Colonial Pipeline: The effects of cyber fatigue and poor regulation on cyber defense.

Alan Schneider

Department of Cybersecurity, Old Dominion University – Norfolk

IDS300W: Interdisciplinary Theory & Concepts

Dr. Kat LaFever

1 April 2023

Abstract

As ransomware attacks, data breaches, denial of service attacks and other cybersecurity incidents continue to increase in number and complexity. Industry leaders, Cybersecurity professionals and Legislators are looking for ways to mitigate the extraordinary economic and national security consequences of this global cybersecurity threat. These attacks are in part enabled by a burgeoning ransomware economy, transnational regulatory and prosecutorial challenges as well as cognitive stress and security fatigue as destroyers of strong cybersecurity defense and response. This paper explores how economic incentives, price discrimination and collective bargaining strategies drive the successes and failures of the current ransomware economy. What are the causes of cognitive stress, burnout, and security fatigue and can we integrate mitigation strategies for these human factors that weaken cybersecurity defense? How does international regulatory and prosecutorial challenges impede coordinated cybersecurity incident reporting and response? A discussion of these co-factors helps build an understanding of the regulatory, cognitive, and economic elements that cybersecurity professionals must use to identify managerial, jurisdictional challenges and high-risk practices that degrade network defense while implementing robust cybersecurity initiatives to reduce risk. Given that cybercriminals continue to exploit economic, regulatory, and cognitive weaknesses to gain access to critical infrastructure.

Introduction.

Ransomware attacks on critical infrastructure are part of a disturbing trend increasingly affecting global security. By 2020, ransomware attacks had exceeded between twenty thousand and thirty thousand per day in the United States alone. Costing victims an average of nineteen days of network downtime and a median payout of $230,000 per incident. “In 2021 global costs associated with ransomware recovery exceeded $20 billion” (Lubin A, 2022, p.1). On May 7, 2021, Colonial Pipeline, a petroleum distribution company responsible for 40% of all fuel consumed on the east coast, was shut down for four days following a ransomware attack. The attack successfully penetrated their Industrial Control System (ICT) network prompting the company to pay the $5.5 million ransom and shut down the pipeline as a precaution against further attacks.

So, what does the Colonial Pipeline ransomware attack indicate about the effects of ransomware economics, cyber fatigue and regulatory challenges on coordinated network defense and recovery? To answer this question, economic insights provide a lens through which risk vs reward factors, influencing decisions to conduct ransomware attacks can be identified. An understanding can be developed of the psychological effects that overexposure to cybersecurity-related work demands, or training has on cognitive disengagement in positive cyber-related workplace behaviors or advice. And a critical analysis of challenges posed to regulatory and prosecutorial efforts by the transnational nature of these attacks can be applied. Interdisciplinary research into this issue establishes a foundation for a holistic review of the complex nature of ransomware attacks. Combining the insights gleaned from each discipline’s narrow field of view into a comprehensive approach increases the likelihood of successful implementation of multi-faceted cybersecurity defense methodology.

A. Definitions

A Reeves, School of Psychology, University of Adelaide, Southern Australia defines *Cybersecurity fatigue* as a form of cognitive disengagement manifesting as a weariness or aversion to cybersecurity-related workplace behaviors or advice (Reeves et al., 2021, p.5)

James Bone, Executive Director, Founder of The GRC Bluebook defines "*Cognitive hacking* as a computer or information system attack that relies on changing human users' perceptions and corresponding behaviors in order to be successful" (Nobles, C. 2022, p.4)

Economics

The concept of extorting money from individuals is nothing new. But, as the methods of ransomware extortion have become more technically complex, so have the economic factors that drive it. The objective of cyber criminals is to maximize the profit from compromised systems while minimizing the risk of attribution and arrest. The profit made is then dependent on the inclination of those victims to pay the ransom demanded. This, in turn, relies on various factors- how critical are the systems or data compromised, the degree of trust that the extortionist will keep their word and the victim's willingness to pay them. Willingness to pay is further complicated by the fact criminals must determine an optimal ransom for each victim. This is where the concept of economic price discrimination comes into play.

Third-degree price discrimination is perhaps the most relevant to ransomware extortion as the ransom is based on grouping victims by type; not tailored to each incident or by quantity; as it would with first or second-degree price discrimination (Hernandez-Castro et al., 2017, p.5) Gaining access to a victims network, files and computers can give cybercriminals useful information about the value of the information collected, the victim's worth, or both, enabling

categorization of the victims correlation between data value and willingness to pay to arrive at an optimal price. However, the economic dynamics of this issue also include bargaining strategies that work for and against both parties.

A standard model of bargaining assumes both parties, make alternating offers (Hernandez-Castro et al., 2017, p.7) The criminal sets a ransom, the victim then either pays the ransom or counteroffers, then the criminal either accepts the counteroffer or sets a new ransom, and so on. But there are factors of control that potentially change the outcome of the standard bargaining model. One factor that criminal's control is to return the data or not to the victims. The greater the chance of data being recovered, positively affects the willingness to pay increasing the size of the ransom that can be set. Another control factor is that of framing severity. Willingness to pay is greater if the criminals emphasize the sure loss of the files. Each of these factors can influence the overall economic outcome of a ransomware attack. But none of these strategies works without a universal payout mechanism, and in a digital age of monetary surveillance, cybercriminals turn to unregulated Bitcoin cryptocurrency. "Bitcoin is a peer-to-peer cryptocurrency initially introduced by Satoshi Nakamoto (a pseudonym) (Paquet-Clouston et al., 2019, p.3) It can be used to execute pseudo-anonymous payments globally within a short period of time. Bitcoin "accounts for over 40% of all identified criminal-to-criminal payments" (Paquet-Clouston et al., 2019 p.9) The payments are difficult to track due to specialized intermediary bitcoin transactions called CoinJoin that take multiple senders and recipients of funds combining their payments into a single aggregated transaction. Breaking the link between the sender (victim) and the receiver (criminal). Use of this secure method of payment meshes well with the attackers' goals of maintaining anonymity and reducing risk while bargaining for the return of the victim's data. These types of economic strategies were in evidence during the

Colonial Pipeline attack. Through previous recon efforts, the hackers had determined that encrypting the pipeline's billing network and exfiltrating 100Gb of proprietary data that they threatened to release would strengthen their bargaining position. Resulting in the pipeline paying the $5 million dollar ransom within hours of the attack.

Psychology

The next discipline relevant to the Colonial Pipeline attack is Psychology, particularly the cognitive phenomenon known as cyber fatigue. Performance of countless security tasks daily both privately and professionally; requires physical and cognitive abilities. "Consequently, they take a toll on individuals, especially if the security functions are deemed excessive, illogical, or impractical to the users" (Nobles, C. 2022, p.3). Cognitive stress, fatigue, and burnout reduce the performance capacity of employees, especially cybersecurity professionals; enabling cybercriminals to capitalize on the employees' debilitated state and lack of awareness. With that in mind, cyber fatigue comprises two important components: type and source., Fatigue type refers to the two ways in which individuals experience and manifest cyber security fatigue. Attitudinal-type fatigue relates to an individual experiencing a negative effect relating to cyber security (Reeves et al., 2021 p.4) This manifests as emotional exhaustion, moral disengagement and cynicism, both toward the value of cyber security directives and the individual's ability to meet its demands. Cognitive- type fatigue focuses on the limited capacity individuals have to make decisions, or to cope with increased cognitive load (Reeves et al., 2021, p.5) Subsequently individuals engage in biased, intuitive, and impulsive decision-making, or complete decisional avoidance. This manifests as security warning dismissal, developing risky security behaviors, or basing trust in emails without verifiable integrity. The second component; source-fatigue is the

aspect of overexposure that is the cause of fatigue; either Actions or Advice (Reeves et al., 2021, p.5). Repetitive cybersecurity tasks, user password expiration requirements and frustration with multifactor authentication systems are common example of action related fatigue. While excessive cybersecurity training, ever changing cybersecurity policy and consistent security alerts are examples of Advice related fatigue suffered by employees. Each fatigue factor, both type and source, in any combination can contribute to weakened cyber readiness and provide attackers with the opening they need to penetrate a network. This element is evidenced by Colonial Pipelines lax user account deletion procedures, enabling hackers to compromise the login credentials of a former employee. As well as weak configuration control policies that allowed outdated VPNs to remain on the network and failure to enforce two-factor authentication enterprise-wide.

Regulation

The last discipline that is relevant to the Colonial Pipeline incident is Law specifically cybersecurity regulation. There are several factors to consider when creating an understanding of how this discipline relates. First is the non-uniform status of state regulations that criminalize ransomware. To date only twelve states have adopted such legislation, none of which have conformity as to each state's interpretation of what constitutes a ransomware attack. In Texas it meets the legal bar for criminality merely to "introduce" the ransomware malware to a device, but in California the accused must demonstrate both an "intent to extort" and actual acquisition of "property or other consideration" because of the extortion. (Lubin, A. 2022, p.10,11) These differences generate real gaps in the way the crimes are defined and enforced. Exacerbating the issue is that state regulators are unable to enforce private company disclosure of a ransomware

incident to federal authorities, nor can it be certain that the notification will be effectively handled once transmitted. The second factor is Indecisive Federal enforcement. Although the Federal government recommends ransomware demands should not be met and warns of sanctions by the Department of Treasury should they be paid (Lubin, A, 2022, p.13). They have not enforced such sanctions, even where local and state entities were the ones making the payment.

The final element to consider is the transnational nature of cybercrime. Under international law most ransomware attacks do not constitute uses of force as defined under Article 2(4) of the United Nations Charter. (Lubin, A, 2022, p.16) Succinctly, a cyberattack must be equivalent, in its scope and consequences, to the harm that may be generated by physical uses of force. Yet, most ransomware attacks only generate economic harm and do not rise to the use of force level recognized by the international community. Added to this limitation is the consistent reluctance for victims to be forthcoming on the details of an incident. Details that are critical in attribution and potential prosecution of offenders As EUROPOL statistics indicate, law enforcement authorities approach victims to assist them by potentially starting a criminal investigation. But "this was not generally a priority of the victim organization, as the primary focus was on business continuity and limiting reputational damage" (Robles-Carrillo & García-Teodoro, 2022, p.13)

Common Ground

So, what kind of common ground can be developed from these disciplines? There are three major findings disclosed by this interdisciplinary research, First, the successful application of economic price discrimination, collective bargaining strategies and the pseudo-anonymous

payout mechanism of cryptocurrency provides motivation to conduct ransomware attacks in lieu of traditional methods. Second cyber fatigue manifesting as stress, burnout, and security fatigue due to overexposure to cybersecurity-related work demands leads to cognitive disengagement in positive cyber-related workplace behaviors or advice. Third inconsistent international regulatory and prosecutorial authority impedes coordinated cybersecurity incident reporting and response. Each contributes to a cyclical process of economic motivation fed by failures to address real cognitive and regulatory issues that weaken coordinated responses to an international problem. Collectively failing to disincentivize these attacks by reducing cognitive risk factors, increasing attackers' risk of attribution and arrest, and minimizing financial reward influencing these types of criminal behaviors.

Disciplinary Conflicts

Research into cyber fatigue focuses solely on internal forces behind cognitive sources of cybersecurity disengagement, with the inclusion of psychology-based professionals in cybersecurity operations as a remedy. This contrasts with research that reveals external economic and regulatory pressures creating a fertile environment of incentivized criminal behaviors. It is then perhaps more productive to place less weight on characterizing each element as internal or external and apply a more holistic approach to answering this issue. Namely, greater regulatory involvement across all disciplines; whether codifying psychology-based professionals' role in cybersecurity, uniform cryptocurrency regulation and tracking, or international treaty pooling intelligence, resources and creating uniform jurisdictional authority.

Conclusion

In conclusion, economic, cognitive, and regulatory theories and practices should not be discounted when tackling the problem surrounding ransomware attacks. A singular focus on IT as both source and answer, robs cybersecurity professionals of wider viewpoints outside their chosen discipline. Constituting missed opportunities to apply more effective and robust approaches that can lead to real world solutions to complex cybersecurity problems.

References

Lubin, A. (2022, August 6). *The law and politics of Ransomware*. SSRN. Retrieved April 7, 2023, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4181964

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle Cyber Fatigue. SAGE Open, 11(1), 215824402110000. https://doi.org/10.1177/21582440211000049

Nobles, C. (2022). Stress, Burnout, and security fatigue in cybersecurity: A human factors problem. HOLISTICA – Journal of Business and Public Administration, 13(1), 49–72. https://doi.org/10.2478/hjbpa-2022-0003

Hernandez-Castro, J., Cartwright, E., & Stepanova, A. (2017). Economic Analysis of Ransomware. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2937641

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz003

Robles-Carrillo, M., & García-Teodoro, P. (2022). Ransomware: An interdisciplinary technical and legal approach. *Security and Communication Networks*, *2022*, 1–17. https://doi.org/10.1155/2022/2806605