# Combating Ransomware: Understanding How Cyber Insurance Influences Hospital Cybersecurity

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

**Feyona Zhang**

Spring 2025

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Sean Murray, Associate Professor of STS, Department of Engineering and Society

*There are only two types of companies: Those that have been hacked and those that will be hacked.*

— Robert S. Mueller, III, former Director of the FBI

## I. Introduction

The United States Department of Justice categorizes ransomware on the same level of concern as terrorist attacks (Yilmaz et al., 2023). Ransomware is a form of malware that locks a person out of their device or system until a ransom demanded by the attacker is paid. In recent years, attacks have evolved to have an additional "double extortion" phase where sensitive information is exfiltrated for ransom (Cartwright et al., 2023). The damage from a ransomware attack can be devastating when it targets critical infrastructure such as utilities and hospitals. In the 2021 Colonial Pipeline incident, ransomware shut down the service of the largest petroleum pipeline in the United States for five days, increasing the price of gasoline for the East Coast by four cents. The company eventually paid $4.4 million in cryptocurrency to the attackers, however, there were unaccounted costs while the pipeline was shut down. Another similar attack, NotPetya, "caused approximately $10 billion in damages spread across multiple international industries and crippled the country's infrastructure" (Wood, 2023). High-profile incidents like the Colonial Pipeline and NotPetya highlight the concern about ransomware. In response, hospitals, other industries, and companies have turned to cyber insurance for risk mitigation as one of the many strategies to defend against cyber attacks.

Ransomware is a relatively new threat abounded by the increased reliance on technology and increased attack surface through the saturated use of devices connected to the internet, or Internet of Things (IoT) devices. As a result, the need for cyber insurance has not appeared until recently, making cyber insurance a relatively new market developing its policies. Thus, it is unknown how the cyber insurance market will develop and what effect it will have on the cybersecurity of hospitals. In this paper, I argue that cyber insurance has a positive regulatory effect on hospital cybersecurity in defense against ransomware attacks, and the adoption of cyber insurance will become more prevalent.

This paper approaches the problem through historical and systems analysis. The historical analysis examines how ransomware attacks and hospital cybersecurity have evolved in tandem to the current state of cybersecurity practices and cyber insurance. At the same time, systems analysis through Actor-Network Theory (ANT) examines key interest groups invested in hospital cybersecurity such as governments, cyber insurance companies, and potential victims of cyber attacks and how they are shaping the current cyber insurance market and hospital cybersecurity.

## II. Problem Definition

### The Monetary Allure of Ransomware for Attackers

The decision to pay or not pay the ransom comes from many factors. Victims are more likely to pay the ransom when the cost of the information ransomed is deemed greater than the ransom payment. Releasing data can have liability costs to a company's reputation and third-party damages (Baker and Shortland, 2022), leading to the ransom more likely to be paid. While systems are shut down, critical services can have supply-chain ripple effects on a large scale. This was illustrated in the Colonial Pipeline ransomware attack. Factoring in ransomware's high success rate and profitability, it has become the most prevalent and damaging cyber threat. The consequences of a ransomware attack include losses in money, reputation, and lives. Ransomware in recent years has developed into a Ransomware-as-a-Service (RaaS) model where attackers can sell small, packaged exploits to those on the dark web (Tsohou et al., 2023). This protects the creator of the ransomware technology and makes the attacks more prevalent as individuals can easily gain access to an exploit. As such, ransomware is profitable for cyber criminals, seen as a way to gain large profits in a short amount of time.

Ideal targets for ransomware attacks are critical system infrastructure and software services. Targeting large software services immediately creates victims of the millions of individuals and companies that use and depend on the software, leading to the ransom more likely to be paid by the target company (Tsohou et al., 2023). Victims of ransomware are more likely to pay the ransom when there are critical time-sensitive losses on the line. This is often seen in utility companies and hospitals. Since hospitals are critical infrastructure vulnerable to ransomware attacks, it is important to explore the effect of ransomware mitigation techniques employed by hospitals such as cyber insurance.

## Cyber Insurance Motivations

The emergence of cyber insurance was largely driven by the move online during the pandemic (Tsohou et al., 2023). Cyber insurance policies are commonly split into two types of coverage: first party and third party losses. First party coverage insures against the losses of the insured company while third party coverage covers liability claims from third parties (Tsohou et al., 2023). The benefits of cyber insurance include offering services for ransom negotiation and payment. According to Baker and Shortland (2022), private lawyers are highly coveted because of the client-attorney privilege and confidentiality. Shopping for these services individually when an attack occurs can be costly, taking time that converts to operational loss.

Cyber insurance can have a regulatory effect on hospital cybersecurity in relation to preventing cyber attacks from occurring. According to Tsohou et al. (2023), cyber insurers have an underwriting process to review the cybersecurity efforts of the insured company to assess whether the insured qualifies for a claim. Such factors and analysis determine the cybersecurity measures a company has in place and at the same time confirm that the insured have put in the effort to prevent cyber attacks by securing their systems.

### Government Regulation of Ransomware

How the government chooses to prevent ransomware is an ongoing debate. While the government has taken a hands-off approach to regulating ransomware, high-profile cases have forced their involvement. Government agencies use military forces to go after criminal groups that cause severe damage with ransomware. In the case of the Colonial Pipeline attack, they were able to recover $2.3 million of the ransom (Wood, 2023). In other cases, the government has successfully taken down criminal groups. Cyber insurance companies and organizations have requested the involvement of the government to help reduce cybersecurity threats, and the government has debated taking a nation-wide stance to prosecute ransomware and reduce the number of attacks. Another potential idea is banning ransomware payments. According to Davidson (2024), governments prohibiting ransomware payments and banning negotiations with cyber criminals are a “moral and fiscal dilemma.” Authorities must balance competing interests to protect critical infrastructure, avoiding funding criminal groups, and discouraging ransomware.

### Ransomware Attacking Hospitals

Hospitals are a large concern in regards to being a target for ransomware attacks because of the nature of the sensitive information they hold. Healthcare providers store and use personally identifiable information (PII) and protected health information (PHI) in their daily operations (Salem et al., 2020). While another industry’s company may store information about their client, it is usually centralized and protected by cybersecurity measures. However, in a hospital, every department, healthcare provider, and electronic device is likely accessing this information in order to view health records, prescribe medication, monitor patients, calculate billing and insurance, and more. This leads to vulnerabilities for cyber extortionists to infiltrate, collect information, and ransom. In addition, immediate access to patients' information is critical for hospitals all the time to proceed with a health procedure or perform a diagnosis. According to Humer and Finkle (2024), medical information is worth ten times more than credit card information on the black market. Credit cards have risk mitigation protocols such as freezing a card, issuing a new one, or reimbursing the client, but when health information is stolen, a patient cannot change information such as their birthdate or blood type (Argaw et al., 2020). In addition, stealing credit card information offers short term payoffs, such as spending a certain amount on a stolen credit card before it is deactivated; however, with medical information, fraudsters can use the information such as names, birthdates, and policy numbers to create fake identities and bill the victims with made-up insurance claims or obtain health services (Humer and Finkle, 2024). As such, hospitals are easy and prime targets for cyber attacks.

## III. Research Approach

This paper utilizes the Actor-Network Theory (ANT) framework to analyze the relationships between different actors involved in regulating ransomware, particularly focusing on cyber insurance providers, healthcare institutions, and government entities. The research draws on a range of sources including peer-reviewed academic literature, industry publications, case studies, and government policies.

Actor-Network Theory (ANT) proposes a framework for technical analysis in which human and non-human entities come together as "actants" in a network each holding equal stake (Latour, 1996). The "framework is concerned with the processes by which scientific disputes become closed, ideas accepted and tools and methods adopted" (Rodger et al., 2009). ANT examines the strategies used by actors to “mobilize allies,” resulting in the construction of a “heterogeneous network” (Callon, 1986). When a network is formed, science is being “black boxed” and becomes an established fact (Latour, 1987). Instead of analyzing the assumptions about nature, the framework analyzes science by following and describing what scientists do to enlist other actors, both human and non-human, that eventually establishes the network (Callon, 1986). According to Callon (1986), ANT “highlights the power is in the relations.” Translation is the process by which an “actor-world” is built from entities through attaching characteristics that establish relationships between them. After a network forms, it may become unstable, and a network can break down and reform as actors dissent or leave the network or when new actors join.

ANT can be applied to my research by examining the relationships between human and non-human actors in the system, illustrated in Figure 1.

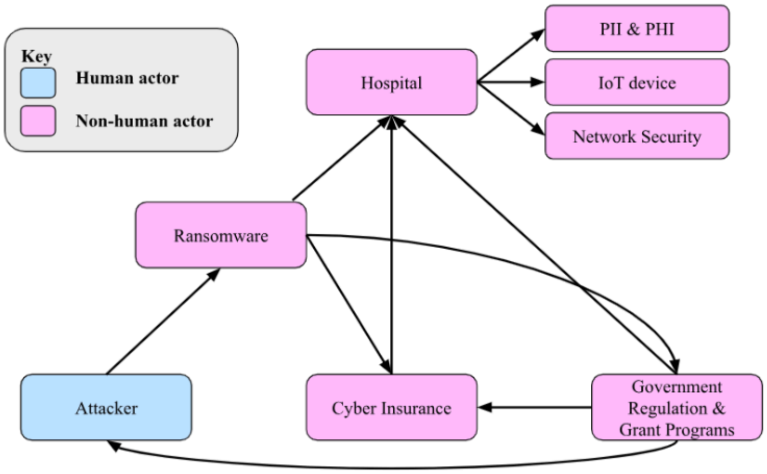
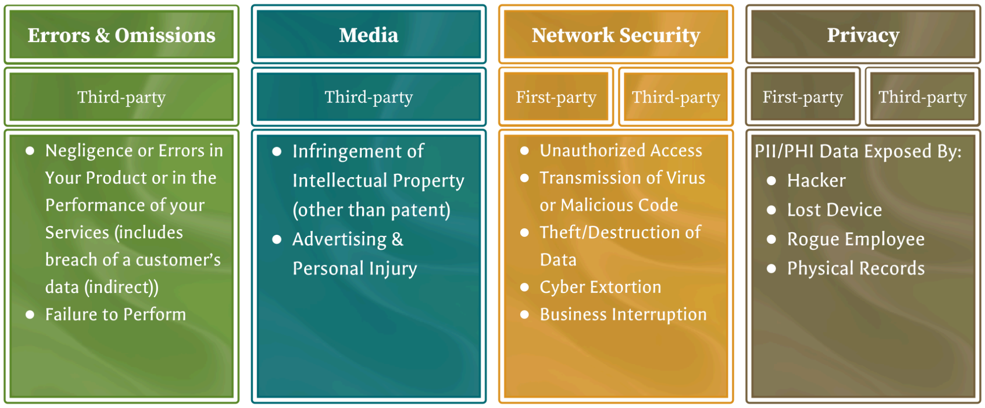


**Figure 1.** Relevant actors in the ransomware, cyber insurance, and hospital cybersecurity system (Figure by author)

Hospitals, government regulation and grant programs, cyber insurance, and ransomware all come together to form a network of non-human actors. Each actant affects each other in different ways, exhibiting power over the system. To analyze the mechanics of power, the research examines ransomware and cyber insurance actors through historical analysis. Since cyber insurance arose as a way to mitigate risk for companies from cyber attacks, a historical analysis framework is applied to analyze how ransomware and cyber insurance developed in tandem. The analysis draws from academic sources.

Tsohou et al. (2023) reports on the current state of cyber insurance policies and why it developed into the way it is today. Tsohou et al.'s (2023) research defines cyber insurance, showing how it formed as a direct consequence of increased attack surface with a significant driver being the recent pandemic. They also break down the different components of cyber insurance including policy types, policy purposes, covered situations, and claim filing procedures. Cyber insurance can be categorized into different areas of coverage, as shown in Figure 2.



| Errors & Omissions | Media | Network Security | | Privacy | |
|---|---|---|---|---|---|
| Third-party | Third-party | First-party | Third-party | First-party | Third-party |
| • Negligence or Errors in Your Product or in the Performance of your Services (includes breach of a customer's data (indirect))<br>• Failure to Perform | • Infringement of Intellectual Property (other than patent)<br>• Advertising & Personal Injury | • Unauthorized Access<br>• Transmission of Virus or Malicious Code<br>• Theft/Destruction of Data<br>• Cyber Extortion<br>• Business Interruption | | PII/PHI Data Exposed By:<br>• Hacker<br>• Lost Device<br>• Rogue Employee<br>• Physical Records | |

**Figure 2.** Categories of coverage policies by cyber insurance (Baker and Shortland, 2023)

Tsohou et al.’s research highlights the relationship of cyber insurance and hospitals through how cyber insurance can be used by hospitals. Research by Baker and Shortland (2022, 2023) analyzes how cyber insurance co-evolved with ransomware and governs cybersecurity risk as its policies developed. Both in cases where there is government intervention and where there isn’t, the authors show how cyber insurance influences the cybersecurity of the organizations they insure as they develop their policies in response to ransomware development. In addition to academic papers, industry perspectives such as blog entries from cyber insurance firms were included to understand current practices and policies brokered between individual companies.

For my research, government actors were studied through regulatory legislation that affect hospital practices pertaining to management of patient health information. Sources such as the FBI’s Internet Crime Complaint Center (IC3) annual report were utilized to provide authoritative data on the financial scale and prevalence of ransomware incidents.

Finally, a case study is applied to show how all the actants meet to form a black box when a ransomware attack occurs, forming a network of interactions between cyber insurance policies, government regulation, and hospital and cyber attacker responses. A central component to this research was the case study of a ransomware attack on University of Vermont Health Network’s hospital. The study illustrates a real-case ransomware attack on a healthcare system and shows how in the aftermath, the hospital utilized cyber insurance to cover monetary losses and improved their cybersecurity practices in response.

## IV. Results

### Evolution of Cyber Insurance Policies

The development of cyber insurance has been unregulated and a system of trial and error co-evolved with ransomware technology. Cyber insurance developed out of the need for companies to manage losses that originated apart from user negligence but happen despite making reasonable efforts, such as hackers, malware, denial of service attacks, and more (Baker and Shortland, 2022). A general trend is that cyber insurance evolved out of existing insurance policies such as general liability or property. As such, there is a wide range of insurance policy types such as those bundled with other insurance or individual standalone policies. Individual cyber insurance policies are often very specific about what they cover.

Companies are hesitant to adopt cyber insurance because they are unsure whether they will qualify for claims (Tsohou et al., 2023). According to Barrett (2022), the cyber insurance industry has a loss ratio of 73% in 2021. This results in a high competition of insurance policies being developed and many insurance companies quitting the field. A survey showed that 14% of North American companies have cyber insurance coverage that exceeds $600,000 (Barrett, 2022) while the total cyber-related losses in 2024 amounted to $16.6 billion (FBI, 2025). As such, cyber insurance companies can set their own premiums and policies. This would be a major consideration for hospitals purchasing cyber insurance, as hospitals often have less developed cybersecurity practices and have less money invested towards security. This is highlighted by the fact ransomware and cyber insurance are both relatively new, compared to insurance for other industries such as banks which have always existed. Getting cyber insurance policies or insurance-covered services is a costly endeavor. In the case where companies do not get a cyber insurance policy, seeking services for ransom negotiation, payment, and recovery are costly and an organizational headache to find individually.

**Regulatory Effect of Underwriting**

Cyber insurance includes an underwriting process which implicitly regulates the cybersecurity of hospitals. The underwriting process determines whether an insurance company will assume the risk for a cyber incident along with determining the business risks, insurability and pricing, and developing the insurance process (Tsohou et al., 2023). The insured company's cybersecurity practices play a large role in determining their policy. Factors such as a list of countermeasures for a cyber incident, record of past cyber incidents, audit reports, IT security budget and spending are considered, and more. Some cyber insurers only offer coverage for third-party faults for a list of named providers or "commonly reputable vendors". This is likely to limit their losses by only covering familiar and trustworthy companies, which goes to show the situational assessment of cyber insurance companies to protect themselves. Thus, organizations have to meet a certain level of cybersecurity standards in order to qualify for cyber insurance which has a co-regulatory effect. According to Tsohou et al. (2023), organizations receive compensation for around 59% of the ransom amount in an attack and around 58% of the cost for other losses. This shows that cyber insurance is largely useful in covering liability and loss from a ransomware attack.

### UVM Health Network Case Study

When a hospital is attacked by ransomware, it can compromise the data of up to one million people, as illustrated by the University of Vermont (UVM) Health Network ransomware attack in 2020. The attack occurred through social engineering with a phishing email where malware was delivered from an employee's personal laptop into the hospital system. UVM Health was able to detect the infiltration after some hospital devices started glitching, and they immediately shut down their systems to perform forensic analysis (House Oversight and Accountability, 2023). They found a text file message from the attackers but didn't respond because they did not plan to negotiate or pay the ransom. According to Dr. Stephen Leffler, MD, Chief Operating Officer at the UVM Medical Center, the hospital had a backup system they could switch to, so they didn’t plan on negotiating or paying the ransom, but the attack affected every part of the system including dialysis patients who depend on hospital machines running to live. In his statement during the House hearing, Dr. Leffler explained that they implemented cybersecurity changes after the attack including sub-segmenting the hospital system into pieces and making it harder for administrators to make changes by implementing multi factor authentication. In total they were shut down for 28 days which amounted to operational losses of about $65 million. Of the total losses, they were only insured for $30 million in their cyber insurance coverage (INSURICA, 2024). Without this coverage, the hospital would have likely had to shut down and would not resume operations. In the House hearing, it was mentioned that the lesson from a ransomware attack is to buy enough insurance to cover losses. This shows how ransomware is a non-human actor contributing to the growth of the cyber insurance industry. At the same time, the case study illustrates how an entity might not negotiate with attackers, aligning with government policies.

**Government Interventions and Policy Approaches**

The UVM Health Network case study illustrates the meeting of key actors, such as ransomware technology, hospital employees, cyber insurance policies, and government regulation, during a ransomware attack to shape the cybersecurity practices of a hospital. Ransomware is commonly effective through social engineering targeting hospital employees. When ransomware occurs, cyber insurance policies will help cover the losses, and the response to ransomware will be shaped by government regulation. Moreover, when the costs become uninsurable, companies will look to the government for aid. In the case of the ransomware attack on UVM Health Network, the health system worked closely with the FBI to source the attack and resolve the incident. Additionally, the Governor of Vermont, Phil Scott, deployed the state’s

National Guard to assist. When the damage caused by a ransomware attack is large, the government tends to step in.

While the government has largely left the cyber insurance industry to regulate itself, some situations have forced government involvement, making them a key actor in regulating ransomware (Baker and Shortland, 2023). For example, when the cost to a ransomware incident is uninsurable, such as attacking critical infrastructure in the Colonial Pipeline incident, the government has stepped in to prosecute the cyber attackers. As a result, there has been a shift from "big-game hunting" to "mid-game hunting" where attackers are incentivized to attack mid-sized companies and receive stable sums, rather than go after high-profile targets, to avoid provoking a geopolitical conflict. Additionally, the Department of Homeland Security (DHS) developed the State and Local Cybersecurity Grant program in 2022 to help entities address cybersecurity risks with a combined funding of $1 billion dollars to be spread over four years.

An action the government is considering to prevent ransomware is banning ransom payments and negotiation. According to Davidson (2024), this would essentially cripple the cyber insurance industry. However, Meredith Ward from the National Association of State Chief Information Officers (NASCIO) explains that the intent of the ban is to take the option of ransom payment entirely off the table. This would take away the motivations for cyber criminals to perform ransomware attacks if there is no payout. In addition, it would remove the third party moral hazard of cyber insurance companies funding cyber criminals to launch more attacks. There is no federal consensus on this but it has been proposed as a means to discourage cyber attackers given the magnitude of the repercussions. North Carolina became the first state to officially ban ransomware negotiations and payments. Applied to hospitals, this is a viable option if they have a backup of their data and can keep most operations running while replacing the infrastructure of their systems, as was the case in the UVM Health Network ransomware attack.

## V. Conclusion

Ransomware gained prominence in the wake of the pandemic when many company systems were moved online. In a digitizing age when hospitals store and collect critical patient data in IoT devices, cyber insurance and government policies are being developed to most effectively regulate ransomware. With these different actants identified, their mutual shaping can be analyzed to strike a balance most effective at limiting ransomware cost and damages. Cyber insurance itself is effective at covering costs but can change its policies to be more cost-accessible to smaller companies and encourage a basic level of cybersecurity that will reduce ransomware attacks and the need to pay altogether.

A limitation of this approach is that cyber insurance is underdeveloped, so there is a lack of information to study. There is no standardization of cyber insurance policies due to the recent emergence of the market and the lack of transparency from victim organizations to preserve their company reputation. The lack of statistical data on how well cyber insurance policies perform in relation to hospitals slows down the development of cyber insurance; however, over time, as more attacks occur and cyber insurance policies are perfected, the cyber insurance market will evolve into a more effective form. It can be seen that the cooperation of actors is necessary for cyber insurance to become effective at regulating hospital cybersecurity. Future research can be done to collect data quantifying the effect of cyber insurance on hospital operations directly.

## References

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1). https://doi.org/10.1186/s12911-020-01161-7

Baker, T., & Shortland, A. (2022). Insurance and enterprise: Cyber insurance for ransomware. *The Geneva Papers on Risk and Insurance - Issues and Practice, 48*(2), 275–299. https://doi.org/10.1057/s41288-022-00281-7

Barrett, L. (2022, November 27). *As cyberattacks and insurance costs grow, time is right for accreditation.* Chief Healthcare Executive. https://advance.lexis.com/document/?pdmfid=1519360&crid=a1b4cff1-0f31-4fd7-b1ee-6e9b8a1dab6f&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A67H3-JY21-F0CR-J4MD-00000-00&pdcontentcomponentid=483557&pdteaserkey=sr2&pditab=allpods&ecomp=hc-yk&earg=sr2&prid=5ff56057-2dd4-46a9-b9ce-8838656a51aa

Callon, M. (1986). Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St. Brieuc Bay. In J. Law (Ed.), *Power, Action and Belief: A New Sociology of Knowledge?* (pp. 196–233). Routledge and Kegan Paul.

Cartwright, A., Cartwright, E., MacColl, J., Mott, G., Turner, S., Sullivan, J., & Nurse, J. R. C. (2023). How cyber insurance influences the ransomware payment decision: theory and evidence. *Geneva Papers on Risk & Insurance, 48*(2), 300-331. https://doi.org/10.1057/s41288-023-00288-8

Cybersecurity and Infrastructure Security Agency. (n.d.). State and Local Cybersecurity Grant Program. https://www.cisa.gov/cybergrants/slcgp

Davidson, N. (2024). Paying the Price. *Government Technology, 37*(6), 32–34.

Federal Bureau of Investigation. (2025, April 24). 2024 IC3 Annual Report. https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/2024ic3report-1.pdf

House Oversight and Accountability. (2023, September 27). Combating Ransomware Attacks. https://www.youtube.com/live/9JobbjLJ54k?t=3477s

Humer, C., & Finkle, J. (2014, September 24). *Your medical record is worth more to hackers than your credit card*. Reuters. https://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924/

INSURICA. (2024, October 21). Cyber Case Study: UVM Health Network Ransomware Attack. https://insurica.com/blog/uvm-health-network-ransomware-attack/

Latour, B. (1987). *Science in action: How to follow scientists and engineers through society.* Harvard University Press.

Latour, B. (1996). On actor-network theory: A few clarifications. *Soziale Welt*, *47*(4), 369–381. http://www.jstor.org/stable/40878163

Li, Z., & Liao, Q. (2023). Does cyber-insurance benefit the insured or the attacker? – A game of cyber-insurance. In J. Fu, T. Kroupa, & Y. Hayel (Eds.), *Decision and Game Theory for Security* (pp. 23–42). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-50670-3_2

Rodger, K., Moore, S. A., & Newsome, D. (2009). Wildlife Tourism, Science, and Actor-Network Theory. Annals of Tourism Research, 36(4), 645–666. https://doi.org/10.1016/j.annals.2009.06.001

Tsohou, A., Diamantopoulou, V., Gritzalis, S., & Lambrinoudakis, C. (2023). Cyber Insurance: State of the art, trends and future directions. *International Journal of Information Security*, 22(3), 737–748. https://doi.org/10.1007/s10207-023-00660-8

Wood, K. (2023, March 7). *Cybersecurity policy responses to the Colonial Pipeline Ransomware attack.* The Georgetown Environmental Law Review. https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/#:~:text=The%20attack%20shut%20down%20Colonial,feared%20gas%20would%20run%20out.

Yilmaz, Y., Cetin, O., Grigore, C., Arief, B., & Hernandez-Castro, J. (2023). Personality types and ransomware victimisation. *Digital Threats*, 4(4), 53:1-53:25. https://doi.org/10.1145/3568994