cyber gaps" [8]. Once these gaps are identified, they can be analyzed for companies to make investments in cybersecurity that can help to prevent the potential loss.

The Cyber Insurance Solution

One of the major issues with cybersecurity is the lack of awareness. Many senior corporate executives are unaware of the risk and the extent of potential business impacts and legal exposure cyber-attacks produce. "Recent publications by the U.S. Department of Homeland Security and several industry entities report significant increases in the number of cyber-attacks against industrial control systems. The sophistication of attacks is also increasing as is the likelihood that they will be physically destructive and cause significant loss" [9]. It is crucial that organizations of all sizes act proactively and create a cyber-risk plan, rather than waiting until after an attack. In addition to the lack of awareness, many institutions are not taking advantage of cyber insurance offerings. Looking at the cyber insurance take-up rates for Marsh clients in Figure 1, it is apparent that there are gaps in the cyber insurance market, with the overall take-up rate for 2019 being only 42% [10]. The take-up rate is the percentage of all Marsh clients that purchased the coverage. Although fewer than half of Marsh clients purchased cyber insurance in 2019, trends in recent years suggest organizations have a heightened appreciation of the risk. From 2017 to 2019, across all industries the take-up rate increased by 11 percentage points from 31% to 42%. Notably, the take-up rate is more than twice the 19% recorded in 2014.

Take-up rates vary substantially across industries (see Figure 2 [10]). Note that Education was the leading buyer of cyber insurance in 2019 with a 74% take-up rate. Healthcare was a close second with a 65% take-up rate. The strong demand for coverage is a reflection of the significant exposure to loss of personally identifiable information (PPI) and protected health information (PHI) across the educational and healthcare sectors.

The average cost of a data breach varies per industry, with healthcare being the leader. Figure 3 [11] displays the average total cost of a data breach by industry. The 2019 study was conducted by the Ponemon Institute and the results were analyzed by IBM Security. The results are based on a sample of 507 companies [11]. Again, in this study, healthcare was the leading industry at an average per data breach being $6.45 million. Health, financial, and energy companies are subject to more stringent regulation than industries such as media, hospitality, and retail. The increased regulations make these industries more susceptible to higher costs per breach.

Figure 1: US Cyber Insurance Take-up Rates (Marsh Clients) [10]

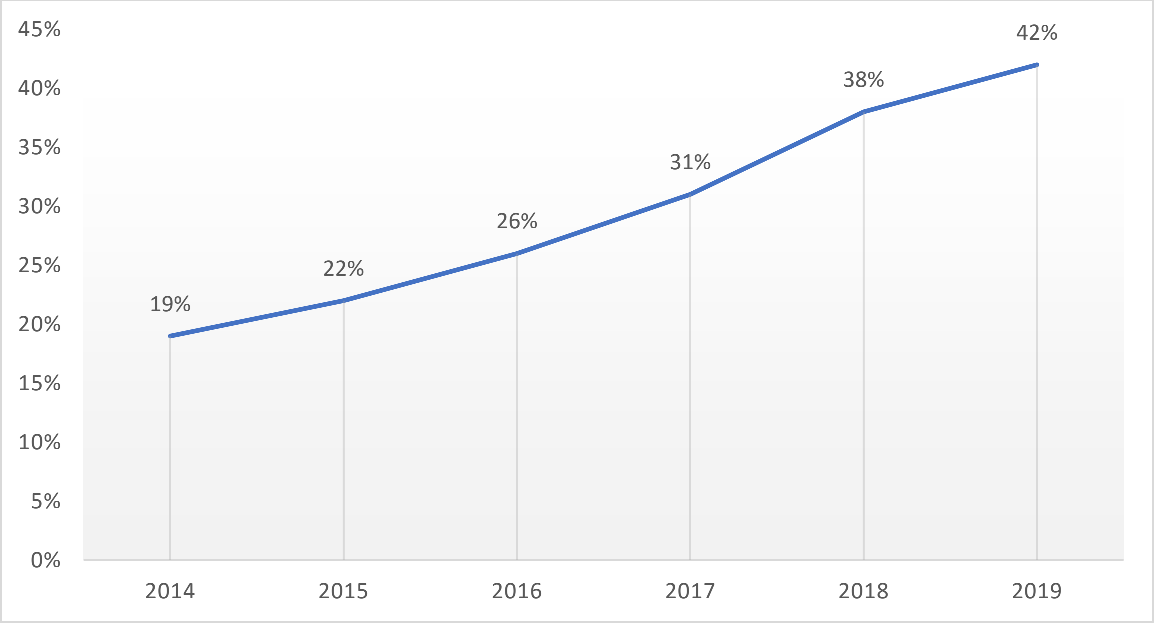


Figure 2: US Cyber Insurance Take-up Rates by Industry [10]

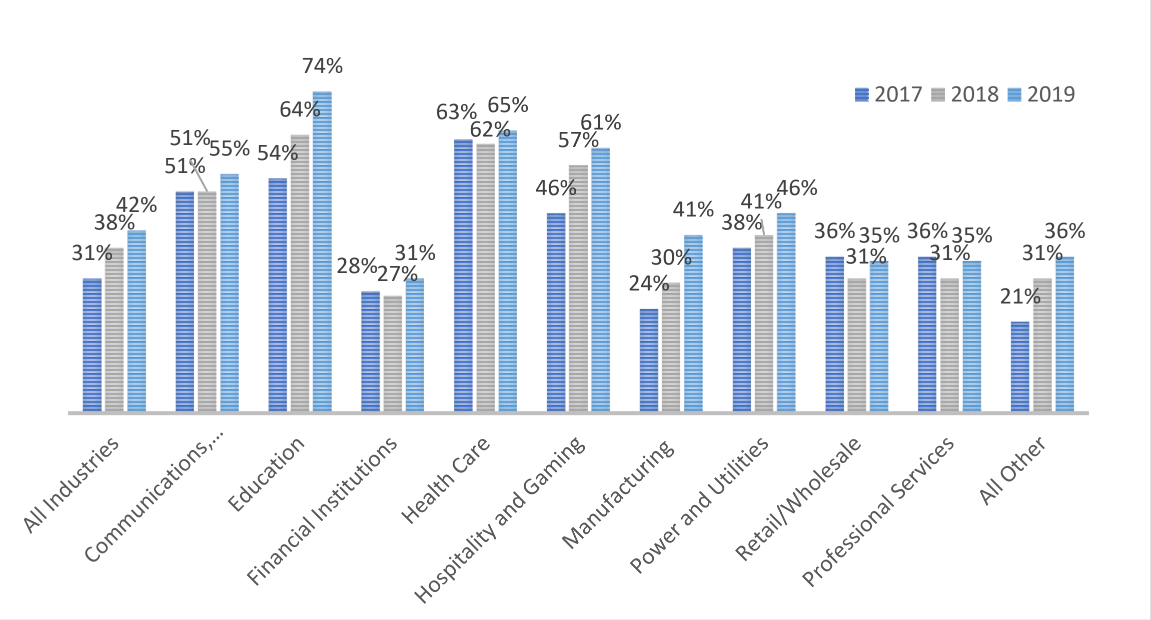
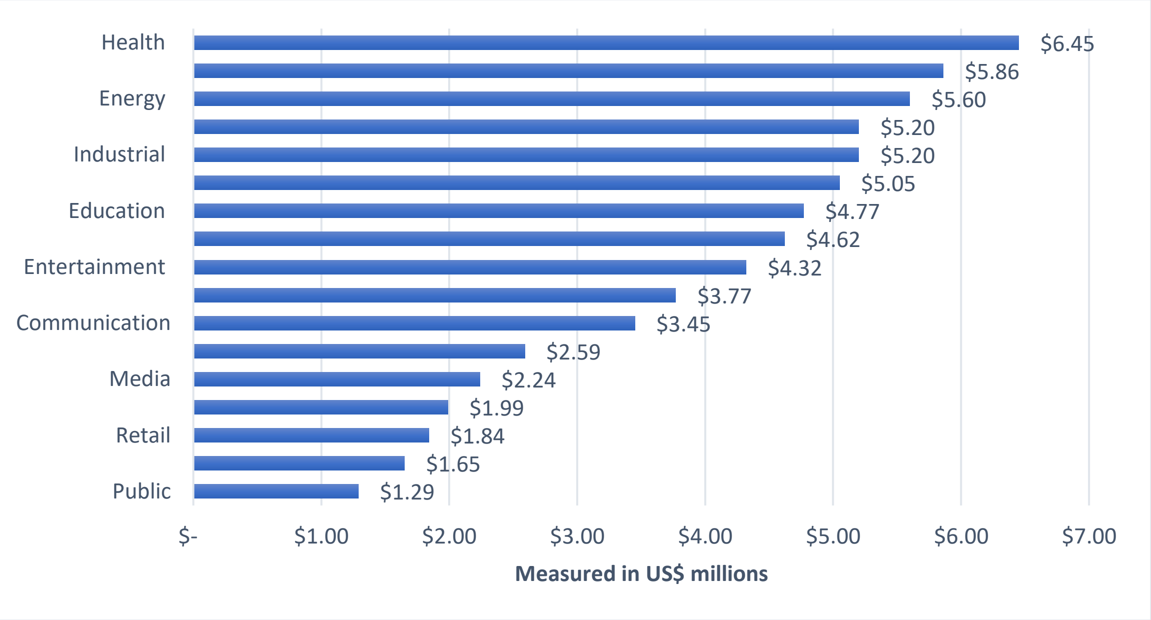


Figure 3: Average Total Cost of a Data Breach by Industry [11]



CYBER RISK IN THE HEALTHCARE SECTOR

The digitization of health records has made many aspects of healthcare administration and delivery more efficient, reducing costs and increasing accessibility, but it has also dramatically increased the exposure of the healthcare sector to cyber-attacks and data breaches. The late 2000s experienced a shift from theft of physical records to hacking of personal and medical information within technology systems. There is a vast amount of data regarding data breaches within healthcare organizations. Based on the data collected for this study, breaches such as email phishing attacks, malware attacks, ransomware attacks, and other various types of hacking methods frequently employed to target healthcare organizations. Despite measures that providers have in place to prevent data breaches, "…89% of healthcare organizations experienced a data breach in the past two years" [12]. Our analysis of the healthcare sector reveals much of the industry's exposed data is related to personal patient information. This information includes, but is not limited to: names, addresses, dates of birth, social security numbers, insurance contract information and numbers, debit and credit card information, phone numbers, and medical information.

The Digitization of the Healthcare Industry

The computerization of the healthcare industry overall has increased productivity, which has at the same time increased reliance on technology. In one of the biggest healthcare data breaches of 2020, Universal Health Services (UHS), one of the largest health networks in the United States, was affected at all of their U.S. sites and hospitals. Specifically, on September 27, 2020, the UHS experienced a ransomware attack which locked company computers and phone systems across the country. The suspected cybercriminals used a strain of ransomware known as

Ryuk [13]. Due to this attack, doctors and nurses were forced “to rely on paper and pencil for record keeping and slowing lab work. Employees described chaotic conditions impeding patient care” [14]. This major attack displays the consequences that cyber-attacks can have on productivity and operations.

The privacy of healthcare information has long been a concern of consumers. The Healthcare Insurance Portability and Accountability Act (HIPAA) enacted in 1996—well before the widespread digitization of personal health information—provides for stringent safeguarding of such information. HIPAA remains to this day the single most important piece of federal legislation governing health information privacy concerns. The law requires that personal health care information must be protected. In 2009, the law further evolved with the passage of the Health Information Technology for Economic and Clinical Health Act (HITECH) under the Obama administration. HITECH imposed financial penalties for violations of HIPAA which increased the cost of HIPAA noncompliance [15]. Sensitivity associated with the compromise of health information is evident in the expensive settlements of healthcare sector cyber-attacks, such as in the 2016 Banner Health cyberattack in which an $8.9 million settlement was paid.

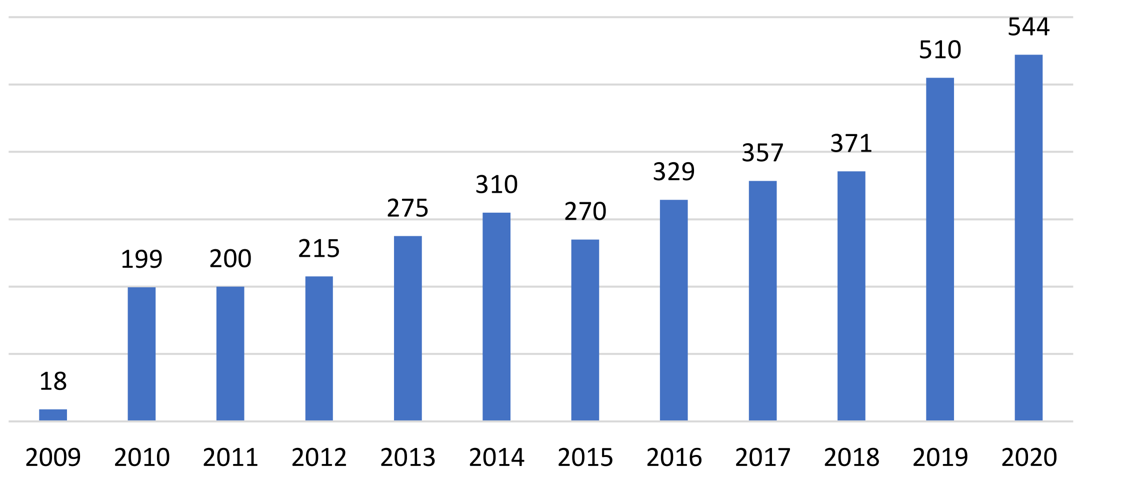
The sheer size of the healthcare sector (nearly 20 percent of the GDP in 2020), the trend toward digitization of medical records, and the rapid evolution of medical technology are just three of many factors that attract the attention of cyber criminals. Despite many attacks in recent years, the healthcare sector remains highly susceptible to debilitating cyber-attacks.

Issues in Common Healthcare Cybersecurity Practices

The healthcare industry is known to have had some of the “worst cybersecurity practices worldwide” [16]. This analysis of healthcare sector data breaches strongly suggests a systemic problem with data and system security throughout this major economic sector. Violations of privacy statutes and allegations of negligence in the wake of data breaches have led to litigation, in which class-action lawsuits for large settlements were filed based on accusations that the companies involved failed to implement reasonable security protocols. These settlements were so substantial because of both the number of patients or records involved and the type of data that was exposed. Healthcare data breaches tend to be extremely costly due to the sensitivity of the exposed data. In the "2020 IBM Report, the average cost of a data breach reported that the most expensive attacks in 2019 occurred in the healthcare sector" [17]. The data that hospitals hold is much more profitable compared to other industries. Healthcare credentials are even "more valuable than credit card information when sold on the dark web" [18]. The danger in the healthcare sector is that a hacker could potentially use one's identity for years once a certain amount of personally identifiable information is obtained through healthcare data breaches.

Based on our dataset, it is apparent that healthcare organizations both large and small are targeted. There has been a steady increase in the number of healthcare data breaches each year. Figure 4 shows the number of breaches involving 500 or more records from 2009 to November 2020 [19 & 20].

Figure 4: Healthcare Data Breaches of 500 or More Records per Year [19& 20]



Note: These are data breaches of 500 or more healthcare records reported to the Department of Health and Human Services' Office for Civil Rights by HIPAA-covered entities and business associates.
**2020 is through November 2020*

Victims range from large for-profit organizations to small nonprofits. Small healthcare organizations may arguably be a more attractive target, because small providers are still struggling with cybersecurity and frequently do not have the human or financial resources necessary to keep pace with state-of-the art governance and risk management strategies. Small providers struggle with even the most remedial of security protocols such as multi-factor authentication (MFA), "…with just half of those providers implementing MFA to shore-up potential vulnerabilities" [21].

Multi-Factor Authentication Protection

Multi-factor authentication adds an additional layer of protection against one of the most common breaches - compromised credentials [22]. Multi-factor authentication helps to insulate an organization against remote attacks and can prevent hackers from easily gaining access to sensitive data. When paired with employee training, multi-factor authentication is even more effective. With a "push" notification, MFA authentication requests a verification code (often via text message or email) in order to login. A trained employee would easily be able to recognize activity as suspicious if they have not recently attempted to log into one of their accounts or systems. According to ValiMail CEO Alexander Garcia-Tobar, "It only takes one click for a person to endanger an entire enterprise" and "healthcare organizations are particularly vulnerable to these attacks because awareness about email authentication is still quite low in the sector as a whole" [23]. Small-to-medium sized healthcare providers frequently lack the resources to implement and maintain robust cybersecurity systems. Worse still, many are overconfident in their current risk management practices—or ignorant of their vulnerabilities. Such failures can have significant financial consequences as evidenced by a spate of recent class action lawsuits against healthcare providers filed in response to data breaches. The lawsuits allege negligence on the part of those providers in that they failed to take reasonable steps to protect confidential patient information. In the case of 21st Century Oncology, the company faced a $2.3 million lawsuit with the court finding that it failed to implement security measures to reduce risks while also failing to apply procedures to review information system activity regularly [24].

Along with the addition of multi-factor authentication, one of the most important aspects of risk management that a healthcare organization can introduce is employee training. According to Michael Bruemmer, vice president of Experian Data Breach Resolutions, 80% of the incidents they serviced had basic employee negligence as a root cause. "That includes such mistakes as losing laptops or clicking on phishing emails. 'Employees are still the weakest link.'" [25]. Additionally, healthcare industry data breaches are commonly linked to theft and loss of laptops. According to a Data Breach Investigations Report, in which 1,300 data breaches involving 20 industries were analyzed, "healthcare was the only industry that had theft and loss as a major cause of security incidents" [26]. This accounted for 46% of the security incidents. This further demonstrates that employee risk needs to be mitigated in order to help reduce cyber vulnerabilities in the healthcare industry.

Sophistication: A Dynamic Threat

Cyber threats are dynamic, and the tools, techniques and strategies employed by those with malicious intent are becoming increasingly sophisticated—and ever costlier to thwart. According to a Ponemon Institute report, "For the 9th year in a row, healthcare organizations had the highest cost of a breach – nearly $6.5 million on average (over 60% more than other industries in the study)" [27]. This lofty cost is partly due to the exponential increase in digitized health information and the fact that compromised health records can produce losses for years after a breach. Identity theft is just one such example of potentially long-lived losses. The nature and modality of cyber-attacks is also shifting. Ransomware attacks, for example, are becoming increasingly common. The shift away from offline backups has made companies more vulnerable to certain types of attack. According to Raimund Genes, CTO at Trend Micro: "Ransomware attacks are surging because attackers have perfected their techniques while enterprises in all sectors have failed to address critical security shortcomings" [28]. The ABCD incident, that is explained in Appendix I, shows that even companies with advanced cybersecurity in place can still become victims of ransomware attacks. While it is not "possible to prevent all ransomware attacks, risk can be reduced to an acceptable level with cybersecurity solutions and securely stored backups of data will ensure ransom demands will not have to be paid" [29].

The ever-increasing sophistication of cyber-attack strategies underscores the critical need for healthcare organizations to implement multi-layered security systems and encryption to help ensure that patient data cannot be accessed by unauthorized third parties [30]. This is particularly crucial because the healthcare industry accounts for a large share of economic activity in the United States. In 2019, health spending accounted for 17.7% of the nation's gross domestic product [31].

Our analysis of major cyber-attacks on the healthcare industry (see appendix) reveals that a substantial proportion of healthcare organizations were not prepared when attacked. Even those who believed they were prepared clearly underestimated the threat. There is no question that the confidential health data of millions of Americans remains extremely vulnerable to cyber-attack and employee negligence. Failure to mitigate against these risks is very costly. Consequently, data security is one of the healthcare industry's biggest concerns today and will remain as such for the foreseeable future [32].

TRANSPORTATION SECTOR

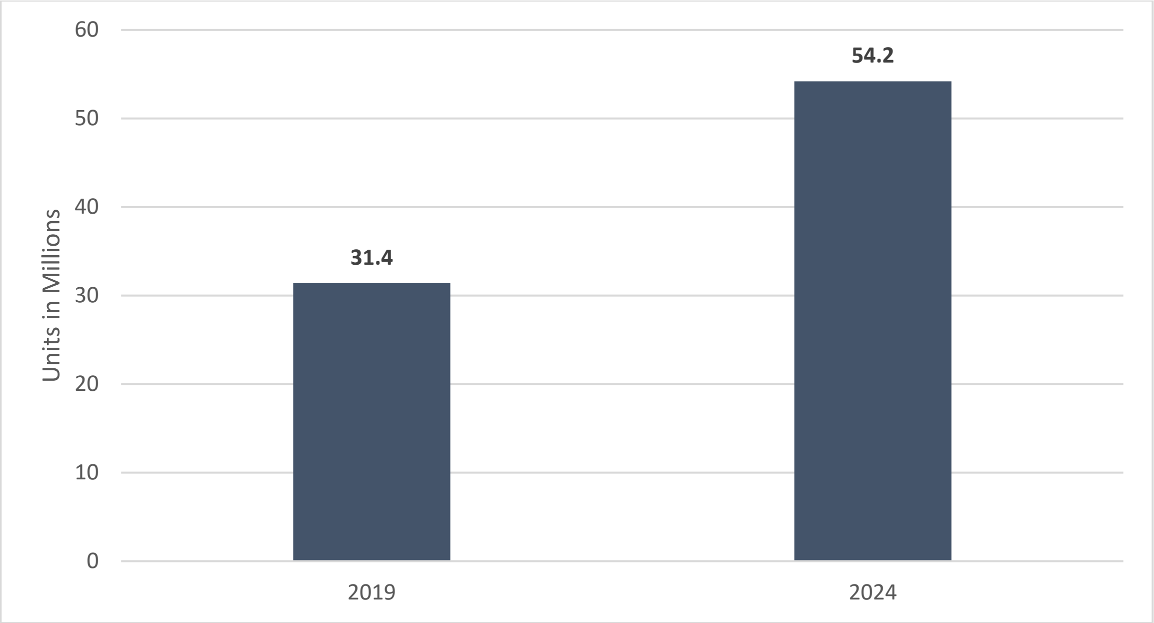
Transportation networks are particularly vulnerable to cyber risks due to increased digitization, vast amounts of data flowing across systems and the immediate impact disruptions can have on travel and supply chains. As more systems and devices are connected—directly or indirectly—the more vulnerable this industry becomes. Advances in communications across electronic networks have caused the potential of disruption to become a serious concern. The interconnected data systems of different branches of the transportation infrastructure including automobiles, aviation, shipping, railways, and trucking compound the likelihood of cyber-attacks causing significant interference and material economic disruption [33].

In the automobile industry, software and electronic components are increasingly prevalent in modern vehicles. According to McKinsey & Company, the software market for vehicles "is expected to grow from USD 238 billion in 2020 to USD 469 billion in 2030, corresponding to an annual growth of over 7 percent per year" [34]. This growth is driven by innovation in four areas: autonomous cars, connectivity, electric cars, and car sharing. Various studies have analyzed the cybersecurity threats to autonomous vehicles. In general, as the degree of vehicle autonomy increases, the increased dependence on computerized control systems increases vulnerability to hacking. "Without sufficient security, vehicle-to-vehicle and vehicle-to infrastructure communication channels can be hacked, which can lead to serious accidents" [35].

Autonomous Vehicles: An Evolving Risk

The market for autonomous vehicles is growing rapidly. "According to a new forecast from International Data Corporation (IDC), the number of vehicles capable of at least Level 1 autonomy will increase from 31.4 million units in 2019 to 54.2 million units in 2024, representing a five-year compound annual growth rate (CAGR) of 11.5%" [36]. See Figure 5 below for a visualization of this information. The Level 1 autonomy described here is established by the Society of Automotive Engineers and consists of "…driver assistance that may assist active steering, breaking, or acceleration; however, the driver still remains responsible and in control of the vehicle [36].

Figure 5: Expected Growth for Autonomous Vehicles [36]



The movement of car sales and customer data to online platforms makes the industry increasingly susceptible to cyber-attacks. In 2019, 198 million car buyer records were exposed in a massive data leak from a car buyer marketing database, DealerLeads. The database that included names, email addresses, phone numbers, and street addresses, was found to be insecurely posted online [37]. DealerLeads was able to password-protect the database once notified, but the data had already been exposed. In reaction to the event, Jonathan Knudsen, a senior security strategist at Synopsys, said "all that was needed was a simple policy that every internet-facing system needs: password protection, data encryption, or other fundamental protections" [37]. This breach highlights the necessity of an increase in security measures within the automobile industry.

<u>Cyber Risk in the Aviation Industry</u>

Further, the aviation industry faces similar challenges and susceptibility. With the proliferation of inflight wireless networks and other systems in recent years, an increasing number of aircraft—including large passenger aircraft carrying hundreds of passengers—are today connected to the internet, which raises concerns over potential cyber-attacks. Overall, commercial aircraft have never been safer. Technical advances have reduced the chances of an accident, but much of the improvement in aviation safety is derived from the computerization of flight systems, both internal and external to the aircraft. These computer systems are critical to essential operations such as inflight control and navigation systems, air traffic control, and passenger reservations. Marsh emphasizes, “As aircraft move ever closer to becoming fully e-enabled and automation increases, pilot practices and training will need to adapt in the event of system failure or security breach” [33]. In 2015, LOT Polish Airlines suffered a DDoS attack which caused the airline's computers to crash. It also destroyed its flight plan IT system. This resulted in a 5-hour disruption that saw 10 flight cancellations, 12 flight delays, and 1,400 passengers grounded. Flights midair were luckily unaffected [38]. Due to the loss of crucial flight information, David Emm, principal security researcher at Kaspersky Lab postulates: “This story highlights the fact that, as more and more aspects of our lives become cyber-dependent, we offer a greater attack surface to cybercriminals – including critical infrastructure systems” [39]. There is no question that the aviation industry’s increasing dependence on globally interconnected digital platforms will only amplify risks in the years ahead.

Cyber Risk in the Rail Industry

Comparably, Rail transportation IT systems require high levels of accessibility. Rail infrastructure is particularly vulnerable due to multiple types of risks. One risk is that railway driver assistance and control systems are highly interconnected. If these systems are infiltrated, serious consequences could arise including loss of control of one or more trains [40].

Transportation system vulnerabilities are present throughout the world and hackers need not be sophisticated to be successful. The public transportation in Lodz, Poland, was attacked in 2008 when a “14-year-old modified a TV remote control so that it could be used to change track points. The teenager broke into a number of tram depots to gather the information needed to build the device, which turned the tram system in Lodz into his own personal train set. As a result, four vehicles were derailed injuring twelve people” [33]. Other rail systems have been attacked, such as the ransomware attack on the Massachusetts Bay Transportation Authority (MBTA) in October 2020. Hackers obtained personal information from workers for MBTA’s commuter rail operator, Keolis, and posted it online in attempt to blackmail the company. Keolis took the systems that were affected offline, notified law enforcement, and took steps to restore the affected systems [41]. Ticketing, rail information systems and system websites represent additional nodes of vulnerability because of the potential for customer financial information to be exposed. Ticket validity is also a concern and websites are vulnerable to multitude of attack modalities [40].

Cyber Risk in the Trucking Industry

Within the trucking industry, connected systems continue to grow. In October 2019, the Volvo Group passed the milestone of one million connected customer assets in terms of delivered trucks, buses, and construction equipment [42]. This connectivity is expected to increase sustainability, uptime, and traffic safety. Connectivity is expected to continue to expand exponentially. According to a McKinsey Global Institute discussion paper, *Connected World: An evolution in connectivity beyond the 5G revolution,* citing a recent International Data Corporation (IDC) estimate, “there could be up to 42 billion connected IoT devices by 2025”

[43]. The more connected transportation networks become, the more vulnerable they are to cyber risk.

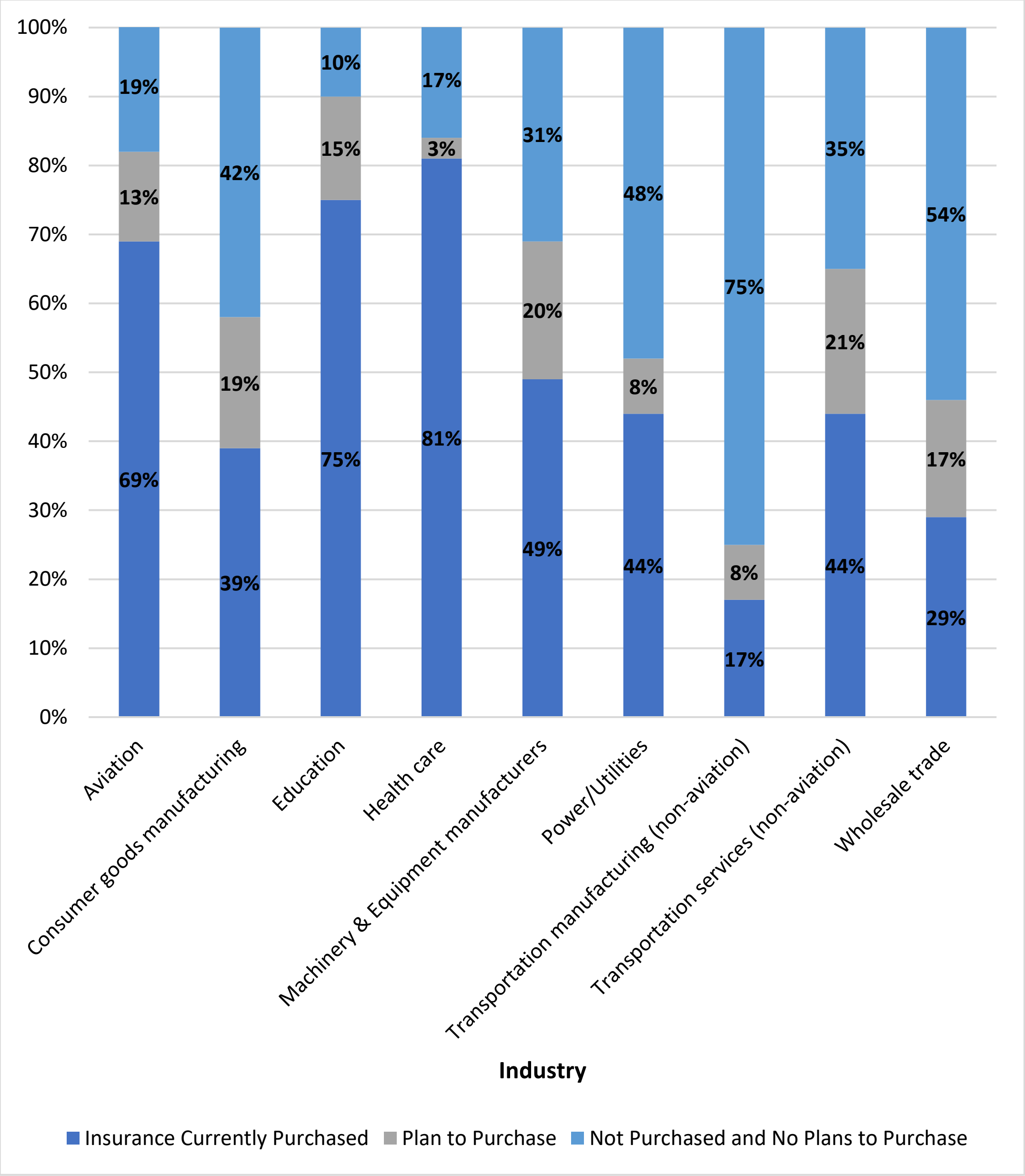
Cyber Risk in the Freight Industry

Analogous to the trucking industry, the shipping industry is likewise vulnerable but on a global scale. Ships utilize electronic navigation devices such as the Global Positioning System (GPS) which if interfered with, can cause serious trouble for ship operators, increasing the likelihood of crashing [44]. Additionally, maritime operations use millions of data points each week, making it crucial for shipping lines to have this data stored securely [45]. In 2017, a cyber-attack against Maersk, a global shipping company, disrupted operations for two weeks and cost the company around $300 million. Maersk was hit by a worm named NotPetya, which locked access to systems that the company uses to operate shipping terminals worldwide. No data was lost, and ships operated normally throughout the period the systems were down. However, for up to two days, the affected terminals could not move cargo, resulting in significant losses from worldwide delays [46]. In order for maritime operators to mitigate attacks, they must have a cybersecurity plan and take steps to strengthen firewalls to stop attacks like the Maersk attack from happening [45].

Despite an evolving risk landscape, with cyber risk moving up the ladder, certain companies are still choosing not to purchase cyber coverage. According to Aon’s 2019 Global Risk Management Survey, less than half (44%) of the transportation service companies (non-aviation) purchased cyber insurance coverage, and 35% of companies had no plan of purchasing cyber-insurance (See Figure 6). The aviation industry is better off, with 69% who have purchased coverage and only 19% with no plans to purchase [47].

Research and analysis reveal that transportation organizations of many different types and sizes are targeted. Many of those attacked were not prepared at the time of the attack nor had a plan in place of what to do after the initial attack. The development and implementation of comprehensive cyber-risk management plans—plans which include the purchase of proper insurance coverage—are critically important in the transportation sector given the extreme interdependence of transportation risks with virtually every other major industry sectors.

Figure 6: Purchase of Cyber Insurance Coverage by Industry [47]



ELECTIONS

Elections are vulnerable to a wide variety of cybersecurity risks due to the rapid adoption of and increasing reliance on digital election infrastructure. This vulnerability came to the forefront in the United States for the first time during the 2008 presidential campaign and has remained a consistent issue since then [48]. Specifically, during the 2008 presidential contest between Democrat Barack Obama and his Republican rival John McCain, the FBI uncovered a massive cyberespionage operation against both campaigns. The operation was ultimately traced back to the People's Republic of China. The goal of the campaign intrusion was thought to be to export internal data from both campaigns. This included internal position papers and private emails to gain leverage with the winner of the election. The intrusion into the campaign's computer networks continued for months after first being detected by the FBI in the summer of 2008. The attack was initially delivered by a "phishing" email which contained an attachment with sophisticated malware that infiltrated the Obama campaign's computer system [49]. This malware allowed threat actors to exfiltrate data from both campaigns. This event was particularly significant because it was the first time that a foreign actor had exfiltrated large quantities of information from a United States presidential race for potential use by a foreign government [50]. Fortunately, in the 2012 elections, there were no documented instances of digital foul play or malicious hacking [51]. Although there was no concrete evidence of a hack from the 2012 election, that does not mean that the large potential threat was nonexistent. Indeed, it is possible that infiltrations occurred but went undetected or were detected but not publicly revealed.

During the United States' 2016 presidential election cycle, the Obama administration accused Russia of interference. In a joint statement from the U.S. Intelligence Community and the Department of Homeland Security, the agencies announced that “The U.S. Intelligence Community is confident that the Russian Government directed the recent compromises of emails from U.S. persons and institutions, including from U.S. political organizations. These thefts and disclosures are intended to interfere with the U.S. election process” [52]. Hackers created a fake email account to send phishing emails to over 30 of Democratic nominee, Hillary Clinton’s staffers. The emails included a link that directed to a document titled "hillaryclinton-favorable-rating.xlsx". This led to a website operated by the hackers where they were able to use stolen credentials to access the Democratic Congressional Campaign Committee network and steal data. They accessed 33 Democratic National Committee (DNC) computers and registered for a website called ‘DC leaks’ to publicize the documents [53]. Special Counsel Robert Mueller, charged with investigating Russian interference in the 2016 election, issued an indictment [1] of twelve Russian intelligence officers in the hacking of the DNC and the Clinton campaign. It was hoped that the indictment would have a deterrent effect and reduce the likelihood of future attacks [54].

While vulnerabilities in election systems certainly remain, much has been done in the United States to strengthen the cyber defenses. Before the 2018 midterms, 40 states invested more than $75 million of federal and state funds to secure election systems after the 2016 election. This also includes 26 states that conducted security assessments and implemented cybersecurity upgrades, 20 states that enhanced cybersecurity training for election officials, 15 states that upgraded voting equipment, and 9 states that expanded post-election audits [55]. While it is impossible to directly assess what impact, if any, the Mueller indictments had on reducing foreign interference in the 2020 presidential, there is clear evidence that the cyber threat was diminished. In late November 2020, Christopher Krebs, director of the Cybersecurity and Infrastructure Security Agency (CISA), claimed the election had been “the most secure in U.S. history” and “there was no indication of evidence that there was any sort of hacking or compromise of election systems on, before or after November 3” [56]. Krebs was subsequently fired by President Trump for speaking out against his various assertions that the election had, in fact, been stolen. Yet state, local and national election officials appear to have taken threats

[1] This indictment detailed the accusation by the American government of the Russian government interference in the 2016 election. From https://www.justice.gov/file/1080281/download.

manifested in the 2016 election seriously, implementing multiple security measures to ensure the validity and integrity of the election process.

Direct cyber-attacks are far from the only means available to perpetrators of election interference. Misinformation and disinformation can also undermine public confidence in the election process. Ahead of the 2020 presidential election, CISA released a resource guide designed to counter some of the more common rumors contributing to public concerns over security of election infrastructure and related processes [57]. This CISA guide provides an in-depth analysis of voting system processes in the United States and dispels numerous false assertions, including suggestions that election software is not reviewed or tested beforehand. CISA went further still, issuing a joint statement in November 2020 with the Elections Infrastructure Government Coordinating Council and other groups. The collective opinion of this consortium of experts on election integrity, as it applies to the 2020 presidential race, is that recounts are to be expected when elections are close. The process has built-in redundancies (e.g., paper ballots to back up votes cast electronically) that allow for the identification and correction of any mistakes or errors [58]. CISA and its partners conclude that despite numerous claims to the contrary, there was "no evidence that any voting system deleted or lost votes, changed votes, or was in any way compromised" during the 2020 presidential election cycle [58].

While the 2020 election was more secure than those of the past, in October 2020, Trustwave, a global cybersecurity company, discovered a hacker was selling personally identifying information on 186 million American voters. Much of the data was already publicly available, but names, email addresses, and voter registration records were found for sale on the dark web. While voter registration data is publicly available in most states, email addresses are often not included in that public data. The databases were listed for sale by "Greenmoon2019" and potentially enabled malicious actors to target registered Democrats or Republicans through email. Zid Mador, the vice president of security research at Trustwave, pointed out: “In the wrong hands, this voter and consumer data can easily be used for geotargeted disinformation campaigns over social media, email phishing and text and phone scams before, during and after the election, especially if results are contested” [59].

While much of America’s attention was focused on securing the presidential election system, one of the biggest known thefts of cybersecurity tools occurred. FireEye[2], one of the largest cybersecurity companies in the United States, announced on December 8, 2020, foreign government hackers with "world-class capabilities" broke into their network and stole tools that they use to test the defenses of thousands of customers including federal, state, and local governments. FireEye partners with a wide range of insurance companies including Marsh, Lockton, Beazley, and Sompo International. FireEye's CEO, Kevin Mandia, released in a statement that the attacker "primarily sought information related to certain government customers." Mandia also stated that he has concluded that the attack was completed by a nation with "top-tier offensive capabilities” [60]. The motive behind the attack remains unclear.

Just five days after the FireEye attack was announced, a much larger attack on IT monitoring and management software SolarWinds stole the headlines. SolarWinds clients include many of the largest technology, telecommunications and consulting firms in the world—along with many agencies of numerous national governments, including the United States. The attacks on FireEye and SolarWinds led to a broader investigation as to whether the Russian

[2] FireEye is a publicly traded cybersecurity company (FEYE). On December 8, 2020 (the day the attack was announced) the stock was trading at 15.52 and dropped to 13.49 on December 9th, representing a decrease of 13%. From https://finance.yahoo.com/quote/FEYE/

hackers had achieved in infiltrating both federal and private networks [61]. In a statement on December 13, 2020, the Russian Embassy in Washington denied any involvement. If Russia's connection is confirmed in this attack, it will be "the most sophisticated known theft of American government data since a two-year spree in 2014 and 2015, in which Russian intelligence agencies gained access to the unclassified email systems at the White House, the State Department and the Joint Chiefs of Staff. It took years to undo the damage..." [61]. This expansive hack could have long lasting potential effects on affected organizations.

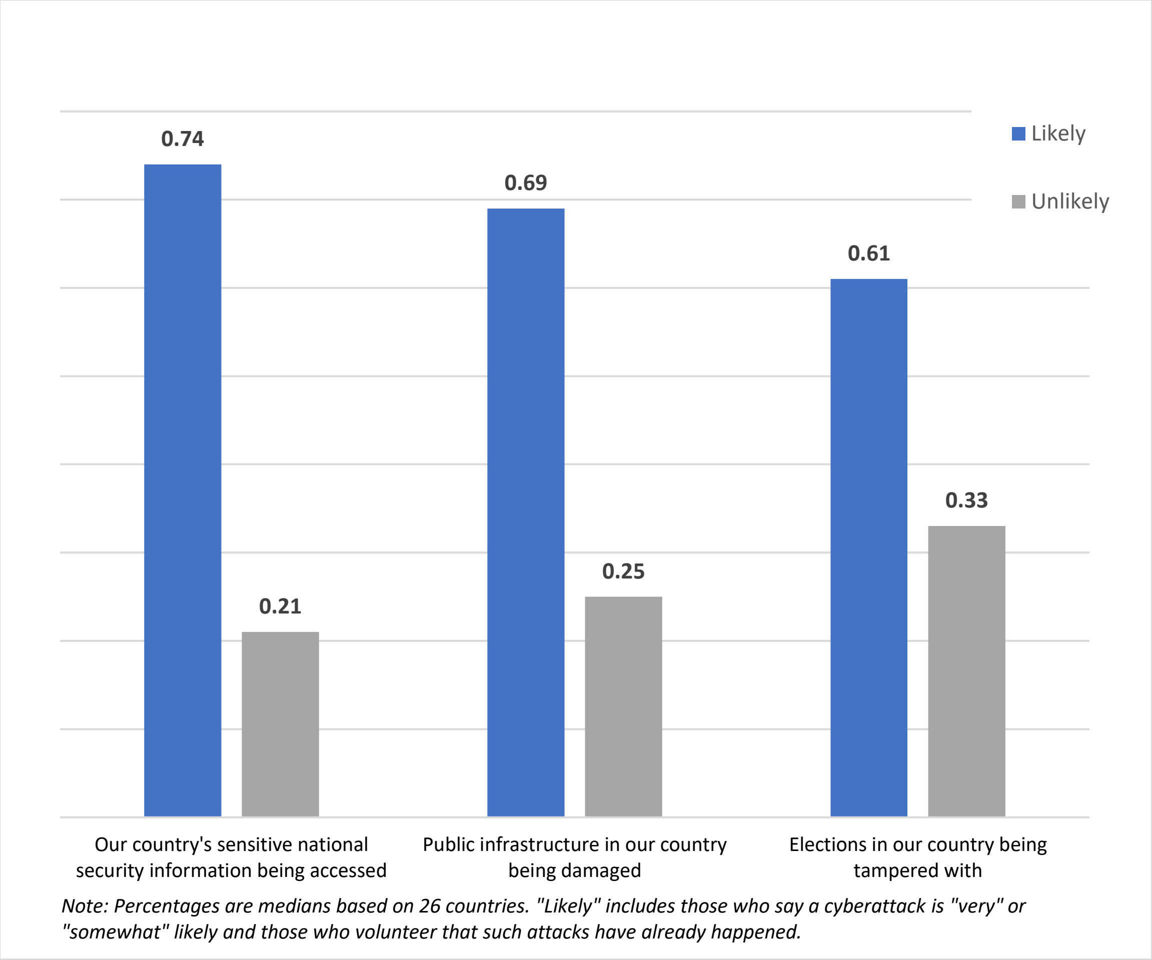
There are a multitude of reasons as to why voting systems in the United States are particularly vulnerable. In a New York Times article, "The Crisis of Election Security" the susceptibility of America's voting systems is analyzed through the past elections. It asks and answers: "How did our election system get so vulnerable, and why haven't officials tried harder to fix it? The answer, ultimately, comes down to politics and money: The voting machines are made by well-connected private companies that wield immense control over their proprietary software, often fighting vigorously in court to prevent anyone from examining it when things go awry" [62]. The risk of cyber-attacks to election infrastructure is not new. The history of Russian theft alone of critical data from the U.S. government spans across more than two decades and resulted in the creation of the United States Cyber Command, which is the Pentagon's evolving cyberwarfare force [61]. Then Secretary of State, Mike Pompeo, in a radio talk show interview with Mark Levin said it was "pretty clear" that Russia was behind the security attack against the United States in 2020. He also said that Russia was on the list of people who "want to undermine our way of life, our republic, [and] our basic democratic principles… you see the news of the day with respect to their efforts in cyberspace. We've seen this for an awfully long time, using asymmetric capabilities to try and put themselves in a place where they can impose costs on the

United States" [63]. It was not until three weeks after the realization of the attack that the United States formally named Russia as the likely source in a joint statement issued by the FBI, Department of Homeland Security, Director of National Intelligence, and National Security Agency [64].

Election Security in Countries Outside the United States

Other countries are also plagued by cyber-attacks in election processes, often with different vulnerabilities being targeted. Figure 7 displays statistics from a study in which 26 countries were asked about the likelihood and preparation for cyber-attacks on national security information, public infrastructure, and elections in their country. A striking 74% of these countries said that it was likely that their country's sensitive national security information was being accessed [65].

Figure 7: Perceived Likelihood of Cyber-attacks within 26 Countries [65]



Note: Percentages are medians based on 26 countries. "Likely" includes those who say a cyberattack is "very" or "somewhat" likely and those who volunteer that such attacks have already happened.

Estonia was one of the first countries to be attacked in the first major act of cyber warfare. In 2007, the Estonian government decided to move the Bronze Soldier, a symbol of Soviet oppression. This decision led to protests which were exacerbated by false Russian news reports that claimed the statue was being destroyed; when it was in reality being moved. In this rioting, 156 people were injured, one person died, and 1,000 people were detained. Additionally, the day after the physical destruction, cyber-attacks affected online services of Estonian banks, media outlets, and government bodies. Also, a massive volume of spam email was sent by botnets, generating large numbers of online requests and overloading servers. Estonians were unable to use online banking services, government employees were unable to email, and newspapers could not deliver news [66]. Estonia faced lost productivity, opportunity cost, remediation, and acquiring alternative web services at emergency rates that is estimated to have cost billions of Euro [67]. Positively, this event transformed Estonia. Estonia was hit particularly hard because it is heavily dependent on online processes and digital infrastructure. In 2008, it was estimated that Estonia was “97% dependent on internet banking” [67]. This event was a “wake-up call, helping Estonians become experts in cyber defense today” [66]. The country’s leading IT experts are trained by the Ministry of Defense. The event helped to earn Estonia a reputation today as a country with extremely strong cyber security. This example was one of the first attacks on one nation by another. Russia has been involved in a multitude of hacks against other nations including, most notably, the United States, Lithuania, and Kyrgyzstan [67].

Ten years later, in 2017, the French were able to successfully counter Russian electoral interference. Two days before the final round of the French presidential elections, data hacked from Emmanuel Macron’s presidential campaign team were released online. Nearly 14.5 gigabytes of emails and personal and business documents were posted to the site Pastebin through links to more than 70,000 files. Officials from Macron’s party said that the attackers mixed fake documents and authentic ones to create confusion and misinformation. One of the reasons the hack was unsuccessful was the speed at which the issue was addressed. Throughout the campaign, the susceptibility to hacking was communicated openly and all hacking attempts were made public. This attempt was announced within a few hours. Additionally, a few hours after the documents were released online, the French mandated period of 48 hours of reflection prior to an election, where the media and campaigns are silent, began. This ‘blackout’ period of mainstream media, which the United States does not implement, helped to make the attempt unsuccessful at deterring popular opinion of the elect. France was able to anticipate, react, and coordinate its response between the Macron campaign staff, the government, and civil society [68].

Misinformation and Disinformation

Democratic elections rely heavily on faith in the electoral process. Therefore, the deliberate introduction and spread of false information can increase voter confusion and devalue a fact-based political debate. In recent years, social media has been the platform of choice for disrupting elections through the dissemination of both misinformation and disinformation, though other electronic methods exist—including ordinary email. The result is a blurring of lines between truth and fiction. The difference between misinformation and disinformation is important and is based on intention. Misinformation occurs when false information is spread, regardless of the intent to mislead [69]. Disinformation is the "deliberate generation and dissemination of false information to manipulate public opinion and perceptions…" The rapid spread of misinformation and disinformation online has led many organizations to strengthen cyber security safeguards [70].

Today, most major social media platforms invest heavily in content screening, including political content. After the 2016 presidential election, Facebook hired thousands of third-party moderators located in the Philippines, India, Dublin, and the United States to help bolster their reputation. There is currently a debate as to whether content moderation is best carried out by humans or largely through the use of artificial intelligence (AI). Mary Gray, a senior principal researcher at Microsoft Research warned "They [Facebook] haven't made enough leaps and bounds in artificial intelligence to take away the best tool we have: human intelligence to do the discernment" [71]. While AI technology is increasingly reliable and is more efficient from a cost perspective, overdependence on it can increase the risk of false information spreading across social media. Forms of disinformation vary and quickly evolve. The deception involved in disinformation is similar to that of phishing. Facebook had nearly 15,000 contractors at 20 sites globally hired to remove pornography, hate speech, terrorism, and other unwanted content from its site. The screening process works to detect deception and misinformation. Due to the coronavirus pandemic, Facebook in 2020 sent home thousands of these human moderators. The social network must now rely more on technology to protect against misinformation [71]. Facebook along with other companies, such as Twitter, have used artificial intelligence and algorithms, but have recognized that humans are vital to removing some of the content. The pressure to combat misinformation regarding a multitude of subjects, including the integrity of the 2020 general election in the United State and the COVID-19 pandemic, is high.

Overall, there does not need to be a cyber-attack in order to disrupt through online platforms. Misinformation and disinformation can be particularly dangerous to elections, because they can threaten democracy by spreading deceit. Disinformation campaigns are a means of interfering with campaigns digitally which undermines confidence in democracies. Lastly, disinformation can damage trust in the media.

Reliability of Online Content

Liability associated with content has evolved due to election integrity. With a multitude of platforms and many posts, it can be difficult to decipher the validity of information spread about Candidates. Recently there has been debate over whether Section 230, which helps platforms to moderate posts, should still be upheld. This provision is known as the “twenty-six words that created the internet.” Created back in 1996, Section 230 was enacted as a part of the Communications Decency Act (CDA). Section 230 was originally created after a court ruling against the online platform Prodigy. In this case, Prodigy argued that it was not responsible for its users' speech, but the court treated Prodigy more like a publisher because they moderate some of their users' posts. While being treated like a publisher, a platform would be legally liable for misleading or harmful content it 'publishes' [72]. Section 230 allowed for companies to moderate material on their platforms without being treated like a publisher under law. It says: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" [73]. Therefore, platforms cannot be held liable for what users post.

The COVID-19 pandemic caused content to be moderated more closely. Prior to the pandemic, misinformation was generally political in nature and was not known to not cause immediate harm. False information relating to the Coronavirus, could however, cause direct harm. Posts claiming the virus was a hoax may have undermined the credibility of public responses that were necessary to slow the spread of the virus and might have encouraged people to ignore warnings and gather in groups [74]. As a result, platforms adopted stricter moderation policies toward COVID-19 misinformation. In addition to COVID-19, political speech made Section 230 one of the most discussed topics of 2020. Donald Trump and other republicans have accused tech companies of censoring conservatives. Some have argued that Big Tech has gained too much control. Two days after the 2021 storming of the United States Capital on January 6th, Twitter suspended President Trump from its platform permanently. Social media companies have long been tested by President Trump who violated Twitter's policy against the glorification of violence [75]. Twitter's announcement said that "After close review of recent Tweets from the @realDonaldTrump account and the context around them we have permanently suspended the account due to the risk of further incitement of violence" [3]. Facebook and Instagram also

[3] https://twitter.com/twittersafety/status/1347684877634838528

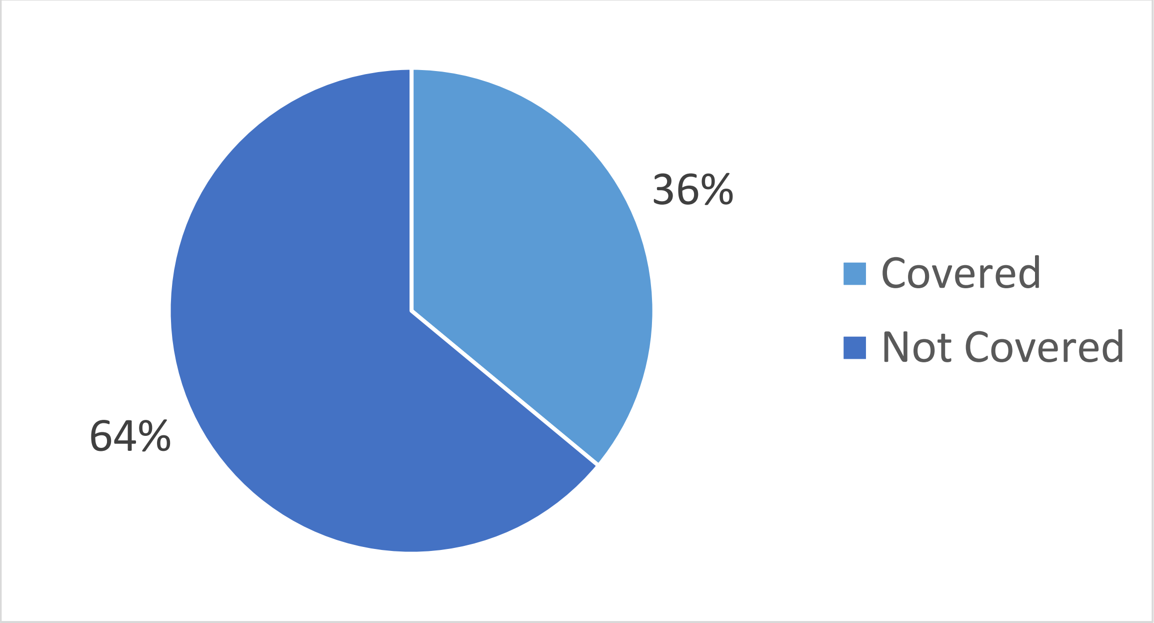
temporarily suspended Trump's account. Regarding Section 230, tech leaders of Twitter, Jack Dorsey, and Facebook, Mark Zuckerberg, said they are open to revising the legislation [76]. Twitter and Facebook have said their platforms balance between promoting free expression and removing harmful content [76]. Democrats, including Joe Biden, have also spoken on the subject of Section 230, urging Congress to revise it to help remove hate speech, election interference, and false information.

The debated question is: should these platforms be held liable for the content it holds? Both parties push for revision of the act, yet for different reasons. Jen Kosseff, an assistant professor of cybersecurity law in the U.S. Naval Academy's Cyber Science Department, said "it would be challenging for Congress to reach consensus on how to alter Section 230" [76]. He also mentioned it would be challenging to satisfy everyone who is upset with the big tech companies. Repealing Section 230 would ultimately lead to more moderation, because of the increased risk of liability of the content that users post.

COVID-19

The COVID-19 pandemic has accelerated a major shift—already underway prior to the pandemic—toward a more digitized workforce and world in general. Many employees are working from home and relying on emails and other platforms to communicate with co-workers and customers. The increased reliance on digital communications technologies increases the probability of both malicious attacks and unintentional breaches. Consistent with the increased vulnerability, the FBI has reported a 400 percent increase in cyber-attacks post-COVID [77], demonstrating beyond any doubt that malicious actors are exploiting an exponential increase in the attack surface. Heightened awareness of cyber threats even before COVID was already driving demand for cyber insurance sharply upward. A Zurich Insurance and Advisen Ltd. study reported that the proportion of companies (all sizes) purchasing coverage grew from 34 percent in 2011 to around 80 percent in 2020 [77]. Smaller businesses, however, appear less aware, willing or able to mitigate the financial consequences of cyber-attacks through the purchase of insurance. According to the 2020 CyberScout survey, "64 percent of U.S. SMBs (small and mid-sized businesses) reported not having cyber insurance coverage for their business and 5 percent didn't know if they have any cyber coverage in their current policy" [78] (See Figure 8). Despite a sharp increase in cyber-attacks aimed at employees working from home—especially ransomware attacks—the reasons why most SMBs continue to lack cyber insurance coverage remains unclear. This disconnect may be attributed to the lack of knowledge and cost. In the future of digital work, business plans must prioritize cyber risk as a top business liability.

Figure 8: Small Businesses with Cyber Policies [78]



<u>Vaccine Vulnerabilities: A Complex Supply Chain</u>

With respect to the Covid-19 vaccine, criminals will likely try to interrupt the distribution. The COVID-19 supply chain is extremely vulnerable to hackers and other cyber security issues, such as ransomware attacks on hospitals and pharmacies. The international police organization, Interpol, in early December 2020 issued a Global Orange Notice, which is a serious and imminent threat to public safety [79]. The Interpol secretary general warned: "As governments are preparing to roll out vaccines, criminal organizations are planning to infiltrate or disrupt supply chains" [80]. This has been seen within the first few weeks of distribution. IBM's cybersecurity division found that a series of cyber-attacks were underway that aimed at the companies and government organizations distributing the coronavirus vaccines [81]. According to the IBM X-Force report, a global phishing campaign targeted organizations within the COVID-19 "cold chain" began as early as September 2020. This cold chain refers to the step of the vaccine supply chain that ensures preservation of the vaccines in a temperature-controlled environment during both storage and transportation [82]. Nick Rossmann, who leads IBM's global threat intelligence teams, said that the cyber-attacks "were working to get access to how the vaccine is shipped, stored, kept cold, and delivered" [81]. This attack emphasizes the need for cybersecurity diligence at each step of the vaccine supply chain.

CONCLUSION

The evolution of cyber risk in the past 25 years has caused the risk to become extremely prevalent in today's society creating an increasingly sophisticated market for cyber insurance. Companies are increasingly dependent on technology, which increases their exposure to cyber threats. Multiple factors affect the risks that corporations face. Three of the most afflicted sectors of cyber risk were analyzed: healthcare, transportation, and electoral systems. Risk mitigation continues to be the goal of corporations, with an increasing focus on cyber risk. One of the most important aspects of mitigating cyber risk will be awareness. As businesses become more connected and interdependent on technology, they become more vulnerable to these types of attacks. I foresee the next wave of cyber risk will be pertaining to personal medical data being held by the companies creating apps for vaccine passports[4]. With an ever-changing world that is constantly evolving technologically, there will always be cyber risks. Cyber insurance coverage needs to be part of every policy. I hope that companies and organizations are preparing for the future by implementing technologies to enhance cyber resilience.

Cyber insurance coverage should be part of a company's multifaceted defense strategy against cyber risks. Some other defenses that should be implemented include Multi-factor Authentication (MFA), password protection, data encryption, and employee awareness training.

I would lastly like to thank my director, Dr. Robert Hartwig, for his outstanding role in guiding me through this research and writing process. I would also like to thank my second reader, Gregory Niehaus, for his time and expertise during this process.

[4] Ideas on vaccination passport apps currently remain uncertain. An analog approach that does not need an app to work would be more accessible, cheaper, and more privacy concerning. A semi-digital approach (that EU is currently considering), with the use of paper records that are verifiable by QR code, could be hacked. From https://www.govtech.com/security/vaccination-passport-apps-could-help-society-reopen--first-they-have-to-be-secure-private-and-trusted.html

REFERENCES

[1] M. Camillo, “Cyber risk and the changing role of insurance,” *Journal of Cyber Policy*, vol. 2, no. 1, pp. 53–63, 2017.

[2] N. Geographic, “Y2K Bug,” *National Geographic*. National Geographics Society, Washington, D.C., 1991.

[3] J. L. Peterson, M. Wheatley, and M. Kellner-Rogers, “The Y2K problem: Social chaos or social transformation?,” *The Futurist*, vol. 32, pp. 21–28, Oct-1998.

[4] Radanliev, Petar et al. (2018): Analyzing IoT cyber risk for estimating IoT cyber insurance, in: Living in the Internet of Things: Cybersecurity of the IoT - 2018. IET Conference Proceedings, ISBN 978-1-78561-843-7, The Institution of Engineering and Technology, London, pp. 1-9, http://dx.doi.org/10.1049/cp.2018.0003

[5] “What Is Cyber Insurance?,” *Nationwide*. [Online]. Available: https://www.nationwide.com/lc/resources/small-business/articles/what-is-cyber-insurance. [Accessed: 10-Oct-2020].

[6] A. Granato and A. Polacek, “The growth and challenges of cyber insurance,” *The Federal Reserve Bank of Chicago*, Chicago Fed Letter, 2019.

[7] J. Monck-Mason and A. Chittock, “The far-reaching impact of Cyber-attacks,” *Willis Towers Watson*, 03-Oct-2019. [Online]. Available: https://www.willistowerswatson.com/en-US/Insights/2019/10/the-far-reaching-impact-of-cyber-attacks. [Accessed: 11-Feb-2021].

[8] T. Finan, “Reassuring the reshoring: A cyber risk management proposal,” *Willis Towers Watson*, 15-Sep-2020. [Online]. Available: https://www.willistowerswatson.com/en-US/Insights/2020/09/reassuring-the-reshoring-a-cyber-risk-management-proposal. [Accessed: 11-Nov-2020].

[9] R. Piggin, “Cyber security trends: What should keep CEOs awake at night,” *International Journal of Critical Infrastructure Protection*, vol. 13, pp. 36–38, Feb. 2016.

[10] *Cyber Insurance Purchasing Grows Again in 2019*, Mar-2020. [Online]. Available: https://www.marsh.com/us/insights/research/cyber-insurance-purchasing-grows-again.html. [Accessed: 10-Dec-2020].

[11] Ponemon Institute, “Cost of a Data Breach Report,” IBM Security. [Online], 2019.

[12] B. Dobran, “31 Alarming Healthcare Cybersecurity Statistics For 2020,” *phoenixNAP Global IT Services*, 08-Jul-2019. [Online]. Available: https://phoenixnap.com/blog/healthcare-cybersecurity-statistics. [Accessed: 15-Feb-2021].

[13] J. Davis, “UPDATE: UHS Health System Confirms All US Sites Affected by Ransomware Attack,” *HealthITSecurity*, 05-Oct-2020. [Online]. Available: https://healthitsecurity.com/news/uhs-health-system-confirms-all-us-sites-affected-by-ransomware-attack. [Accessed: 16-Dec-2020].

[14] M. James, “FBI warns ransomware assault threatens US health care system: At least 5 hospitals have been hit this week,” *USA Today*, 06-Nov-2020.

[15] HIPAA Guidance, “The History of HIPAA,” *Accountable*, 14-May-2020. [Online]. Available: https://www.accountablehq.com/post/history-of-hipaa. [Accessed: 16-Oct-2020].

[16] A. Steger, “What Happens to Stolen Healthcare Data?”, *Technology Solutions That Drive Healthcare,* 30-Oct-2019. [Online]. Available: https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon. [Accessed: 15-Nov-2020].

[17] A. Hamilton, “Data Breaches in the Healthcare Industry Continue Due to Availability of Valuable Information,” *Identity Theft Resource Center*, 11-Aug-2020. [Online]. Available: https://www.idtheftcenter.org/data-breaches-in-the-healthcare-industry-continue-due-to-availability-of-valuable-information/. [Accessed: 15-Nov-2020].

[18] Netcom Solutions, “Why do hackers target healthcare organizations?”, *Netcom Solutions*, 10-Dec-2018. [Online]. Available: https://www.netcomsolutions.net/2018/12/why-do-hackers-target-healthcare-organizations/#:~:text=In%20fact%2C%20healthcare%20credentials%20are,sector%20is%20attacked%20by%20malware.&text=This%20makes%20it%20easier%20for,to%20the%20hospital's%20sensitive%20information. [Accessed: 15-Dec-2020].

[19] “Healthcare Data Breach Statistics,” *HIPAA Journal*. [Online]. Available: https://www.hipaajournal.com/healthcare-data-breach-statistics/. [Accessed: 24-Oct-2020].

[20] “November 2020 Healthcare Data Breach Report,” *HIPAA Journal*, 22-Dec-2020. [Online]. Available: https://www.hipaajournal.com/november-2020-healthcare-data-breach-report/. [Accessed: 16-Jan-2021].

[21] J. Davis, “Small Providers Still Struggling with Cybersecurity, Risk Management,” *HealthITSecurity*, 01-Jul-2019. [Online]. Available: https://healthitsecurity.com/news/small-providers-still-struggling-with-cybersecurity-risk-management. [Accessed: 20-Oct-2020].

[22] LBMC, “Why Multi-Factor Authentication Is a Must,” *LBMC Family of Companies*, 31-Jan-2020. [Online]. Available: https://www.lbmc.com/blog/why-multi-factor-authentication-is-a-must/. [Accessed: 15-Oct-2020].

[23] R. Francis, “Ransomware makes healthcare WannaCry,” *CSO Online*, 15-May-2017. [Online]. Available: https://www.csoonline.com/article/3196827/ransomware-makes-healthcare-wannacry.html. [Accessed: 16-Dec-2020].

[24] E. Snell, “$2.3M OCR Settlement Reached for 21st Century Oncology Data Breach,” *HealthITSecurity*, 14-Dec-2017. [Online]. Available: https://healthitsecurity.com/news/2.3m-ocr-settlement-reached-for-21st-century-oncology-data-breach. [Accessed: 16-Dec-2020].

[25] M. K. McGee, “Biggest Health Data Breaches in 2014,” *Data Breach Today*, 22-Dec-2014. [Online]. Available: https://www.databreachtoday.com/biggest-health-data-breaches-in-2014-a-7705#:~:text=The%20largest%20breach%20in%202014,which%20affected%204.5%20mi

llion%20individuals.&text=The%20Community%20Health%20Systems%20incident,breach%20notification%20rule%20in%202009. [Accessed: 15-Jan-2021].

[26] P. Stricker, “Healthcare Data Breaches and Their Frequency, Impact, and Cost - TCS,” *TCS Healthcare Technologies,* 30-May-2019. [Online]. Available: https://www.tcshealthcare.com/healthcare-data-breaches-frequency-impact-cost/. [Accessed: 15-Nov-2020].

[27] “IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years,” *IBM News Room,* 23-Jul-2019. [Online]. Available: https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years. [Accessed: 16-Nov-2020].

[28] V. Haran, “Why Is Ransomware So Successful?”, *Bank Information Security,* 20-Sep-2016. [Online]. Available: https://www.bankinfosecurity.com/interviews/interview-raimund-genes-ransomware-virus-total-issue-i-3328. [Accessed: 08-Nov-2020].

[29] “More than 55,000 Patients Impacted by ABCD Pediatrics Ransomware Attack,” *HIPAA Journal,* 04-Apr-2017. [Online]. Available: https://www.hipaajournal.com/more-than-55000-patients-impacted-by-abcd-pediatrics-ransomware-attack-8753/. [Accessed: 16-Oct-2020].

[30] S. Alder, “Community Health Systems Cyber Attack Puts 4.5M Patients at Risk,” *HIPAA Journal,* 2014.

[31] CMS.gov, “Historical,” *Centers for Medicare and Medicaid Services,* 16-Dec-2020. [Online]. Available: https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsHistorical#:~:text=The%20data%20are%20presented%20by,spending%20accounted%20for%2017.7%20percent. [Accessed: 15-Jan-2021].

[32] “Why Data Security is The Biggest Concern of Health Care,” *UIC Online Health Informatics,* 08-Jul-2020. [Online]. Available: https://healthinformatics.uic.edu/blog/why-data-security-is-the-biggest-concern-of-health-care/. [Accessed: 28-Dec-2020].

[33] “Marsh Insights: Cyber Risk in the Transportation Industry,” *Marsh*, 2015. [Online]. Available: https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Risk%20in%20the%20Transportation%20Industry-03-2015.pdf. [Accessed: 20-Oct-2020].

[34] O. Burkacky, J. Deichmann, B. Klein, K. Pototzky, and G. Scherf, “Cybersecurity in Automotive,” *McKinsey & Company*, Mar-2020. [Online]. Available: https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Cybersecurity%20in%20automotive%20Mastering%20the%20challenge/Cybersecurity-in-automotive-Mastering-the-challenge.pdf. [Accessed: 20-Nov-2020].

[35] A. Taeihagh and H. S. Lim, “Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks,” *Transport Reviews*, vol. 39, no. 1, pp. 103–128, 2018.

[36] "A New IDC Forecast Shows How Vehicles Will Gradually Incorporate the Technologies that Lead to Autonomy," *IDC*, 28-Sep-2020. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS46887020#:~:text=According%20to%20a%20new%20forecast,(CAGR)%20of%2011.5%25. [Accessed: 17-Sep-2020].

[37] D. Winder, "Bought A Car Recently? 198 Million Car Buyer Records Exposed in Massive Data Leak," *Forbes*, 16-Sep-2019. [Online]. Available: https://www.forbes.com/sites/daveywinder/2019/09/15/bought-a-car-recently-198m-car-buyer-records-exposed-in-massive-data-leak/?sh=285d9b037391. [Accessed: 17-Oct-2020].

[38] "Cyber Resilience in the Aviation Sector," *Aon*, 2018. [Online]. Available: https://www.aon.com/getmedia/475a36e5-fae0-484b-b333-a7507c13b62b/cyber-sellsheet-aviation.aspx. [Accessed: 17-Feb-2021].

[39] A. Kharpal, "Hack attack leaves 1,400 airline passengers grounded," *CNBC*, 22-Jun-2015. [Online]. Available: https://www.cnbc.com/2015/06/22/hack-attack-leaves-1400-passengers-of-polish-airline-lot-grounded.html#:~:text=Ten%20planes%20and%20around%201%2C400,to%20the%20aircraft%20before%20takeoff. [Accessed: 17-Oct-2020].

[40] A. S. Prevost, "The rail industry in the connected era: promising potential versus cyber risks," *Stormshield*, 23-Mar-2020. [Online]. Available: https://www.stormshield.com/news/the-rail-industry-in-the-connected-era-promising-potential-versus-cyber-risks/. [Accessed: 17-Sep-2020].

[41] S. P. Cotter, “MBTA Commuter Rail operator hit by ransomware,” *Boston Herald*, 22-Oct-2020. [Online]. Available: https://www.bostonherald.com/2020/10/22/mbta-commuter-rail-operator-hit-by-ransomware/. [Accessed: 17-Nov-2020].

[42] “The Volvo Group passes the milestone of one million connected customer assets for increased sustainability, uptime and safety,” *Volvo*, 03-Oct-2019. [Online]. Available: https://www.volvogroup.com/en-en/news/2019/oct/news-3436058.html. [Accessed: 17-Oct-2020].

[43] “Connected World: An evolution in connectivity beyond the 5G revolution,” *McKinsey Global Institute*, Feb-2020. [Online]. Available: https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/Telecommunications/Our%20Insights/Connected%20world%20An%20evolution%20in%20connectivity%20beyond%20the%205G%20revolution/MGI_Connected-World_Executive-summary_February-2020.pdf. [Accessed: 17-Dec-2020].

[44] N. Goud, “Shipping companies are extremely vulnerable to Cyber Attacks,” *Cybersecurity Insiders*, 13-Jan-2017. [Online]. Available: https://www.cybersecurity-insiders.com/shipping-companies-are-extremely-vulnerable-to-cyber-attacks/. [Accessed: 17-Oct-2020].

[45] “COSCO Cyber Attack and The Importance of Maritime Cybersecurity,” *Cyber Security Intelligence*, 31-Jul-2018. [Online]. Available: https://www.cybersecurityintelligence.com/blog/cosco-cyber-attack-and-the-importance-of-maritime-cybersecurity-

3622.html#:~:text=Maritime%20operations%20cough%20up%20millions,there%20is%20a%20cyber%20attack. [Accessed: 09-Sep-2020].

[46] J. Leovy, "Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks," *Los Angeles Times*, 17-Aug-2017. [Online]. Available: https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html. [Accessed: 17-Sep-2020].

[47] "Global Risk Management Survey - 2019," *Aon*, 2019. [Online]. Available: https://www.aon.com/getmedia/8d5ad510-1ae5-4d2b-a3d0-e241181da882/2019-Aon-Global-Risk-Management-Survey-Report.aspx. [Accessed: 29-Oct-2020].

[48] A. Brill, "Case Study - Protecting the 2008 U.S. Presidential Election from Cyber Attacks," *Kroll.com*, 09-Jun-2020. [Online]. Available: https://www.kroll.com/en/insights/publications/cyber/protecting-2008-us-presidential-election-obama-campaign-cyber-attacks. [Accessed: 21-Dec-2020].

[49] M. Isikoff and N. B. C. News, "Chinese hacked Obama, McCain campaigns, took internal documents, officials say," *NBCNews.com*, 07-Jun-2013. [Online]. Available: https://www.nbcnews.com/id/wbna52133016. [Accessed: 05-Jan-2021].

[50] "Compromise of U.S. presidential campaigns in 2008," *Council on Foreign Relations*, Nov-2008. [Online]. Available: https://www.cfr.org/cyber-operations/compromise-us-presidential-campaigns-2008. [Accessed: 04-Jan-2021].

[51] D. Gross, “How secure is your electronic vote?”, *CNN*, 03-Nov-2012. [Online]. Available: https://www.cnn.com/2012/11/03/tech/innovation/electronic-vote-security/index.html. [Accessed: 23-Dec-2020].

[52] E. Nakashima, “U.S. government officially accuses Russia of hacking campaign to interfere with elections,” *The Washington Post*, 07-Oct-2016. [Online]. Available: https://www.washingtonpost.com/world/national-security/us-government-officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html. [Accessed: 03-Jan-2021].

[53] CNN Editorial Research, “2016 Presidential Campaign Hacking Fast Facts,” *CNN*, 28-Oct-2020. [Online]. Available: https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html. [Accessed: 15-Jan-2021].

[54] M. Mazzetti and K. Benner, “12 Russian Agents Indicted in Mueller Investigation,” *The New York Times*, 13-Jul-2018. [Online]. Available: https://www.nytimes.com/2018/07/13/us/politics/mueller-indictment-russian-intelligence-hacking.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=a-lede-package-region®ion=top-news&WT.nav=top-news. [Accessed: 21-Dec-2020].

[55] “CSIS Election Cybersecurity Scorecard: The Outlook for 2018, 2020 and Beyond,” *CSIS.org*, 29-Oct-2018. [Online]. Available: https://www.csis.org/analysis/csis-election-cybersecurity-scorecard-outlook-2018-2020-and-beyond. [Accessed: 23-Nov-2020].

[56] L. Barr, “Trump campaign lawyer calls for fired DHS election security official to be 'shot',” *ABC News*, 01-Dec-2020. [Online]. Available: https://abcnews.go.com/Politics/trump-campaign-lawyer-calls-fired-dhs-election-security/story?id=74479123. [Accessed: 10-Feb-2021].

[57] “#Protect2020 Rumor vs. Reality,” *cisa.gov*, 2020. [Online]. Available: https://www.cisa.gov/rumorcontrol. [Accessed: 04-Jan-2021].

[58] “Joint Statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees,” *cisa.gov*, 12-Nov-2020. [Online]. Available: https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election. [Accessed: 16-Feb-2021].

[59] K. Dilanian, “Cybersecurity company finds hacker selling info on 186 million U.S. voters,” *NBCNews.com*, 21-Oct-2020. [Online]. Available: https://www.nbcnews.com/politics/2020-election/cybersecurity-firm-finds-hacker-selling-info-148-million-u-s-n1244211. [Accessed: 19-Dec-2020].

[60] D. E. Sanger and N. Perlroth, “FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State,” *The New York Times*, 08-Dec-2020. [Online]. Available: https://www.nytimes.com/2020/12/08/technology/fireeye-hacked-russians.html. [Accessed: 18-Feb-2021].

[61] D. E. Sanger, “Russian Hackers Broke into Federal Agencies, U.S. Officials Suspect,” *The New York Times*, 13-Dec-2020. [Online]. Available:

https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html. [Accessed: 23-Feb-2021].

[62] K. Zetter, “The Crisis of Election Security,” *The New York Times*, 26-Sep-2018. [Online]. Available: https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html. [Accessed: 12-Jan-2021].

[63] F. Bajak and J. Colvin, “Trump undercuts Pompeo, saying China may be responsible for cyberattack after secretary of state says Russia 'pretty clearly' did it,” *chicagotribune.com*, 19-Dec-2020. [Online]. Available: https://www.chicagotribune.com/nation-world/ct-nw-russia-hacking-cyberattack-20201219-l5mgq3q7mncgjb2fe7csbkbdiu-story.html. [Accessed: 03-Jan-2021].

[64] K. Johnson, “U.S. formally links Russia to massive 'ongoing' cyber-attack; scope of hacking unclear,” *USA Today*, 06-Jan-2021. [Online]. Available: https://www.usatoday.com/story/news/politics/2021/01/05/u-s-formally-links-russia-massive-cyberattack-hack-ongoing/6552803002/?itm_source=AMP&itm_medium=UpNext. [Accessed: 23-Jan-2021].

[65] J. Poushter and J. Fetterolf, “International Publics Brace for Cyberattacks on Elections, Infrastructure, National Security,” *Pew Research Center*, 09-Jan-2019. [Online]. Available: https://www.pewresearch.org/global/2019/01/09/international-publics-brace-for-cyberattacks-on-elections-infrastructure-national-security/. [Accessed: 02-Mar-2021].

[66] D. McGuinness, “How a cyber-attack transformed Estonia,” *BBC News*, 27-Apr-2017. [Online]. Available: https://www.bbc.com/news/39655415. [Accessed: 03-Feb-2021].

[67] “Executive Summary: 2007 Cyber Attacks on Estonia,” *Central and Eastern European Online Library*, 2019. [Online]. Available: https://www.ceeol.com/search/gray-literature-detail?id=804501. [Accessed: 23-Jan-2021].

[68] “Successfully Countering Russian Electoral Interference,” *csis.org*, 21-Jun-2018. [Online]. Available: https://www.csis.org/analysis/successfully-countering-russian-electoral-interference. [Accessed: 08-Dec-2020].

[69] “‘Misinformation’ vs. ‘Disinformation’: Get Informed on The Difference,” *Dictionary.com*, 19-Jan-2021. [Online]. Available: https://www.dictionary.com/e/misinformation-vs-disinformation-get-informed-on-the-difference/. [Accessed: 08-Feb-2021].

[70] “Disinformation and Electoral Integrity: A Guidance Document for NDI Elections Programs,” *ndi.org*, 13-May-2019. [Online]. Available: https://www.ndi.org/publications/disinformation-and-electoral-integrity-guidance-document-ndi-elections-programs. [Accessed: 21-Mar-2021].

[71] N. T. Elizabeth Dwoskin, “Facebook sent home thousands of human moderators due to the coronavirus. Now the algorithms are in charge,” *The Washington Post*, 24-Mar-2020. [Online]. Available: https://www.washingtonpost.com/technology/2020/03/23/facebook-moderators-coronavirus/. [Accessed: 21-Feb-2021].

[72] L. Feiner, “Both Trump and Biden have criticized Big Tech's favorite law - here's what Section 230 says and why they want to change it,” *CNBC*, 28-May-2020. [Online]. Available: https://www.cnbc.com/2020/05/28/what-is-section-230.html. [Accessed: 24-Jan-2021].

[73] “47 U.S. Code § 230 - Protection for private blocking and screening of offensive material,” *Legal Information Institute*. [Online]. Available: https://www.law.cornell.edu/uscode/text/47/230. [Accessed: 08-Jan-2021].

[74] M. Feeney and W. Duffield, “A Year of Content Moderation and Section 230,” *Cato Institute,* 02-Nov-2020. [Online]. Available: https://www.cato.org/blog/year-content-moderation-section-230. [Accessed: 19-Jan-2021].

[75] B. Fung, “Twitter Bans President Trump Permanently,” *CNN*, 09-Jan-2021. [Online]. Available: https://www.cnn.com/2021/01/08/tech/trump-twitter-ban/index.html. [Accessed: 17-Feb-2021].

[76] J. Guynn, “Donald Trump and Joe Biden vs. Facebook and Twitter: Why Section 230 could get repealed in 2021,” *USA Today,* 04-Jan-2021. [Online]. Available: https://www.usatoday.com/story/tech/2021/01/04/trump-biden-pelosi-section-230-repeal-facebook-twitter-google/4132529001/. [Accessed: 24-Dec-2020].

[77] M. Corbett, “Ransomware, COVID-19 and Cyber Insurance - The Big Disconnect,” *Gen Re Perspective*, 09-Dec-2020. [Online]. Available: https://www.genre.com/knowledge/blog/ransomware-covid-19-and-cyber-insurance-the-big-disconnect-

en.html?utm_campaign=Subscription+Management+Center&utm_medium=email&_hsmi=102359540&_hsenc=p2ANqtz--zI3-zcAuYMeLDmnTnkPluMe5oXRri1n9uaq5P6UBzWWCOE8XLU-zP8OLQA3GxUk89pejPIFQumBgUgRYDVM4TnNvaBkTT0-LPk7DdoM6xtPQaGwo&utm_content=102359540&utm_source=hs_email. [Accessed: 16-Jan-2021].

[78] "2020 SMB Cybersecurity Survey: Small Business, Huge Risks," *www.CyberScout.com*, 2020. [Online]. Available: https://go.cyberscout.com/rs/746-PTV-801/images/CS-2020-SMB-Cybersecurity-Survey.pdf. [Accessed: 01-Jan-2021].

[79] J. Hookway, "Covid-19 Vaccines Are 'Liquid Gold' to Organized Crime, Interpol Says," *The Wall Street Journal*, 03-Dec-2020. [Online]. Available: https://www.wsj.com/articles/virus-vaccines-are-liquid-gold-to-organized-crime-interpol-warns-11607000854?st=8z9oxew6bm6l41y&reflink=article_email_share. [Accessed: 08-Feb-2021].

[80] "Interpol warns of organized crime threat to COVID-19 vaccines," *Interpol*, 02-Dec-2020. [Online]. Available: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-organized-crime-threat-to-COVID-19-vaccines. [Accessed: 04-Feb-2021].

[81] D. E. Sanger and S. Lafraniere, "Cyberattacks Discovered on Vaccine Distribution Operations," *The New York Times*, 03-Dec-2020. [Online]. Available:

https://www.nytimes.com/2020/12/03/us/politics/vaccine-cyberattacks.html. [Accessed: 11-Jan-2021].

[82] C. Zaboeva and M. Frydrych, “IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain,” *Security Intelligence*, 03-Dec-2020. [Online]. Available: https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/. [Accessed: 21-Jan-2021].

[83] “Anthem to Pay Record $115M to Settle Lawsuits Over Data Breach,” *NBCNews.com*, 23-Jun-2017. [Online]. Available: https://www.nbcnews.com/news/us-news/anthem-pay-record-115m-settle-lawsuits-over-data-breach-n776246. [Accessed: 11-Mar-2021].

[84] J. Davis, “UPDATE: 2.9M Patients Impacted by 9-Year Dominion National Hack,” *HealthITSecurity*, 31-Jul-2019. [Online]. Available: https://healthitsecurity.com/news/insurer-dominion-national-reports-server-hack-that-began-august-2010. [Accessed: 11-Jan-2021].

[85] “More Than 600,000 Michigan Residents Affected by Wolverine Solutions Breach, Warns AG Nessel,” *HIPAA Journal*, 15-Mar-2019. [Online]. Available: https://www.hipaajournal.com/more-than-600000-michigan-residents-affected-by-wolverine-solutions-breach-warns-ag-nessel/. [Accessed: 08-Feb-2021].

[86] E. Dietsche, “Data breach at Atrium Health's billing vendor affects 2.65M patients,” *MedCity News*, 29-Nov-2018. [Online]. Available: https://medcitynews.com/2018/11/atrium-health-billing-vendor-patients/. [Accessed: 11-Mar-2021].

[87] Dissent, “MSK Group notifying patients of data security incident,” *DataBreaches.net*, 10-Jul-2018. [Online]. Available: https://www.databreaches.net/msk-group-notifying-patients-of-data-security-incident/. [Accessed: 08-Feb-2021].

[88] “Analysis of 2018 Healthcare Data Breaches,” *HIPAA Journal*, 08-Feb-2019. [Online]. Available: https://www.hipaajournal.com/analysis-of-healthcare-data-breaches/. [Accessed: 04-Feb-2021].

[89] J. Drees, “Piedmont Cancer Institute email phishing incident exposes 5,226 patients' info,” *Becker's Hospital Review*, 01-Oct-2020. [Online]. Available: https://www.beckershospitalreview.com/cybersecurity/piedmont-cancer-institute-email-phishing-incident-exposes-5-226-patients-info.html. [Accessed: 04-Mar-2021].

[90] J. Davis, “UnityPoint Health Reaches $2.8M Settlement Over 2018 Data Breach,” *HealthITSecurity*, 29-Jun-2020. [Online]. Available: https://healthitsecurity.com/news/unitypoint-health-reaches-2.8m-settlement-over-2018-data-breach. [Accessed: 01-Mar-2021].

[91] J. Roman and R. Ross, “China Hackers Suspected in Health Breach,” *Healthcare Information Security*, 18-Aug-2014. [Online]. Available: https://www.healthcareinfosecurity.com/china-hackers-suspected-in-health-breach-a-7204. [Accessed: 11-Feb-2021].

[92] J. Leyden, “US healthcare provider pays $5 million in 2014 data breach settlement,” *The Daily Swig | Cybersecurity news and views*, 09-Oct-2020. [Online]. Available:

https://portswigger.net/daily-swig/us-healthcare-provider-pays-5-million-in-2014-data-breach-settlement. [Accessed: 11-Jan-2021].

[93] E. Snell, “Report Finds 16.6M Affected by 2016 Healthcare Data Breaches,” *HealthITSecurity*, 03-May-2017. [Online]. Available: https://healthitsecurity.com/news/report-finds-16.6m-affected-by-2016-healthcare-data-breaches#:~:text=The%20largest%20healthcare%20data%20breach,occurred%20on%20June%2017%2C%202016. [Accessed: 05-Jan-2021].

[94] J. Davis, “Judge Approves $8.9M Banner Health Settlement Over 2016 Data Breach,” *HealthITSecurity*, 24-Apr-2020. [Online]. Available: https://healthitsecurity.com/news/judge-approves-8.9m-banner-health-settlement-over-2016-data-breach. [Accessed: 23-Mar-2021].

[95] “More than 55,000 Patients Impacted by ABCD Pediatrics Ransomware Attack,” *HIPAA Journal*, 04-Apr-2017. [Online]. Available: https://www.hipaajournal.com/more-than-55000-patients-impacted-by-abcd-pediatrics-ransomware-attack-8753/. [Accessed: 04-Feb-2021].

[96] “NY: Arc of Erie County fined $200,000 for online security breach,” *DataBreaches.net,* 29-Aug-2018. [Online]. Available: https://www.databreaches.net/ny-arc-of-erie-county-fined-200000-for-online-security-breach/#:~:text=The%20Arc%20of%20Erie%20County,Social%20Security%20numbers%20and%20other. [Accessed: 02-Feb-2021].

[97] “The Cyber Attack - From the POV of the CEO,” *Hancock Regional Hospital*, 30-Apr-2019. [Online]. Available: https://www.hancockregionalhospital.org/2018/01/cyber-attack-pov-ceo/. [Accessed: 03-Mar-2021].

[98] “$2.3 Million 21st Century Oncology HIPAA Settlement Agreed with OCR,” *HIPAA Journal*, 15-Dec-2017. [Online]. Available: https://www.hipaajournal.com/2-3-million-21st-century-oncology-hipaa-settlement-agreed-ocr/. [Accessed: 24-Feb-2021].

[99] J. Davis, “UPDATE: 1.5M Patients Impacted by Inmediata Breach, Mailing Issue,” *HealthITSecurity*, 19-Jul-2019. [Online]. Available: https://healthitsecurity.com/news/mailing-error-for-inmediata-while-reporting-health-data-breach. [Accessed: 02-Feb-2021].

[100] “Michigan Attorney General Looking into Inmediata Breach, Mailing Error,” *HealthITSecurity*, 19-Jul-2019. [Online]. Available: https://healthitsecurity.com/news/michigan-attorney-general-looking-into-inmediata-breach-mailing-error. [Accessed: 03-Feb-2021].

[101] “23K Patients of Mayfield Clinic Sent Malware-Infected Email,” *HIPAA Journal*, 10-May-2016. [Online]. Available: https://www.hipaajournal.com/23k-patients-mayfield-clinic-sent-malware-infected-email-3422/. [Accessed: 18-Jan-2021].

[102] M. James, “FBI warns ransomware assault threatens US health care system: At least 5 hospitals have been hit this week,” *USA Today*, 06-Nov-2020. [Online]. Available: https://amp.usatoday.com/amp/6065612002. [Accessed: 19-Feb-2021].

[103] M. K. McGee, “Ransomware Attack's Economic Impact: $67 Million,” *Bank Information Security*, 02-Mar-2021. [Online]. Available: https://www.bankinfosecurity.com/ransomware-attacks-economic-impact-67-million-a-16095. [Accessed: 30-Mar-2021].

[104] C. Hauser, “EasyJet Says Cyberattack Stole Data of 9 Million Customers,” *The New York Times*, 19-May-2020. [Online]. Available: https://www.nytimes.com/2020/05/19/business/easyjet-hacked.html. [Accessed: 04-Feb-2021].

[105] “British Airways faces record £183m fine for data breach,” *BBC News*, 08-Jul-2019. [Online]. Available: https://www.bbc.com/news/business-48905907. [Accessed: 23-Jan-2021].

[106] “LUFTHANSA Miles & More Accounts Hacked; Damage Minimal, No Data Stolen,” *Lufthansa Flyer*, 13-Apr-2015. [Online]. Available: https://lufthansaflyer.boardingarea.com/lufthansa-miles-damage-minimal-no-data-stolen/. [Accessed: 11-Mar-2021].

[107] D. Niepow, “Rail Insider-San Francisco's Muni hack: A case study in prepping for ransomware attacks. Information for Rail Career Professionals from Progressive Railroading Magazine,” *Progressive Railroading*, Jan-2017. [Online]. Available:

https://www.progressiverailroading.com/security/article/San-Franciscos-Muni-hack-A-case-study-in-prepping-for-ransomware-attacks--50602. [Accessed: 03-Mar-2021].

[108] K. Holland, “Update on SFMTA Ransomware Attack,” *SFMTA*, 28-Nov-2016. [Online]. Available: https://www.sfmta.com/blog/update-sfmta-ransomware-attack. [Accessed: 01-Apr-2021].

[109] A. Vaccaro, “Commuter rail operator hit with ransomware attack - The Boston Globe,” *BostonGlobe.com*, 23-Oct-2020. [Online]. Available: https://www.bostonglobe.com/2020/10/23/metro/commuter-rail-operator-hit-with-ransomware-attack/. [Accessed: 12-Feb-2021].

[110] N. Tabak, “Files from TFI's Canpar leak after ransomware attack,” *FreightWaves*, 25-Aug-2020. [Online]. Available: https://www.freightwaves.com/news/files-from-tfis-canpar-leak-after-ransomware-attack. [Accessed: 09-Feb-2021].

[111] E. Lopez, “COSCO restores service 5 days after cyberattack,” *Supply Chain Dive*, 30-Jul-2018. [Online]. Available: https://www.supplychaindive.com/news/COSCO-cyberattack-restores-service/528897/. [Accessed: 08-Mar-2021].

[112] “NotPetya cyber-attack cost TNT at least $300m,” *BBC News*, 20-Sep-2017. [Online]. Available: https://www.bbc.com/news/technology-41336086. [Accessed: 17-Jan-2021].

[113] P. Muncaster, “Vietnamese Hackers Compromised BMW and Hyundai: Report,” *Infosecurity Magazine*, 09-Dec-2019. [Online]. Available: https://www.infosecurity-magazine.com/news/vietnamese-hackers-compromised-bmw/. [Accessed: 02-Feb-2021].

[114] N. Perlroth, “Trump Campaign Website Is Defaced by Hackers,” *The New York Times*, 27-Oct-2020. [Online]. Available: https://www.nytimes.com/2020/10/27/technology/trump-campaign-website-defaced-hackers.html. [Accessed: 11-Mar-2021].

[115] K. Mandia, “FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community,” *FireEye*, 08-Dec-2020. [Online]. Available: https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html. [Accessed: 08-Feb-2021].

[116] R. Donadio, “Why the Macron Hacking Attack Landed with a Thud in France,” *The New York Times*, 08-May-2017. [Online]. Available: https://www.nytimes.com/2017/05/08/world/europe/macron-hacking-attack-france.html. [Accessed: 16-Jan-2021].

APPENDICES

Appendix I: Healthcare

Entity, Date, and Type of Attack	Summary	Records Lost	Financial Loss/Impact	Resolution (date)	Adjustments to Cyber Risk Management
Anthem Blue Cross Blue Shield 1/29/15 Type: Data Breach	An unknown hacker accessed a database that had personal information such as names, birthdays, social security numbers, addresses, emails, and income information [83].	78.8 million policyholders' personal information	Lawsuit of $115 M	Anthem paid out $115 M to settle lawsuits (June 2017).	Anthem provided free credit monitoring and identity protection services to all who were affected for up to two years.
Dominion National 6/1/2019 Type: Medical Data breach	An internal alert notified Dominion National of unauthorized access to computer servers that breached data from as early as August 2010. This data varied, but included names, Social Security numbers, taxpayer identification numbers, bank account and routing numbers, member ID numbers, group numbers, subscriber numbers, addresses, and email addresses [84].	2.96 million patient's personal information	Class Action Lawsuit (on going) filed by Tousley Brain Stephens for the negligent handling of the data.	Individuals were notified (investigation ended April 2019).	The insurer has enhanced its monitoring and alerting software. Dominion National reported the security incident to the FBI. All of the patients received two years of credit and fraud protection services.
Wolverine Solutions Group 9/23/18 Type: Ransomware Attack	Ransomware encrypted files that contained protected health data. The attack is believed to have started with the download of the Emotet Trojan, which has been used in several attacks. The exposed information includes names, addresses, dates of birth, social security numbers, insurance contract information and numbers, phone numbers, and medical information [85].	600,000 patients		Wolverine issued notifications to affected individuals (notified by March 2019).	Affected patients received free access to credit monitoring and identity theft protection services.
AccuDoc Solutions, Inc. (third party vendor of Atrium Health) 9/22/18 Type: Hacking/IT Incident	In October of 2018, Accudoc informed that an unauthorized party gained access to Accudoc's third party vendor, AccuDoc Solutions in late September. Impacted information included names, addresses, dates of birth, social security numbers, etc. [86].	2.65 Million individuals		Individuals were notified (starting October 2018).	Accudoc brought on a forensic firm to help secure its database. They also contacted the FBI. Those whose SSNs were exposed were offered free credit monitoring and identity protection services.
MSK Group 5/7/18 Type: Hacking/IT Incident	MSK Group discovered that its computer networks experienced a security event. After investigation, they did not believe records containing personal information were removed from the computer network; however, there was unauthorized access to the network that stored personal information such as driver's licenses, SSNs, insurance, and medical information [87].	566,000 patients [88].		Individuals were notified (approximately July 9, 2018).	Offered individuals one year of free identify theft protection services.

Entity, Date, and Type of Attack	Summary	Records Lost	Financial Loss/Impact	Resolution (date)	Adjustments to Cyber Risk Management
Piedmont Cancer Institute, P.C. 9/15/20 Type: Email phishing	The institute began notifying over 5,000 patients in September 2020 that their personal health information was exposed during an email phishing incident. An unauthorized individual gained access to a Piedmont Cancer's employee email account between April 5 and May 8. Personal information that was exposed includes names, birthdays, financial account information, and debit and credit card information [89].	5226 patients		Individuals were notified (September 2020).	Piedmont implemented multifactor authentication across its emails and added additional security awareness training.
UnityPoint 3/2020- 5/2020 Type: Email phishing	The health system's email system was hit by a series of targeted phishing emails that appeared to be sent from an executive within UnityPoint. An employee fell for the email thereby giving hackers access to internal email accounts from March 14 to April 3, 2018. It was found that the hackers were likely attempting to divert vendor or payroll payments. The hacked accounts' data that was exposed included names, addresses, medical data, treatment information, lab results, insurance information, payment cards, and SSNs [90].	1.4 Million patients	$2.8 million dollar settlement	The settlement provided the breach victims with monetary relief, including 1 year of comprehensive credit monitoring and identify theft protection services (June 2020).	UnityPoint reset the passwords to the compromised accounts, added phishing education for employees, added secure tools to identify suspicious emails, and implemented multi-factor authentication.
Community Health Systems, Inc. August 2014 Type: Malware attack	Attackers used a sophisticated malware to bypass Community Health System's Security and was able to copy and transfer information out of the system. The compromised information included names, addresses, birthdays, phone numbers, and SSNs [91].	6.2 Million patients	$5 million lawsuit settlement	According to Iowa's Attorney General, CHS failed to implement reasonable security practices. They faced a six-year lawsuit relating to this wrongdoing (October 2020) [92].	CHS agreed to "implement and maintain a comprehensive information security program" to prevent future security failure.
Banner Health 6/17/16 Type: Cybersecurity attack	Banner reported that their computer servers and systems that process payment card data at certain Banner Health food and beverage outlets were affected in the attack. The attack was targeting payment card data including cardholder names, card numbers, expiration dates and internal verification codes. For the providers: names, addresses, birthdays, Tax identification numbers, National Provider Identifier numbers, and SSNs were affected in the data breach [93].	3.6 Million individuals	$8.9 million lawsuit settlement [94]	Lawsuit was due to victims claiming that Banner failed to thoroughly investigate and harden their systems against risks (April 2020).	Banner claimed to be enhancing the security of its systems.

Entity, Date, and Type of Attack	Summary	Records Lost	Financial Loss/Impact	Resolution (date)	Adjustments to Cyber Risk Management
ABCD Pediatrics 2/6/2017 Type: Ransomware attack	ABCD Pediatrics discovered that someone gained unauthorized access to its servers and used ransomware to encrypt data. The attack involved a ransomware called Dharma. The encryption process was stopped by the anti-virus solution used by ABCD Pediatrics, isolating the affected servers and taking them offline. The type of information that was potentially compromised includes patients' names, addresses, phone numbers, demographic information, SSNs, insurance billing information, and medical records [95].	55,447 patients impacted	N/A	Individuals were notified; impacted individuals received credit monitoring and identity theft protection services for one year (notified after March 2018).	The investigation found the source of the attack and additional security solutions such as state-of-the-art network cyber monitoring were added to ABCD's security measures.
Arc of Erie County (Non-profit) 7/2015-2/2018 Type: Breach of client information	An investigator found that clients' personal information was publicly available on the internet from July 2015 to February 2018 [96].	3,751 clients	$200,000 penalty to the state	In Match, 2018, clients were formally notified. They were provided with a one-year subscription to LifeLock to protect against identity theft. The case was handled by the Bureau of Internet and Technology Deputy Bureau Chief, Clark Russell. The Arc of Erie County paid $200,00 in fees for violating HIPAA (August 2018).	The Arc of Erie County announced that it will review its policies and analyze its vulnerabilities of all electronic equipment and data systems.
Hancock Health Hospital 1/11/2018 Type: Ransomware attack	A criminal group that is believed to be located in Eastern Europe obtained the log in credentials of a vendor that provides hardware for one of the information systems used by the hospital. SamSam malware was used to encrypt data files associated with this system. Messages appeared on the hospital PC screens saying that the system was encrypted using SamSam ransomware, it also demanded a payment be made within seven days or there would be permanent encryption of the data. The CEO decided to pay the ransom of four bitcoin to retrieve the private encryption keys. It appears patient data was not transferred outside of the hospital's network [97].	N/A purpose was to obtain a ransom payment, not take patient data	4 Bitcoin in ransom	Friday evening, Hancock paid the four-bitcoin transaction to receive the private keys from the attackers. Critical systems were restored by Monday (1/14/2018).	Hancock validated that the files were safely recovered, encrypted files were deleted, and information systems were brought back online.

Entity, Date, and Type of Attack	Summary	Records Lost	Financial Loss/Impact	Resolution (date)	Adjustments to Cyber Risk Management
21st Century Oncology 10/3/2015-12/13/2015 Type: Data breach	It was discovered by the FBI that an unauthorized individual accessed and stole information from one of their patient databases. It was accessed by a Remote Desktop Protocol from an exchange server that contained protected health information of over two million individuals [98].	2,213,597 individuals	$2.3 million-dollar settlement	21st Century Oncology agreed to pay the Human Services' Office for Civil Rights (OCR) $2.3 million and to adopt a corrective plan of action to bring its policies up to standards of HIPAA (December 2017).	21st Century Oncology agreed to adopt a corrective action plan that included revising its policies and procedures or reporting violations of HIPAA rules, and training staff on the new policies, and conducting an organization-wide risk assessment.
Inmediata Health Group January 2019 Type: Web exposure data breach	Officials discovered that some electronic health information was left online that was exposed y a webpage that allowed search engines to index Inmediata's internal webpages. The webpage was then deactivated, and the compromised data was found to include patient names, addresses, birthdays, gender, and medical claims data. There was no evidence of copying or saving of the files [99].	1.56 million patients impacted	Facing class action investigations	Individuals were emailed beginning April 22, 2019. It was found that there were mailing mistakes, and some patients claimed to receive multiple letters addressed to other patients (ongoing lawsuits) [100].	The company has implemented new server and database procedures, as well as additional security to avoid future incidents of similar nature.
Mayfield Clinic February 2016 Type: Ransomware emails	Patients of the Mayfield Clinic of Cincinnati were sent an email that contained an attachment which downloaded ransomware onto the patients' devices. The victims were told they needed to pay a ransom to unlock the encryption. No personal or medical data was accessed, just the emails. Mayfield was able to alert many of the people on the email list the same day [101].	23,000 patients		Mayfield used a computer virus protection service, and all recipients of the email were sent information to download software to remove the ransomware virus (February 2016).	Mayfield assessed its controls and provided anti-scanning updates to employee emails. It also discontinued the distribution of electronic newsletters.
Universal Health Services September 2020 Type: Ransomware attack	Universal Health Services experienced a ransomware attack on September 27. This attack locked computers and phone systems across UHS facilities in the United States. The suspected cybercriminals use a strain of ransomware known as Ryuk. This attack forced doctors and nurses to rely on paper and pencil for record keeping, which slowed lab work. Chaotic conditions were described [102].	All United States sites were impacted; Electronic medical records were not directly impacted	$67 million [103]	The systems were quickly disconnected, and the network was shut down to prevent further destruction. The UHS IT Network was restored (10/5/2020).	The recovery and restoration process were enacted by UHG, no other future plans were explicitly announced.

Appendix II: Transportation sector

Entity, Date, and Type of Attack	Summary	Records Lost	Financial Loss/Impact	Resolution (date)	Adjustments to Cyber Risk Management
EasyJet May 2020 Type: Cyberattack	EasyJet (a low-cost airline based in England) was the target of a "highly sophisticated" cyberattack which exposed the email addresses and travel plans of about 9 million customers. Around 2,000 of the customers had their credit card details stolen [104].	9 million customers	UK's Information Commissioner's Office (ICO) is investigating whether the airline had properly protected the personal data of its customers. This will likely result in a heavy fine.	The company contacted individuals affected by the end of May 2020.	The airline got in contact with the National Cyber Security Centre, a British organization that helps companies avoid computer security threats and the Information Commissioner’s Office (British agency that reviews data breaches).
British Airways June 2018 Type: Data breach	A variety of information was compromised including log in information, payment cards, and travel booking details of about 500,000 customers [105].	500,000 customers’ information	20 million pound fine ($25.9M) from the UK's Information Commissioner’s Office (ICO) for failing to protect personal customer information.	The 183 million pound fine from the ICO was reduced to 20m due to the airline's financial circumstances. The investigators found that British Airways had failed to put sufficient security measures in place to protect its customer's data (7/2019).	British airways planned to make improvements to the security of their systems since the attack.
Lufthansa 4/1/2015 Type: Cyber attack	Hackers used a botnet to decipher customer login credentials used for the airline's online portal. Hackers then made purchases using miles on users' frequent flyer accounts. According to Lufthansa, the damage was limited to a few hundred accounts. The miles and travel vouchers that were stolen were returned to their owners. Lufthansa's IT department identified fraudulent activity and discovered 'Bots' trying to use usernames and passwords until obtaining the right combinations [38].	Several Hundred customer pages	N/A	For the accounts affected, Lufthansa has reimbursed them and changed the account numbers and contacted members to change their usernames and passwords (April 2015) [106].	The account information of all customers was changed. No other risk mitigation plan was explicitly mentioned.

Entity, Date, and Type of Attack	Summary	Records Lost	Financial Loss/Impact	Resolution (date)	Adjustments to Cyber Risk Management
San Francisco Municipal Transportation Agency (SFMTA) April 2015 Type: Ransomware attack	On Black Friday 2016, a cryptic message blocked access to SFTMA's computer screens reading "You hacked, ALL Data Encrypted." The hacker's goal was to obtain 100 bitcoins ($73,000) from SFTMA for the release of its symptoms. The malware infected about 1/4 of SFTMA's computer systems and gained access to physical ticketing machines. SFTMA was forced to give free rides to passengers that weekend, and the bus drivers resorted to hand-written routes. SFTMA denied paying the ransom and restored the systems on their own. By Sunday, the systems were restored [107].	2,000 of SFTMA's 8,000 computer systems	Agency expected loss was approximately $599,000 each day SFMTA was unable to collect fares.	By Sunday the computer systems were restored, and an official statement was released: "Transit service was unaffected and there were no impacts to the safe operation of buses and Muni Metro. Neither customer privacy nor transaction information were compromised. The situation is now contained, and we have prioritized restoring our systems to be fully operational" (11/27/2016) [108].	Not explicitly stated in prevention of future attackers obtaining this information. It was mentioned that SFMTA would reach out to staff to remind them of the impacts of clicking on links and opening emails from unfamiliar sources.
Keolis in Boston 10/10/2020 Type: Ransomware attack	Hackers obtained personal information from workers for the Massachusetts Bay Transportation Authority (MBTA) commuter rail operator, Keolis, and posted it online to attempt to blackmail the company. Keolis took the systems that were affected offline, notified law enforcement, and took steps to restore the systems [109].	Amount of employee data released not disclosed.	N/A	For impacted employees, Keolis provided credit monitoring and identity theft protection (October 2020).	Not explicitly mentioned.
LOT Polish Airlines June 2015 Type: Distributed Denial of Service (DDoS) Attack	In 2015, LOT Polish Airlines suffered a DDoS attack which caused the airline's computers to crash. It also destroyed its flight plan IT system. This resulted in a 5-hour disruption that saw 10 flight cancellations, 12 flight delays, and 1,400 passengers grounded. Flights midair were luckily unaffected [38].	1,400 airline passengers grounded [39].	N/A	No direct access to the data was obtained. The passengers affected flew on later flights or were put up in hotels by LOT (June 2015).	Thee chief executive emphasized “This is an industry problem on a much wider scale, and for sure we have to give it more attention” [39].

Entity, Date, and Type of Attack	Summary	Records Lost	Financial Loss/Impact	Resolution (date)	Adjustments to Cyber Risk Management
TFI subsidiary Canpar Express August 2020 Type: Ransomware attack	Files were stolen from TFI International's Canpar Express and leaked onto the dark web after a ransomware attack targeted this Canadian trucking and logistic company's courier subsidiaries. The ransom was not paid, and TFI was able to operate normally after a few days [110].	The leak consisted of three documents, and the company's four parcel and courier subsidiaries reported being targeted in the ransomware attacks.	The data release suggested that TFI likely decided not to pay the ransom.	TFI declined to comment further on the ransomware attack themselves. They said "We continue to meet most customer shipping needs, and we are not aware of any misuse of client information. Out of an abundance of caution we want to make our clients aware of the incident, should you be experiencing any issues (August 2020).	Not explicitly mentioned other than making the clients aware of the incident.
Maersk June 2017 Type: Malware attack	In early April, Maersk was hit by a worm named NotPetya, which locked access to systems that the company uses to operate shipping terminals worldwide. No data was lost, and ships operated normally throughout the period the systems were down. Although, for up to two days, the affected terminals could not move cargo [46].	Temporary shutdown of the Port of Los Angeles' largest cargo terminal.	$200-$300 million.	There were many workarounds to keep business going. After two weeks, business was back to normal (June 2017).	The attack was able to exploit technological, procedural, and behavioral weaknesses for Maersk to improve upon.
COSCO Shipping 7/24/2018 Type: Cyber attack	On July 24, 2018, a cyber-attack took place on the shipping agency's digital assets affecting communication in the American region. This affected the carrier's ability to communicate with vessels, customers, and marine terminals [45].	Systems in U.S, Canada, Panama, Argentina, Brazil, Peru, Chile, and Uruguay were disabled in the attack.	Caused a loss of $250-$300 million.	About 5 days after the incident, Cosco announced in a customer advisory from its Shanghai headquarters that "its network applications in the Americas had been fully recovered" (7/30/2018) [111].	Cosco mentioned it would conduct its operations via remote access, to ensure uninterrupted service to the Americas.
FedEx June 2017 Type: Petya cyber attack	A subsidiary of Fed Ex, TNT Express fell victim to the Petya cyber-attack. TNT's operations in Europe were disrupted by the attack causing significant financial loss due to lower-than-expected results in first quarter earnings [112].	No breach or data loss occurred, but the company may not be able to recover all of the systems affected in the attack.	$300 million	In August, TNT resolved to using WhatsApp for internal communication due to the email system still be inaccessible. Customer volumes were restored to expected levels (September 2017).	They mentioned the plan to instill confidence with customers so that they can fully meet their expectations.

Entity, Date, and Type of Attack	Summary	Records Lost	Financial Loss/Impact	Resolution (date)	Adjustments to Cyber Risk Management
BMW December 2019 Type: Cyber attack	OceanLotus (aka APT32), believed to be a Vietnam-backed group that targets threats, targeted BMW in 2019. This software installed a Cobalt Strike testing tool to remotely spy on machines. The hackers were blocked in December 2019. The attackers did not breach the central data center in Munich, Germany [113].	No sensitive data was leaked.	N/A	BMW's cybersecurity team was able to notice the attack and carefully monitor the group's activity, before kicking out the attackers in December.	BMW made a general statement saying, "We have implemented structures and processes that minimize the risk of unauthorized external access to our systems and allow us to quickly detect, reconstruct, and recover in the event of an incident" (December 2019) [113].

Appendix III: Election Sector

Entity, Date, and Type of Attack	Summary	Records Lost	Financial Loss/Impact	Resolution (date)	Adjustments to Cyber Risk Management
Donald Trump's Campaign October 2020 Type: Cyber attack	It was discovered that Trump's campaign website was hacked. Hackers claimed to have compromised multiple devices which gained them access to "internal and secret conversations of the president" and classified information. The hackers were seeking cryptocurrency. The site visitors were invited to donate cryptocurrency to two different funds: one labeled "Yes, share the data" and the other "No, do not share the data". The payments solicited were in Monero, which is a difficult to trace cryptocurrency. The message also said, "After the deadline, we will compare funds and execute the will of the world." Tim Murtaugh, a spokesman for the Trump campaign, confirmed that there was no exposure of sensitive data because none of it is stored on the site [114].	N/A; website was restored	N/A	The website was restored, and the Trump campaign said they were working with law enforcement authorities to investigate the source of the attack (October 2020).	Intelligence agencies closely monitored hacking groups that may attempt to break into election-related systems.

Entity, Date, and Type of Attack	Summary	Records Lost	Financial Loss/Impact	Resolution (date)	Adjustments to Cyber Risk Management
Hillary Clinton's Campaign April 2016 Type: Phishing attack	Hackers created a fake email account to send phishing emails to over 30 Clinton staffers. The emails included a link that directed to a document titled "hillaryclinton-favorable-rating.xlsx". This led to a website operated by the hackers. The hackers were able to use stolen credentials to access the Democratic Congressional Campaign Committee network, stealing data [53].	They accessed 33 DNC computers and registered for a website called DC leaks to publicize the documents.	N/A	The counsel investigating Russian interference in the 2016 election issued an indictment of 12 Russian intelligence officers in the hacking of the Democratic National Committee and the Clinton Campaign (July 2018) [54].	They worked with the FBI to safeguard the electoral voting process.
Trustwave October 2020 Type: Cyber attack	Trustwave, a global cybersecurity company, says a hacker was selling information on 186 million U.S. voters. Much of the data is publicly available, but names, email addresses, and voter registration records were found for sale on the dark web. While voter registration data is publicly available in most states, email addresses are often not a part of the public data. The databases were listed for sale by "Greenmoon2019" which would allow for malicious acts by targeting email addresses of only registered Democrats or only registered Republicans [59].	186 million U.S. voter records and 245 million records of other personal data	N/A	Trustwave said in a statement that they are committed to investigating fraud during the election. They assured that the FBI is closely working with their federal, state, and local partners to safeguard the voting process (October 2020).	Working with FBI to safeguard the electoral voting process.
FireEye 12/8/2020 Type: Cyberespionage	One of the largest cybersecurity companies in the United States, FireEye, said that on Tuesday, December 8th, foreign government hackers with "world-class capabilities" broke into their network and stole tools that they use to test the defenses of thousands of customers including federal, state, and local governments. FireEye's CEO, Kevin Mandia, released in a statement that the attacker "primarily sought information related to certain government customers." Mandia also stated that he has concluded that the attack was completed by a nation with "top-tier offensive capabilities" [60].	Accessed certain Red Team assessment tools used to test customer security	Potential loss of customers. Stock price went down after the reveal of the attacks.	FireEye is investigating the attack with the FBI and Microsoft Corp. They are publishing information that can help to neutralize the tools that were stolen (December 2020 and ongoing) [115].	FireEye is working to innovate and adapt to protect customers from threat actors.

Entity, Date, and Type of Attack	Summary	Records Lost	Financial Loss/Impact	Resolution (date)	Adjustments to Cyber Risk Management
Obama and McCain presidential campaigns 2008 Type: Cyberespionage through a phishing attack	The United States traced the massive cyberespionage operation against the 2008 presidential campaigns of Barack Obama and John McCain back to the People's Republic of China. The goal of the campaign intrusion was to export internal data from both campaigns, including internal position papers and private emails to gain leverage with the winner of the election. The intrusion into the campaign's computer networks continued for months after first being detected by the FBI in the summer of 2008. The attack was delivered by a "phishing" email that contained an attachment with sophisticated malware that infiltrated throughout the Obama campaign's computer system [49].	A large number of internal files were compromised	Theft of intellectual property costs the U.S. money. A report from the former Intelligence Director Blair and the former U.S. Ambassador to China estimated this theft (mostly from China) to be costing the U.S. around $300 billion per year.	The campaign dispatched a computer security team from Kroll Advisory Solutions to Chicago to cleanse the infected computers. Chinese officials have denied any role in cyber-attacks against the U.S. government and private enterprise (2013) [49].	More cyber security measures were taken and improved upon since this attack.
Emmanuel Macron's campaign May 2017 Type: Cyberattack (releasing data and spreading disinformation)	Two days before the final round of the French presidential elections, data hacked from Macron's presidential campaign team were released online. Nearly 14.5 gigabytes of emails, personal and business documents were posted to the site Pastebin through links to more than 70,000 files. Officials from Macron's party said that the attackers mixed fake documents and authentic ones to create confusion and misinformation [116].	14.5 gigabytes of documents and emails	N/A	The attack failed to influence the electoral process. Macron still won the election. Factors such as anticipation and reaction by the Macron campaign staff, government, and civil society and mainstream media can be attributed to resisting the attempted Russian influence (May 2017) [68].	The increase of further prevention of "information laundering" in the media due to the resilience of the French media environment [68].

Entity, Date, and Type of Attack	Summary	Records Lost	Financial Loss/Impact	Resolution (date)	Adjustments to Cyber Risk Management
Estonian Government April 2007 Type: Cyber-attack and disinformation	In 2007, the Estonian government decided to move the Bronze Soldier, a symbol of Soviet oppression. This decision led to protests which were exacerbated by false Russian news reports that claimed the statue was being destroyed. In this rioting, 156 people were injured, one person died, and 1,000 people were detained. The day after the physical destruction, cyber-attacks affected online services of Estonian banks, media outlets, and government bodies. The massive spam that was sent by botnets generated large amounts of online requests, overloading servers. Estonians were unable to use online banking services, government employees were unable to email, and newspapers could not deliver news. The attacks came from Russian IP addresses and Russian language was used. The attacks continued until May 19, 2007 [67].	Estonian governmental, political, and financial websites and e-services were targeted.	Estonia faced lost productivity, opportunity cost, remediation, and acquiring alternative web services at emergency rates are estimated to have cost billions of Euro.	The attacks ceased on May 19, 2007. In January 2008, the Estonian government indicted one of the responsible hackers (5/19/2007) [67].	In May 2008, the Estonian Ministry of Defense implemented a National Cyber Security Strategy [66].