City University of New York (CUNY)
CUNY Academic Works

Student Theses | John Jay College of Criminal Justice

Winter 8-9-2022

The Economic Impact of Cyberattacks in the United States

Habibullah Asadi
CUNY John Jay College, hothab@yahoo.com

How does access to this work benefit you? Let us know!

More information about this work at: https://academicworks.cuny.edu/jj_etds/255
Discover additional works at: https://academicworks.cuny.edu

This work is made publicly available by the City University of New York (CUNY).
Contact: AcademicWorks@cuny.edu

The Economic Impact of Cyberattacks in the United States

A Thesis Presented in Partial Fulfillment of the Requirements for the Degree of

Master of Arts in Criminal Justice

John Jay College of Criminal Justice

City University of New York

Habibullah Asadi

Summer (Spring) 2022

Abstract

In recent years, the global economy has been beset by cyber-attacks. These events disrupt business and governmental operations, large and small, and include broad-horizon attacks on infrastructure and pointed network takeovers. The attacks can include malicious online activities directed at stealing financial and intellectual property or, manipulating, destroying, and denying access to critical information. Despite increased awareness of these challenges, the victimization of private and public networks continues, and the economic impacts mount daily. This research will present the economic impact of cyberattacks on United States businesses and governmental agencies.

The Economic Impact of Cyberattacks in the United States

Introduction

In the past four decades, the rise of cyber technologies has been met by action. Most public and private organizations adopt information security systems and protocols to help run their operations. Information security systems have become an integral part of the U.S. economy, with data security personnel and new routines helping to establish a seamless flow of operations across industries. The advancement of cyber technologies has also been met with trepidation owing to the new threats introduced by malicious actors. Cyber threats are serious and costly. The growth of cyber-attack mechanisms has put the U.S. economy at risk. Therefore, we need a standardized framework to help assess the economic impacts on American private and public organizations so that enterprises can adopt minimal standards for cybersecurity. Understanding the economic impact of cyber-attacks on the U.S. economy motivates organizations to prioritize their security. This research examines the economic impacts of cyber-attacks in the U.S. and discusses the lessons learned from these attacks and proposes a standardized assessment strategy for enterprises to follow. The ultimate goal is to achieve a higher standard of cybersecurity practice that can help enterprises to reduce the economic impacts of cyber-attacks.

Two cases demonstrate the severe impacts that cyber-attacks cause to the U.S. economy: The 2012 U.S. Office of Personnel Management data breach and the May 2021 Colonial Pipeline ransomware attack.

In two episodes, one in 2012 and the other in 2015, the U.S. Office of Personnel Management (OPM) suffered data breaches. In the 2012 data breach, hackers made away with the personal information of federal employees, including their social security numbers, assignments, and training information. The OPM also confirmed that the usernames and

passwords of applicants for background investigation were also stolen. The second round of data breaches involved the loss of 19.7 million records of current, former, and prospective employees (Finklea, 2015). With the identities of federal employees compromised, it was difficult for them to perform their work roles within and outside the U.S., especially where these roles required a high level of discretion. The slow response in identifying the sources of the OPM cyber-attack further complicated the employment scenario for the federal government. The attack causes a review of OPM's cyberinfrastructure to prevent future cyber-attacks. These reviews and the changes after that translated into costs that the taxpayer would pay to ensure that the OPM gets back on its feet and is secured from future threats.

By studying past cyber-attacks and their economic impacts, the present research seeks to provide impactful data that businesses and governmental agencies can use to manage to avoid the pervasive effects of cyber-attacks. There is a need for a standardized framework that helps understand the scale of economic impacts while pointing toward the directions that could be taken to minimize these impacts. Below is a discussion of how the OPM and Colonial Pipeline cases reveal the economic impacts of cyber-attacks.

Literature Review

The past decades have seen a heightened interest in cybersecurity literature, with most scholars focusing on the unique threat landscape of cyberattacks as well as the tools and mechanisms that attackers use to execute their hidden agendas. These unique studies give rise to ideas and opinions that could be relied on to create a standardized framework that helps determine the economic impacts of cyber-attacks. The works that document cybersecurity issues within the U.S. and beyond show how important it is to develop cybersecurity literature and practice. This section focuses on how various literary sources have assisted in conceptualizing

cyber security threats and why we need to develop a standardized framework for studying and analyzing these threats.

A report produced by the Homeland Security department has warned of numerous sources from which cyber-threats could arise. According to HSDL (2018), a wide range of malicious actors are actively trying to jeopardize cyberinfrastructure in the U.S. These actors have different motivations for their attacks, which need to be studied and framed to provide new insights into cybersecurity management. One of the threat sources for cyber-attacks detected within the U.S. is nation-states. According to DNI (2017), the main actors with respect to cyber threats in the U.S. are Russia, China, Iran, and North Korea. Investigations of the OPM breaches in 2012 and 2015 show links to China (Finklea et al., 2017), even though these allegations have not been officially confirmed. Nation-states' interests in cybersecurity within the U.S. arise from motivators such as industrial espionage. For instance, the attack on OPM amassed data on federal employees and the assignments they were working on. With this data, it is easier to initiate strategic defenses and diplomatic actions that could hurt the U.S. economy.

Corporate competitors and hacktivists are identified as some of the main threat sources for private and public businesses. Corporate competitors sometimes seek illegal access to intellectual property that they could use to compromise each other's operations. These unhealthy competition practices result in direct targets of companies' information systems in the form of cyber-attacks. Therefore, it becomes imperative for businesses to shield their information systems to ward off aggression from their competitors. On the other hand, hacktivists are private individuals who have a political agenda against organizations in private and public domains. In a politically motivated context, hacktivists seek to cripple information systems belonging to businesses and government agencies. These forms of actions tend to undermine the integrity of

information systems while exposing the affected organizations to the rueful effects of cyber-attacks.

Other threat sources include organized criminal groups, opportunists, and company insiders. Organized criminal groups seek to benefit from the proceeds of cybercrimes and could go to varying lengths to bring down information systems. According to HSDL (2018), organized criminal groups profit from the sale of personal identification information (PII) on the dark web and ransomware payments collected from system infiltration. The motivations for profit could be situated within the OPM attacks as well as the Colonial Pipeline ransomware attack. In the OPM case, selling confidential employee data on the dark web shows there is money to be made from stolen PII. In the Colonial Pipeline case, the hacker group behind the attack was motivated by profits based on how the attack unfolded and ended. Organized criminal groups have the advantage of diverse skill sets and financial backing, allowing them to plan and execute cyberattacks.

On the other hand, opportunists are termed amateur hackers who have a desire for notoriety. Regardless of the motives of opportunists, organizations should not underrate the impacts that random acts of cyber violence could have on the operations of an organization and the economy of the U.S. These attacks could come even from disgruntled employees or ex-employees looking for revenge or financial gain by selling the secrets of an organization to malicious actors. Understanding the motivations of these actors in advance helps in the preparation of cyber defenses and policies that help minimize the potential impact of cyber-attacks on the performance of an organization. Additionally, considering multiple threat sources helps build preparatory strategies to limit the damage from cyber-attacks.

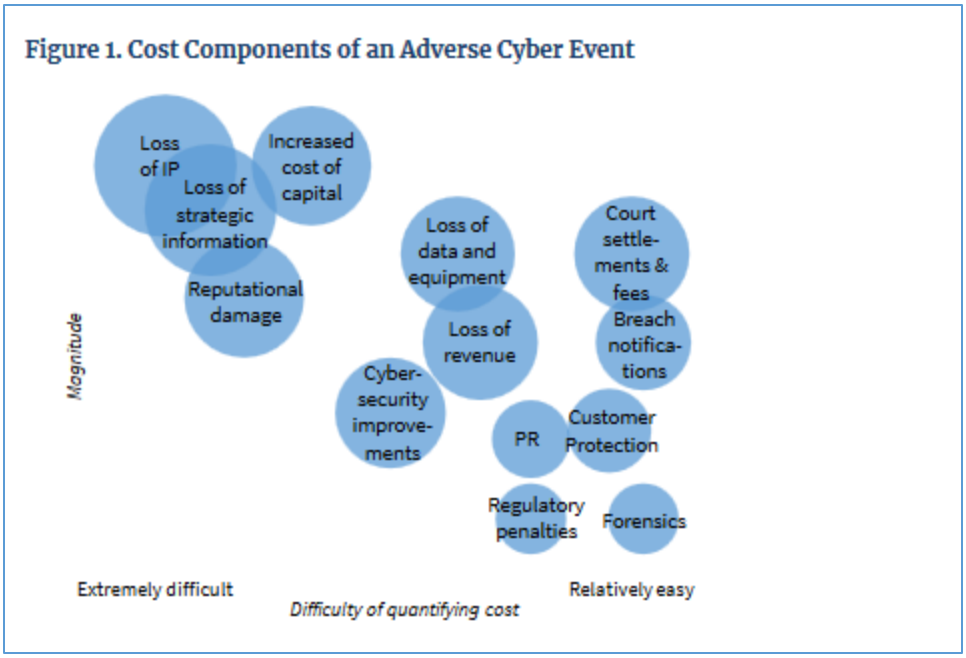


Figure 1. *Quantifying the Costs of Cyber-attacks*

HSDL, a leading example in this field, has already put forward a cost framework to evaluate the impact of cyber-attacks which could help organizations determine the extent of damage they have suffered from these attacks. Figure 1 above shows the HSDL framework for quantifying financial impacts of cyber-attacks. According to HSDL (2018), it is easier to quantify the costs of forensics, regulatory penalties, breach notifications, and P.R., among other cost areas, which could aid in understanding the pronounced effects of cyber-attacks. However, as attacks become more sophisticated and widespread, revenue losses, cybersecurity improvements, and data losses create uncertain situations for victim organizations. HSDL (2018) notes that in the most extreme cases, quantifying the loss of intellectual property, reputational damage, loss of strategic information, and increased cost of capital makes it difficult for businesses to recover from the costs of cyber-attacks. Recognizing these cost areas helps justify the expenditures that businesses and government agencies must engage in to respond to the

adverse effects of cyber-attacks. This study will use these examples OPM and Colonial as a base for my own study to develop further knowledge on the costs of cyber-attacks.

Some scholars have studied the impact of cyber-attacks by studying specific sectors within the U.S. economy. Eisenbach, Kovner & Lee (2021) focused on how disruptions to the wholesale payment networks of banks could lead to economic losses. The researchers observed that impairment to any of the five most active U.S. banks could affect 38 percent of payment networks. Eisenbach, Kovner & Lee (2021) also note that banks' responses to uncertainty through liquidity hoarding could result in foregone payments activity, reaching more than 2.5 times the daily GDP. Duffie & Younger (2019) further note that high-value payments and settlement systems remain a natural candidate for a malicious attacker's intent on inflicting the largest possible damage to financial systems and the broader economy. These effects are more specific in terms of the adverse effects on the economy due to cyber-attacks. Such observations make a case for due diligence and other strategies to pursue when building strong cyber defenses.

To determine the market reactions to cyber-attacks, assessing the short and long-term effects of cyber-attacks on stock prices provides an insightful way to examine the economic threats. Kvochko & Pant (2015) observed that in the aftermath of data breaches, the stock prices of businesses slightly decrease and then quickly recover. However, the slight decreases in stock prices of businesses affected by cyber-attacks mirror losses that affect the financial stability of the affected organizations. For instance, in a cyber-attack on Target, the business still recorded losses amounting to $236 million despite recovering from the attack. The same impacts were studied by Hillary et al. (2016) when examining the impacts of cyber-attacks on Sony and Home Depot. It is unclear whether malicious actors foresee the damages they could inflict on organizations. Private businesses and government agencies need to build a framework to

anticipate the impacts of cyber-attacks and make plans to cover these effects. Kvochko & Pant (2015) note that the lack of sufficient information about the breaches and the tools used in the process could make it difficult to build accurate reflections of the potential effects of cyber-attacks. The present research will discuss avenues that organizations can leverage to develop an accurate assessment of cyber-attacks on their operations.

In some of the most extreme cases, attackers destroy data, files, and hardware, which are pivotal to the operations of a business. The HSDL (2018) framework recognizes data and operational disruptions and some of the common cost areas that organizations need to consider in evaluating their cyber-attack impacts. The DarkSeoul malware – detected in computers in South Korea – and the Corkow malware – detected in Russia – have been used in the past to erase data from information systems (Kopp, Kaffenberger & Wilson 2017). The loss of data can be quantified in economic terms by evaluating the financial value of the data and its advantage in sustaining the economy. In evaluating impacts on the economy, a forward look at the bigger picture should consider how data losses force changes due to service and business continuity measures.

The above review provides a summary of the literature that describes the state of cybersecurity in the U.S. These pieces of literature provide a background for the current research, which is the first of its kind. Based on the analysis of the impacts and mechanisms of cyberattacks described above, the next sections build on the review of the Colonial Pipeline and OPM attacks by highlighting the unique impacts of the attack. No study has analyzed two attacks in parallel by comparing them to existing literature. No actual dollar amount of damage has been produced from studies on cyber-attacks due to the lack of cost measurement area that can be used

to locate the exact amount of damages. The present study aims to produce criteria that can be used to calculate the financial losses due to cyber-attacks.

Methods /Materials

This research focuses on two particular cases, OPM and Colonial Pipeline, to study the economic impacts of cyber-attacks on the U.S. I was able to investigate these two cases based on available literature and built a systematic framework for analyzing the economic effects of cyber-attacks. The research process considers secondary literature produced by scholars and government agencies to map the effects of cyber-attacks on the U.S. economy from the lens of the selected case studies. This literature provides a lens through which the Colonial Pipeline and OPM cyberattacks can be analyzed to situate their impacts on the U.S. economy and build a framework for future use in cybersecurity analysis. The reason for choosing the Colonial Pipeline and OPM attacks is due to their scope. The Colonial Pipeline attack embodies a direct impact on the economy given the critical role that gas plays in economic continuity. The OPM attack, on the other hand, was a national-level incidence and its analysis could reveal the economic impacts of cyber-attacks from a wider perspective.

Criteria for Selecting Research Articles

The research articles considered for the systematic literature review within the present research context are all dated after 2010. The rationale for selecting this timeline is that the most current articles on cyber-attacks within the U.S. provide relevant data regarding the current cyber threats. Additionally, the ever-evolving nature of cyber-attacks means that one has to retain the most current evidence to gain more impactful insights into the threat landscape of today's cyber-attacks. The articles considered for this research include empirical analyses of evidence from

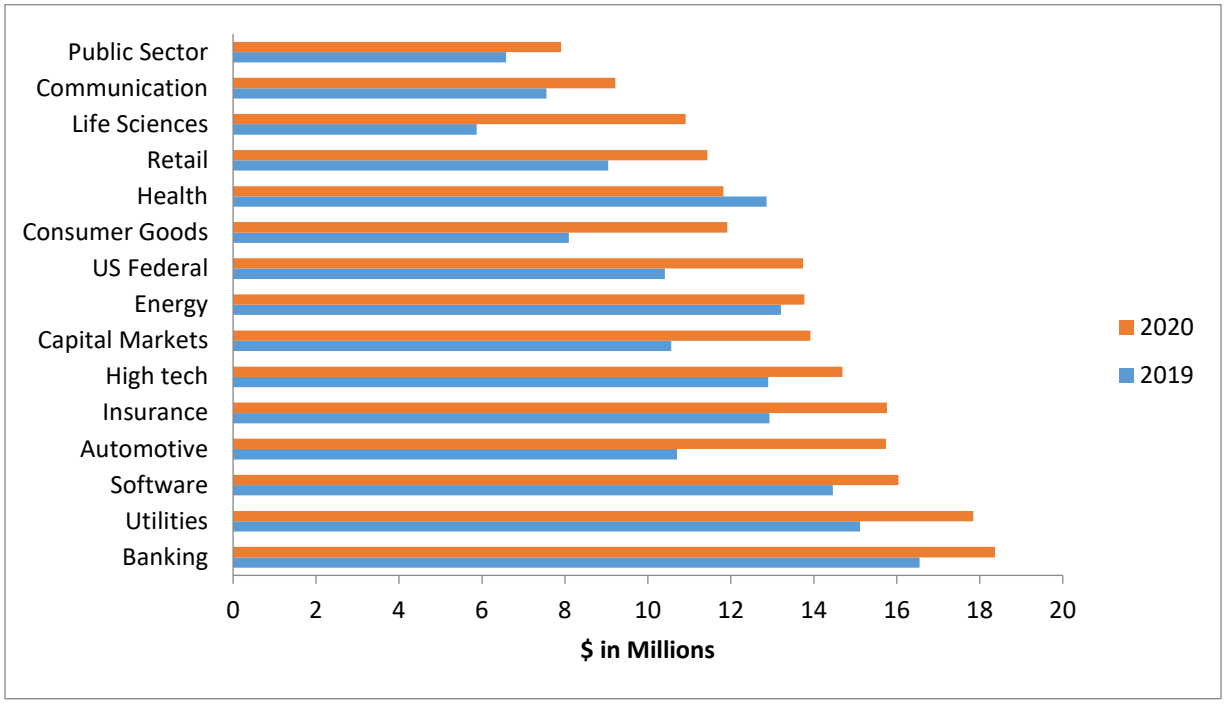
previous cyber-attacks. This evidence will help formulate and present a comprehensive overview of the economic impact of cyber-attacks and why a standardized framework is necessary.

The cost of cyber-attacks – Industry Analysis

In the literature review for this research, Eisenbach, Kovner & Lee (2021) and Duffie & Younger (2019) studied the impact of cyber-attacks on the financial sector, focusing on the wholesale payment systems that help to run payment systems. While the banking industry remains an integral part of the U.S. economy, there are also other areas of the economy where cyber-attacks could potentially cause a detrimental impact. Graph 1 below shows an overview of some of the cost effects of cyber-attacks on U.S. industries. The results, documented by Bissell & Ponemon (2020), corroborate Eisenbach, Kovner & Lee's (2021) study that conceptualizes the banking sector as one of the most vulnerable industries to cyber-attacks.

Graph 1:

Average Annual Cyberattacks Cost in the United States Economic Sector in 2019 and 2020



The authors considered a cyber-attack as an attack on an organization's information system and used this definition to describe their results. The results indicate that the U.S. banking sector spent $18.35 million on cyber-related incidents in 2020. The figure represents a slight increase from 2019 costs, which stood at $16.55 million. The increased spending on cyber-related incidents could mean that cyber incidents are increasingly burdening banks. The continued prevalence of these trends could make it difficult for banks to play their roles in regulating economic performance.

From the results shown in the graph above, utilities, software, and automotive industries follow banking regarding the amounts spent on mitigating cyber-attacks. The attack on Colonial Pipeline could be contextualized within the utility sector, with the sudden halts in gasoline transportation having the potential to affect other critical sectors that depend on gasoline. For instance, the failed transportation of gasoline to the southeastern U.S. could have halted food supplies made through trucks. The payment that Colonial Pipeline made to the hacker group could be understood as a possible way of mediating the adverse effects that the ransomware attack could have caused if it had lasted several hours longer.

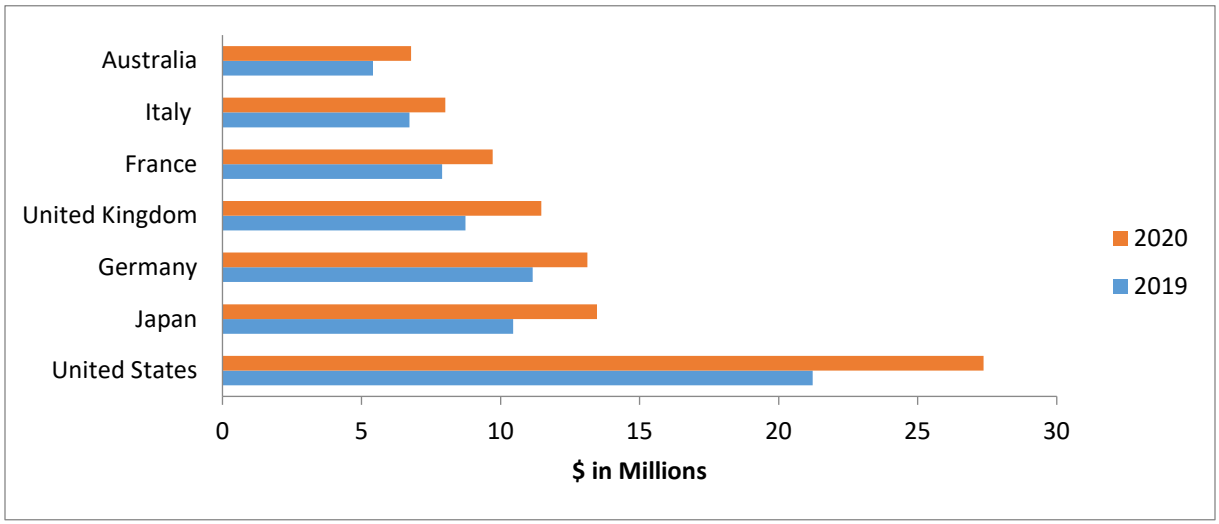
The results from the graph also summarize how government agencies were affected by cyber-attacks. According to Bissell & Pinemon (2020), the government reported $6.55 million in costs related to cyber-attacks in 2019 and $7.91 million in 2020. The attack on OPM provides the context for understanding how a cyber-attack could disrupt the operations of a government agency. The results by Bissell & Pinemon (2020) confirm the assessments made by Finklea et al. (2015) based on the perceived impact of cyber-attacks on the financial performance of government agencies.

Grouping the Consequences of Cyberattacks

The damages caused by cyberattacks to the U.S. economy can be understood by examining individual consequences on operational areas of business and government agencies. Bissell & Pinemon (2020) identified four main areas that could cause a decline in the economy of the U.S. The four main areas include business disruption, information loss, revenue losses, and equipment damages.

Graph 2:

The Cost of Cyberattacks by Country



In terms of business disruptions, cyber-attacks halt the operations of critical sectors based on the techniques, tools, and strategies employed by attackers. To this effect, the costs of business disruptions due to cyber-attacks in the U.S. were established at $13.0 million in 2018 (Bissell & Pinemon, 2020). These costs only provide an overview of formally reported cases. Still, the disruptions to energy sectors could easily affect sectors of the economy that depend on energy to facilitate their operations. The Colonial Pipeline case provides evidence of how the disruption to an energy sector could warrant urgent actions to help alleviate the perceived costs of cyber-attacks.

According to Bissell & Pinemon (2020), researchers observed increments in revenue losses and equipment damages in the last two years. Again, any direct hits to a business that supports the flow of service in the economy could have untold effects on the long-term financial performance of individual businesses and the economic outputs of countries. Kitchen (2019) noted that cybercriminals costed the global economy more than $6 trillion annually in 2021, up from $3 trillion in 2015. The scale and magnitude of these attacks are important in determining how resilient the economy can stay amidst frequent attacks. Kitchen (2019) uses the term economic warfare to define the steps that individual businesses and government agencies need to take to maintain the integrity of their operations while stimulating economic performance.

The economic impacts discussed above translate to GDP losses when viewed closely. The loss of business revenues due to disruptions caused by cyber-attacks undermines the taxes that businesses remit to state and federal state governments. Additionally, attacks on government agencies reduce the capacity of these agencies to perform actions that help to insulate the economy from artificial crises. Furthermore, cyber-attacks could exacerbate the already difficult economic conditions present in the U.S. The results show a continuity in the cumulative effects of cyber-attacks on the U.S. Year-over-year increments in the scale and complexity of cyber-attacks pose a threat to the sustainable development of the economy. The next section discusses the possible effects of the noted results and the potential directions that businesses and government agencies could take to understand the threat posed to the economy of the U.S. These steps would help map the long-term impact of these threats on the integrity, confidentiality, and availability of critical services in the U.S. economy.

Results

From the analysis of research data on the effects of cyber-attacks on the U.S. economy, a wide range of results has been established that help explain the need for concerted efforts in building strong cyber systems. The content analysis results have been grouped into themes, which helps to provide an overview of the impact landscape on the U.S. economy. The results were drawn from key findings in scholarly articles and insights provided by scholars to help paint a clear and accurate picture of the negative effects of cyber-attacks. There is a need to develop minimum standards for cyber-security based on cost analysis of cyber-attacks.

Multi-factored risk analysis for economic effects of cyber-attacks

Colonial Pipeline and OPM cyber-attacks provides a comprehensive summary of the economic risks of cyber-attacks. The Colonial Pipeline case shows how an attack on critical infrastructures such as gas and energy systems could block the economies of many states at once, even when the states are not the recipients of the cyber-attack. On the other hand, the OPM case shows how potential leakages of confidential government information could result in repair costs and damage control expenses for the government. While understanding these risks is necessary, there is a need to evaluate the costs of these risks to provide actionable points that can be relied on streamline security in government agencies and private businesses in the U.S. A multi-factor risk analysis of organizations based on the value of the information owned by a business and the I.T. assets contained by the organization. Some of the risk areas to consider are described below:

- **Number of internet-ready desktops:** These risk areas would determine the percentage of the organization that is outward-facing towards the internet and to what extent a cyber-attack could break down operations. For example, in the Colonial Pipeline and OPM

case, the respective entities would have to determine the number of computers that provide external links to the organization to gauge the levels of protection needed.

- **Number of email accounts:** The number of email accounts helps determine the points of entry that could be exploited to compromise the network's integrity. Email accounts in the Colonial Pipeline case and other ransomware attacks provide means for phishing, spamming and other types of attacks that could be used to distribute malware.
- **Number of websites:** The number of websites being run by the organization is an important indicator of the level of work that needs to be done to attain all-around protection of the business. The number of websites run by OPM or linked to it would provide a summary of the communication lines that need to be authenticated to ensure that only authorized users access and run these websites.
- **Number of datalinks to the net:** The number of links to the internet helps draw a perimeter around the organization that could determine the intensity of protection mechanisms for multiple connections. These data links would have assisted both Colonial Pipeline and OPM in sealing pathways for ransomware and any other attack that tried to gain access to confidential data.
- **Number of servers with open ports to data-sharing peers**: The number of ports that remain open to data-sharing peers could help analyze peripheral risks and how peers could affect the integrity of an organization's network. The number of open ports applies to the OPM case, mostly given the high number of informational channels it needs to open for federal bodies who need to access data about their employees.
- **The total daily value of income:** Analyzing the total daily value of income points towards the potential losses that could be incurred based on the length of a blackout

caused by a cyber-attack. The total daily value of income for Colonial Pipeline would help to alert the organization of the losses it would incur if operations are stalled due to cyberattacks.

- **The total daily value of accounts payable**: The daily accounts payable indicates the level of disruptions that should be anticipated and the actions that should be taken to maintain payment commitments in the event of a cyber-attack. Accounts payables at Colonial Pipeline would signal how much the business would need to sustain payments to different entities in the event of an attack. This risk area would help Colonial Pipeline and other businesses determine how much money they need to sustain operations.
- **Total debt load**: Total debt load as an area of risk evaluates how an attack could add to the debt load while establishing alternative sources of finance to aid in recovery from attacks. The debt load for Colonial Pipeline would help it to calculate how long it would take before creditors start to apply pressure and how they would tackle the negotiations for debt deferrals.
- **Available cash:** The available cash at any time in the business shows the starting point for economic recovery and stipulates the key areas where cash should be committed in the event of a cyber-attack. The available cash at Colonial Pipeline at any point in time would help the business to determine which areas to prioritize in recovering from an attack. Priority areas could be payments to suppliers, restoration of systems, or covering daily operational expenses, among other spending areas.
- **Total insurance coverage available**: The total cyber insurance coverage is an area of analysis that indicates the levels of risk mitigation and the funds potentially available to recover or restart operations after a cyber-attack. The total insurance coverage for

Colonial Pipeline would need to consider both infrastructural and data losses and the amount of compensation they expect to return to normal operations.

The above points provide a mix of infrastructure and cost considerations that go into multi-factor risk analysis processes. Still, there is a need to delineate the typical costs that an organization could incur as part of its daily information security management operations. These costs help provide directions on responding to a possible cyber-attack. The cyber-attacks on Colonial Pipeline and OPM generate two unique landscapes for understanding the economic risks of cyber-attacks. However, when responding to these attacks, general cost areas need to be considered as part of evaluating the economic implications of recovery processes. The costs identified with respect to both cases are as follows:

- **Total endpoint security subscriptions –** These are solutions that Colonial Pipeline and OPM would need to adapt to improve their security status in anticipation of future attacks.
- **Year-over-year threat protection hardware costs –** Apart from software solutions to boost their systems, Colonial Pipeline and OPM would need to acquire hardware such as modern firewalls, routers, switches, and intrusion prevention and detection systems to help upgrade their security.
- **Year over year threat protection hardware/software maintenance costs –** These are costs that apply in maintaining I.T. systems, both hardware and software, to ensure that they are up to date with the latest security standards. The costs identified here include repair, update, and service costs.
- **Annual salaries for InfoSec/Compliance personnel –** OPM needs to comply with NIST standards and other federal standards that provide the basis for strong

operational security. It would need to adopt compliance personnel on a consultancy basis to test and determine if their systems are compliant. For Colonial Pipeline, hiring compliance personnel is voluntary but is still recommended. These processes would attract new cost areas regarding salaries, wages, and bonuses paid to compliance personnel.

- **The annual cost of subscription service for an emergency response contract -** Colonial Pipeline, OPM, and any other organization need to pay subscriptions for emergency response contacts to improve their capacity to react to threats. These costs increase the economic impact of handling cyber-attacks.
- **Annual costs of offsite and cloud backup solutions –** Both OPM and Colonial Pipeline need backup and offsite solutions for their data and mirror versions of their systems, respectively. Backing-up data in the cloud would attract new costs in information security, while offsite systems would require additional investments in the form of infrastructure costs.
- **Annual insurance costs for data loss and consequential damage coverage -** Colonial Pipeline and OPM would need to consider insurance plans for data losses and damages that could result from cyber-attacks. These considerations would mean paying extra costs in premiums as part of cybersecurity strategies.

The above risk analysis areas provide potent factors that could aid a government agency or a private business draft a risk mitigation plan. Using the list above provides businesses with specific actions and financial commitments to help improve business outcomes after cyber-attacks.

The above factors help an organization calculate its risks and take steps to mitigate these risks. However, organizational managers need to understand that risk environments are ever-evolving. A calculation of a risk today often fails to produce the same results if the risk is calculated after six months. When the calculation of risk goes beyond the figure initially conceived, the company's values could go down, and the business needs to spend more on risk mitigation costs. For instance, I.T. precautions and compliance with new rules and regulations regarding security generate new cost areas that should be addressed in concurrent risk management budgets. Continuous measurement and assessment of risks are needed to help organizations adjust accordingly to the increasing or decreasing threats from cyber-attacks.

Discussion

The results posted in the previous section show industry analyses of cyber-attacks and their potential impacts on the economic health of businesses and government agencies. The results highlight a need for urgency in handling cyber threats and vulnerabilities. The repeat OPM attack in 2015 showed failures by the government agency to seal the loopholes that attackers had used in 2012 to compromise the records of federal employees. Furthermore, the year-on-year increases in costs for cyber-responses by businesses in the U.S. indicate the delicate balance that exists between threat analysis and mitigating strategies to ward off the effects of cyber-attacks on the economic performance of the U.S. CISA (2020) observes the need for a repeatable methodology that can be used for a tailored business impact analysis. These methodologies are found in the National Institute of Standards and Technology (NIST) guidelines. NIST Special Publication 800-30 highlights the pathways businesses and government agencies should take to assess cyber-risks (Al Fikri et al., 2019). However, the NIST standard on risk assessment lacks an avenue for understanding how cyber-attacks could affect the economy.

The roles of government agencies and public and private agencies in the economy should be mapped out to assert response strategies during cyber-attackers. One of the prime examples in recent news is the Colonial Pipeline and how the FBI assisted in the coordination of ransom payments. Collaboration between businesses and government agencies could help alleviate the threats posed by cyber-attacks. Still, one would disagree with paying ransomware to attackers under the premise that meeting the demands of hacker groups only encourages rather than prevents cyber-attacks. Romanovsky et al. (2019) note that there is a need for a more involved process in conducting detailed business impact analysis for systems of interest. Adjustments to the NIST framework need to be made to alert key businesses to apply stringent measures to mediate the widespread impacts of cyber-attacks.

The present discussion reveals complex issues in cyber-security planning and analysis that businesses and government agencies need to consider when drafting their future cyber-responses. The results affirm the limited understanding of the economic effects of cyber-attacks, with the most focus being on the numbers. Organizations need to avoid treating cyber-attacks as isolated events and see the attacks as part of a network of effects that could be stopped through preventive measures. Government agencies need to consider how an attack could affect their strategic role in the economy and take steps to prevent new attacks. The repeat attack on OPM signals how a limited understanding of the economic effects of cyber-attacks could lead to complacency and allow attackers a greater sphere of influence in the economic performance of government agencies and the economy at large.

The need for a standardized framework is further affirmed by the fact that adhering to regulatory requirements attracts soft costs, especially when assessing risks in a system. Private businesses and government agencies need to employ the services of security analysts and

develop tools that would help build strong defenses in their systems. The addition of costs related to compliance is part of the economic effects that need to be considered when evaluating the possible impacts of cybersecurity. Excluding these costs could lead to backlashes in terms of fines and lost revenues used to settle the damages caused by cyber-attacks. The fines could result from political pressure as the public demands answers for disruptions caused by cyber-attacks. A standardized process for evaluating the economic effects of cyber-attacks needs to go deeper and identify the soft costs related to compliance that could undermine security efforts within an organization.

Additional cost areas that need to be included in the standardized framework for evaluating cyber-attacks include the costs of acquiring cyber-insurance and anti-virus services. These services are contingencies that help reduce levels of damage and losses that could be incurred from cyber-attacks. As private businesses and government agencies work toward streamlining their cyber infrastructure, they need to adopt measures such as intrusion detection and prevention services, whose prices are on the rise. The costs of cyber defenses have become difficult to sustain. They continue to pile pressure on private businesses and government agencies that have to make accommodations within their budgets, which are sometimes insufficient in meeting cybersecurity needs.

Conclusion

The OPM and Colonial Pipeline cyber-attacks provide subtle examples that affirm the need for critical insights on the sustainability of cyber defense strategies. The present research dissects the economic landscape of cyber-attacks by showing how businesses could suffer if they do not plan for their protection against adverse cyber events. The results documented here provide insightful metrics and discussions that businesses and government agencies can use to

assess their cybersecurity plans and develop better response plans. However, the present research is limited because it does not consider any primary data. Future research around this area of study should try to determine how individual cyber-attack scenarios could adversely affect the economy of the U.S. using a top-down approach. Such developments would aid in building formidable data sources and practical frameworks that can be used to produce stellar results in cyber defense strategies used by a wide range of businesses and government agencies.

References

Bissell, K. & Ponemon, L. (2020). The Cost of Cyber Crime. *Accenture Security*. Retrieved from https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.

CISA. (2020). Costs of a Cyber incident: Systematic Review and Cross-Validation. Retrieved from https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf.

DNI (Director of National Intelligence). (2017). World Threat Assessment of the U.S. Intelligence Community. Retrieved from https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf.

Duffie, D. & J. Younger (2019). Cyber runs. *Hutchins Center Working Paper 51*, Brookings Institution.

Eling, M., Elvedi, M., & Falco, G. (2022). The Economic Impact of Extreme Cyber Risk Scenarios. *North American Actuarial Journal*, 1-15.

Eisenbach, T. M., Kovner, A., & Lee, M. J. (2021). Cyber risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics.*

Al Fikri, M., Putra, F. A., Suryanto, Y., & Ramli, K. (2019). Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in a profit-based organization: A case study of ZZZ information system application in ABC agency. *Procedia Computer Science*, *161*, 1206-1215.

Finklea, K., Christensen, M. D., Fischer, E. A., Lawrence, S. V., & Theohary, C. A. (2015, July). Cyber intrusion into U.S. office of personnel management: In brief. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

Hilary, G., Segal, B., & Zhang, M. H. (2016). *Cyber-risk disclosure: Who cares*? (Georgetown McDonough School of Business Research Paper No. 2852519). https://doi.org/10.2139/ssrn.2852519.

HSDL (2018). The cost of malicious cyber activity to the U.S. economy. Retrieved from https://www.hsdl.org/?view&did=808776.

Hobbs, A. (2021). *The colonial pipeline hack: Exposing vulnerabilities in U.S. cybersecurity*. SAGE Publications: SAGE Business Cases Originals.

Kitchen, K. (2019). A major threat to our economy – three cyber trends the U.S. must address to protect itself. *The Heritage Foundation*. Retrieved from https://www.heritage.org/cybersecurity/commentary/major-threat-our-economy-three-cyber-trends-the-us-must-address-protect.

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). *Cyber risk, market failures, and financial stability*. International Monetary Fund.

Kvochko, E., & Pant, R. (2015, March 31). Why data breaches do not hurt stock prices. *Harvard Business Review*. Retrieved from https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity 2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001.