Issues in Information Systems
Volume 23, Issue 4, pp. 230-242, 2022

DOI: https://doi.org/10.48009/4_iis_2022_120

Ransomware: A primer, suggested deterrence and a systems thinking approach

Jennifer L. Breese, *Penn State University, jzb545@psu.edu*
Mark Fox, *Indiana University South Bend, mfox1@iusb.edu*
Ganesh Vaidyanathan, *Roosevelt University, gvaidyanathan@roosevelt.edu*

Abstract

This paper focuses on trends in ransomware attacks and proposes that systems thinking is a useful approach to thwart these attacks. Ransomware attacks are a form of malware involving a breach in a company's data and holding it hostage for a price or "ransom." The popularization of cryptocurrencies and an increase in remote working have facilitated a greater incidence of ransomware attacks. Ransomware has resulted in companies investing in training, information sharing, and in further government intervention as means of prevention against ransomware. This paper identifies ransomware prevention and detections, suggesting the potential for systems thinking to further augment these methods. A systems thinking approach could provide a useful framework for analyzing information effectively within organizations and its relationship to external systems.

Keywords: Cybersecurity, Data breaches, Malware, Ransomware, Systems Thinking.

Introduction

Cyber criminals and Advanced Persistent Threat groups target vulnerable people, organizations, and systems. The pandemic of recent years has furthered their efforts (Pranggono, 2020). The popularization of cryptocurrencies and an increase in remote work have facilitated greater incidents of ransomware attacks. These threats have resulted in companies investing in established resources such as training and information sharing, supported by further government interventions as means of prevention against ransomware. A systems thinking approach provides a common framework for analyzing information effectively within organizations and its relationship to external systems. This paper identifies ransomware prevention and detections, suggesting the potential for systems thinking to further augment these methods.

Ransomware is a type of malware that encrypts files and drives in order to potentially hijack systems and disrupt operations, typically for financial gain. Ransomware deployment consists of three distinct phases: infection, payment demand, and release of control (Ransomware.org, 2022). During the *infection* phase, a seemingly legitimate phishing email with a message containing a link to a website that hosts a ransomware code is sent to a target system. Taking advantage of common software or operating system (OS) vulnerabilities, the malicious code is injected into a company's system. Once the ransomware code is executed, users are shut out of their system or organizational data is encrypted using advanced encryption methods. During the *payment demand* phase, the owner of the infected system receives instructions on how to regain access through an email. A ransom with preferred currency, payment method, and a deadline is presented in that email. If the terms of the ransom are met, the attacker may trigger a *release* of the attack code or provide a decryption code, or the attacker may simply take the ransom money without restoring access. If the victim refuses to pay, they face the prospect that their data will be published or sold online (Ransomware.org, 2022).

Ransomware operators may be part of Ransomware-as-a-Service (RaaS) platforms. Attackers may subscribe to access the platform and gain access to a given type of established ransomware software. Ransomware platforms include Cerber, Darkside, Gandcrab, Maze, Locky, NotPetya, REvil, and WannaCry. Ransomware software needs to communicate with such platforms in order to retrieve an encryption key and distribute that key, which acts like a digital certificate. A digital certificate is a file or an electronic password that provides authenticity for a device, server, or user through cryptography and public key infrastructure (Cheng et al., 2018). Digital certificate authentication helps organizations ensure that only trusted devices and users can connect to their networks (Cheng et al., 2018). Such actions require that the attackers need to disguise their Internet Protocol (IP) addresses and the hosting company servers to ignore those illegal activities. These hosting companies are called Bulletproof Hosting and are invariably based in China or Russia (Segura, 2016).

Literature overview

The intent of malicious software or “malware” is to damage a victim's computer system or networks (Rieck et al., 2008). While there are many types of malware (such as viruses, ransomware, spyware, etc.), organizations have increasingly focused on ransomware. Ransomware threats have risen rapidly in the past few years, particularly due to the transfer of work to remote locations during the pandemic. This shift has signaled that urgent work needs to be done to address this threat in all industries. For example, a ransomware threat affected more than 60 trusts within the United Kingdom’s National Health Service and spread to more than 200,000 computer systems in 150 countries (Collier, 2017).

According to the Identity Theft Resource Center (ITRC), 1,111 data breaches were publicly reported in 2021 (Brooks, 2021). About 37% of global organizations said they were victims of some form of ransomware attack in 2021 (Dickson & Kissel, 2021). The losses ranged from as little as $70 to as much as $1.2 million, with a median loss of $11,150 (Verizon, 2021). In July 2021, a single ransomware attack committed by the REvil Group caused a widespread downtime for over 800 to 1500 small to medium-sized companies (Osborne, 2021). In 2021, ransomware incidents were also targeted at 14 of the 16 United States critical infrastructure sectors, including defense, food and agriculture, government facilities and information technology (Cybersecurity and Infrastructure Security Agency et al., 2022).

Ransomware can either be crypto ransomware or locker ransomware. Crypto ransomware encrypts files and data. In contrast, locker ransomware locks computer systems or other devices, preventing the victims from using it, but rarely corrupts stored data (Hansman & Hunt, 2005). Ransomware has thrived because of cryptocurrencies. A demand for payment to restore or unlock systems often involves payment by cryptocurrency. The transactional anonymity of Bitcoin and other cryptocurrencies makes it harder to trace the ransom being extorted (Richardson & North, 2017). Below, Table 1 illustrates some of the prominent ransomware attacks in 2021 (Kerner, 2022).

Table 1: Prominent Ransomware Attacks in 2021 (Kerner, 2022)

Company	Industry	Date	Description	Ransom paid
Acer	IT Hardware	March 2021	Attack executed using the REvil ransomware platform	Unknown
can	Finance	March 2021	Attack executed by a group known as Phoenix	Unknown
Colonial Pipeline	Oil/Energy	May 2021	Attack that affected the flow of oil across the eastern U.S.	Unknown
JBS USA	Meat processing	June 2021	Attack that reduced the company's ability to package meat products using the REvil ransomware platform	$11 million
Kaseya	Software	July 2021	A supply chain attack using the REvil ransomware platform	Unknown
Sinclair Broadcast Group	Entertainment Broadcasting	October 2021	Attack that crippled the network's broadcast operations	Unknown

Next, we review the extant literature and explore why a systems thinking approach could provide useful insights into how to thwart ransomware and related attacks.

Ransomware prevention

Prevention of ransomware attacks starts with preventing infection in the first place. It also involves taking precautions to maintain business continuity or restore inaccessible data and information, if infected. The following are the common methods to prevent ransomware from current literature.

Data backup

As discussed earlier, ransomware encrypts data files. Those files, when backed up, prevent the restoration of clean data files from backups. Backups are useful to restore data and systems to a prior state (Thomas & Galligher, 2018); however, the backup systems themselves are a potential target of ransomware attack, necessitating that they also should be protected (Brewer, 2017). One of the easiest ways to avoid this situation and to restore data after an attack is to conduct regular data backups with necessary protections. To this end, data backups should be current at all times, either using a cloud backup or a remote system backup. Furthermore, backup systems should be duplicated, evaluated, audited, and improved to combat ransomware attacks.

Emails and email attachments

A common method employed in ransomware attacks is phishing. For example, employees of an organization may receive a resume from an unknown sender or fake billing/shipping invoices. To help protect their companies from phishing attempts, Information Technology departments must encourage employees to turn off Java and JavaScript as well as standardize and implement ad blocking software.

Employees should be made aware not to click on links or open attachments in spam emails. Corporate and IT managers should make use of focused screening and training programs to help prevent phishing attacks (Thomas, 2018).

System software

System software, such as the operating system, browsers, and security software, are vulnerable to malware or ransomware attacks. They must always be current with the most recent patches and maintenance updates. If Java and JavaScript must be used, they must be kept with current versions and all current patches updated.

Antivirus software

Most companies rely on antivirus software (AV) to protect their digital assets from ransomware. Many modern malware attacks attempt to circumvent AV defenses through obfuscation, polymorphism, denial of service attacks, or malformed packets (Genç et al., 2021). In this regard,
"AVs react by complementing signature-based detection with anomaly or behavioral analysis, and by using OS protection, standard code, and binary protection techniques" (Genç et al., 2021, p. 4:1). While antivirus programs are typically extremely effective and computationally efficient in detecting malware in general, they can find it difficult to deal with some attacks (Genç et al., 2021). Pérez-Sánchez and Palacios (2022) have proposed an event-based strategy demanding rapid responses to events as a second layer of analysis to improve detection rates.

Minimization of attacks

Shutting down an infected system or network is the first defense against the possible spread of malware. IT employees must be trained to watch for malware attacks and act quickly to prevent the spread of malware. However, training alone is not enough, and human error remains the main entry point for ransomware infections (Pagán & Elleithy, 2021). Enhanced protection is possible with the setup of additional firewalls, which should be configured to block access to known malicious IP addresses.

Researchers are investigating the possibility of automating human interventions. One such approach is the implementation of a layered defense with innovative anti-malware software installed on local machines, properly configured firewalls, active DNS/Web filtering, email security, backups, and staff training (Pagán & Elleithy, 2021). A layered approach enables ransomware attempts to be identified and stopped at multiple points (Pagán & Elleithy, 2021).

Risk Mitigation

Organizations cannot make informed decisions without fully understanding the extent of a ransomware threat. Organizations must develop a risk strategy for malware attacks by identifying data, personnel, devices, systems, and all facilities. Organizations must understand the risks of cyber-attacks and prioritize those risks to make informed cybersecurity risk management decisions. The policies, procedures, and processes to manage and monitor organizational regulatory, legal, risk, environmental, and operational requirements must be understood to manage cybersecurity risks (National Institute of Standards and Technology, 2018). Only authorized users and devices should be allowed to perform activities and transactions on company systems. Security policies, processes, and procedures should be maintained and used to manage protection of information systems and assets (Barker et al., 2021). Accordingly, maintenance and repairs of industrial control and information system components should be performed in ways that are consistent with organizational policies and procedures (Barker et al., 2021).

System Administrator Duties

System administrators need to be careful to prevent malware attacks. First, they need attention to detail when opening unsolicited attachments. They should not give themselves more login power than necessary and they should not stay logged in as an administrator any longer than needed. Regarding administrator rights, browsing or opening documents randomly should be avoided (Tailor & Patel, 2017).

Next, we review key trends in ransomware. These are based on academic literature reviews and reports from commercial parties that have an interest in preventing ransomware.

Ransomware trends

Crowdstrike (2022) reported an 82% increase in ransomware data leaks for 2021 compared to 2020. Of particular interest, they noted that ransomware attacks were adapting to become more targeted and gave the example of Russia targeting both IT and cloud computing providers to exploit what "trusted relationships" those businesses have with their clients (Crowdstrike, 2022). Crowdstrike also noted that ransomware attacks highlighted vulnerabilities in critical infrastructure.

McIntosh et al. (2021) observes two major trends that have been highlighted in news reports. First, ransomware attacks are increasingly targeting enterprises rather than individuals and are demanding larger ransoms. Second, attacks are increasingly looking for system vulnerabilities rather than being more passive (e.g., going phishing).

The coronavirus pandemic also made ransomware a growing problem caused by an increased focus on the importance of healthcare providers and more people working from home (and the associated system vulnerabilities associated with this) (Bearman et al., 2021; Pranggono, 2020). The pandemic itself also enabled ransomware attackers to lure victims using fake information that was COVID-related (Bearman et al., 2021).

Verizon found that during 2020 ransomware became the third most common type of attempt to breach data (Verizon, 2021). This occurred in around 10% of breaches with phishing and use of stolen credit cards (hacking) occurring in 36% and 25% of breaches, respectively. Verizon suggested this change may be partly due to more people working from home and to the increased use of "name and shame" tactics by perpetrators of ransomware whereby "These actors will first exfiltrate the data they encrypt so that they can threaten to reveal it publicly if the victim does not pay the ransom." (Verizon, 2021, p. 16). Verizon also examined the losses associated with ransomware and found a medium loss of $11,150 and a significant range of losses ranging between $70 and $1.2 million. Verizon notes that organized crime was a key element in all cybercrimes, including the deployment of ransomware. Specifically, they noted the role of collaborative law enforcement efforts to combat what is an international problem:

> "Criminals can be either formally or informally organized, at times in partnership with nation-state malicious actors, based on a common interest in illicit profit. Cyber actors quickly shift their activity based on emerging opportunities to steal and launder funds using any tactics, techniques and procedures available to them. Collaboration between domestic and foreign law enforcement

> partners to combat cybercriminal groups and their schemes is key to dismantling organized crime and apprehending cyber actors." (Verizon, 2021, p. 114).

In 2019, FireEye, a cybersecurity solutions company, identified cybersecurity trends based on input from 800 or so senior executives from around North America, Europe, and Asia (FireEye, 2020). About 14% of cyberattacks in the previous 12 months were ransomware (targeted phishing, malware, and exploited vulnerabilities ranked higher). Coincidentally, 86% of organizations reported having blockchain initiatives.

Blockchain technologies have also become a focus of ransomware considering their increasing prominence and their use of cryptocurrencies for illegal money laundering. By one estimate, half of Bitcoin transactions are associated with illegal activity (Foley, 2019). One way that malware is used is to deploy ransomware to a victim's computer that limits their access to their cryptocurrency account if they do not pay a ransom before they can access their systems (Sokolov, 2021). This issue is compounded by when pending blockchain transactions exceed the capacity of a blockchain provider (known as blockchain congestion). As Sokolov notes:

> "… conventional electronic payment networks are, however, closely monitored by authorities. This makes blockchains more attractive for processing ransom payments. Since ransomware typically specifies a limited amount of time when victims can pay the ransom and unlock the data, victims are unlikely to wait for congestion to resolve. Therefore, ransom processing often contributes to blockchain congestion." (Sokolov, 2021, p. 781)

Based on a recent review of ransomware research, Bearman et al. (2021) categorized developments into two categories:

1. Ransomware prevention approaches: access control; data backup; key management; and user awareness
2. Ransomware detection approaches: analyzing system information; ransom note analysis; file analysis; finite state machines; honeypots; network traffic analysis; and machine learning.

Bearman et al. (2021) noted that prevention techniques may help deter attacks and reduce the damage of attacks when they do occur. Specifically, it was observed that access control and data backups "can incur significant computational costs" and that data backup can lead to computational performance issues, particularly during times of peak usage (Bearman et al. 2021).

Interestingly, Bearman et al. (2021) also found that the most common way to detect ransomware was machine learning models that were "trained to recognize the general behavioral patterns of ransomware". However, other literature reviews find that mutant forms of ransomware are increasingly being used to thwart these detection techniques (McIntosh et al., 2021; Reshmi, 2021).

Systems thinking

Systems thinking pioneer, Jay Wright Forrester, made the core contributions to the field under the term "system dynamics", while Barry Richmond is credited with coining "systems thinking" (Richmond, 1994). Systems thinking crosses a plethora of disciplines. It is relevant in many areas as it brings clarity to the need for cohesive efforts aimed at understanding and addressing growing organizational complexities and connectedness with technology, even in small to mid-sized companies, non-profits, and government entities in the United States.

According to Richmond (1991), "Systems Thinking is the art and science of making reliable inferences about behavior by developing an increasingly deep understanding of underlying structure" (Richmond, 1994, p. 139). More recently, Arnold and Wade (2015) attempted to consolidate differing definitions of systems thinking that distill the complexity of both the term and its reference in varying discipline literature as it has been critical to define the intricacy in the systems community. The authors developed a singular definition of systems thinking from both literature and application: "Systems thinking is a set of synergistic analytic skills used to improve the capability of identifying and understanding systems, predicting their behaviors, and devising modifications to them in order to produce desired effects. These skills work together as a system." (Arnold & Wade, 2015, p. 675).

Figure 1 below illustrates that each definition was examined to determine if it contained the three core concepts: purpose, elements (characteristics), interconnections (the way elements feed into one another).

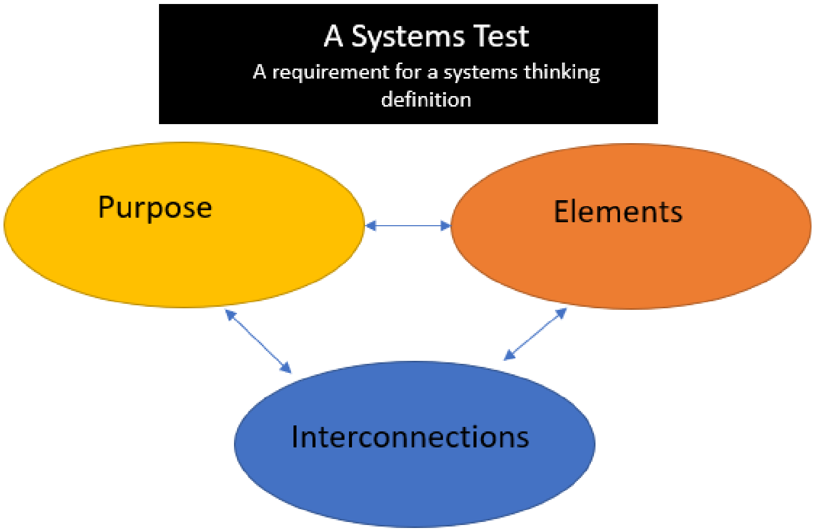


Figure 1: A Systems Test for Systems Thinking Definition (Arnold & Wade, 2015, p. 3)

Arnold and Wade (2015) further discuss the need to learn in new ways as our interdependencies increase. New learning therefore should be couched in a common language and framework to share specialized knowledge, expertise, and experience with experts from other areas of the web; interdependency necessitates systems thinking. While many authors in systems thinking literature express frustration with the slow adoption of the concepts it seems to be based on varied and often conflicting ideas of the concept. Furthermore, while many have discussed the concept, generally specific components and ordering of the components is lacking (Stave & Hopper 2007).

Understanding the impact of actions and connectedness with systems nested inside of bigger systems can be learned; much educational literature on the topic addresses this issue. Some people have an inherent ability to understand how systems work in context with one another. The literature review completed by Stave and Hopper (2007) identified a consensus around seven components that can be used to determine a person's competency in systems thinking:

1. Recognizing Interconnections
The base level of thinking systemically is recognizing that systems exist and are

composed of interconnected parts. …. Recognizing interconnections requires seeing the whole system and understanding how the parts of the system relate to the whole.

2. Identifying Feedback
This characteristic includes the ability to identify cause-effect relationships between parts of a system, describe chains of causal relationships, recognize that closed causal chains create feedback, and identify polarity of individual relationships and feedback loops.

3. Understanding Dynamic Behavior
A key component is understanding that feedback is responsible for generating the patterns of behavior exhibited by a system. This includes defining system problems in terms of dynamic behavior, seeing system behavior as a function of internal structure rather than external perturbations, understanding the types of behavior patterns associated with different types of feedback structures, and recognizing the effect of delays on behavior.

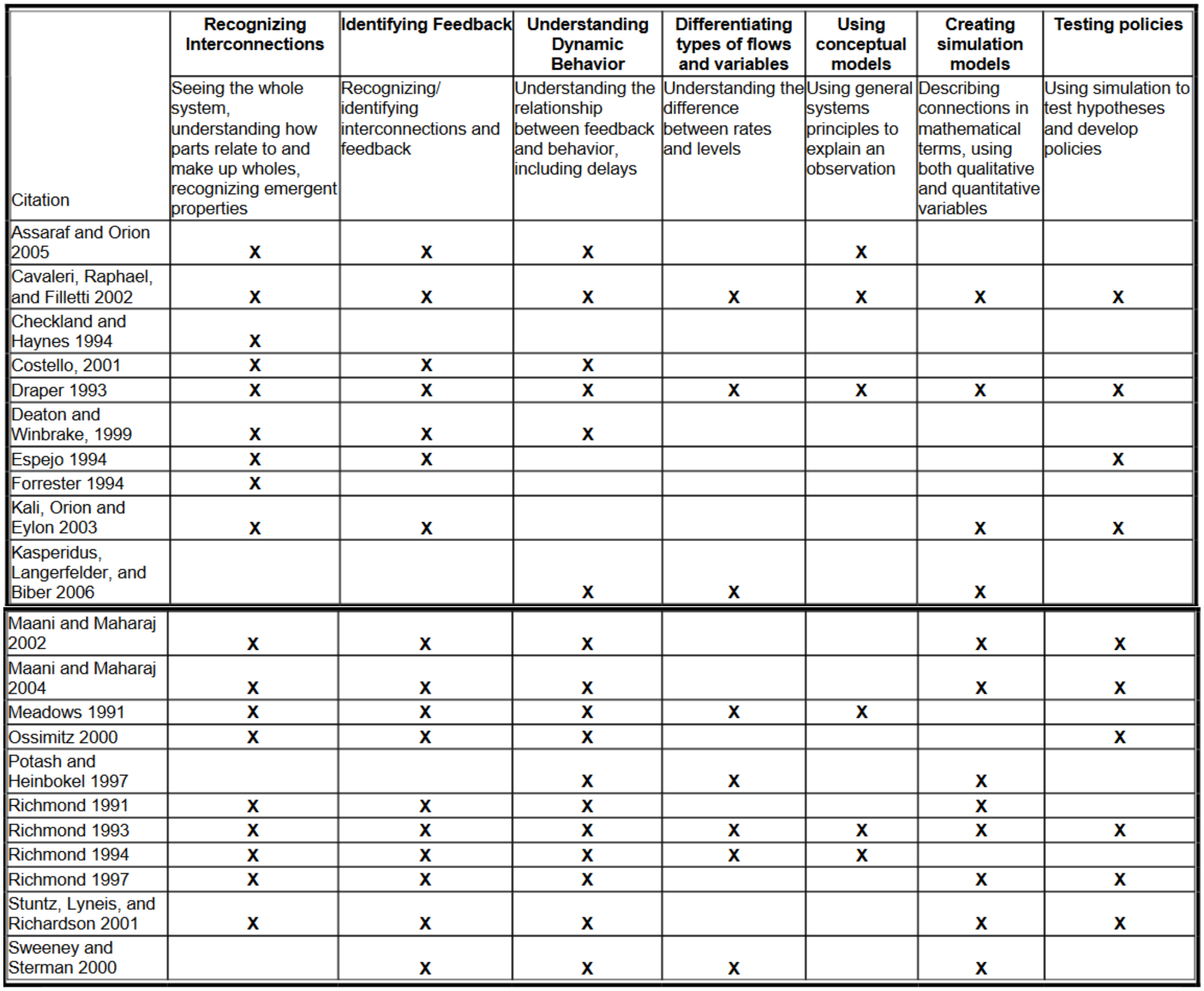
4. Differentiating types of flows and variables
Simply recognizing and being able to describe causal relationships is not sufficient for a systems thinker. Understanding the difference between, being able to identify rates and levels and material and information flow, and understanding the way different variables work in a system is critical.

5. Using Conceptual Models
Being able to explain system behavior requires the ability to synthesize and apply the concepts of causality, feedback, and types of variables.

6. Creating Simulation Models
The ability to create simulation models by describing system connections in mathematical terms is an advanced component of systems thinking according to some authors. Others see simulation modeling as beyond the definition of systems thinking. This category includes the use of qualitative as well as quantitative data in models, and validating the model against some standard. It does not specify which type of simulation model must be used.

7. Testing Policies
… This includes the use of simulation models to understand system behavior and test systemic effects of changes in parameter values or structure.
(Stave and Hopper, 2007, pp. 8-9)

Table 2: Key Characteristics of Systems Thinking (Stave & Hopper, 2007, p. 10)



	Recognizing Interconnections	Identifying Feedback	Understanding Dynamic Behavior	Differentiating types of flows and variables	Using conceptual models	Creating simulation models	Testing policies
Citation	Seeing the whole system, understanding how parts relate to and make up wholes, recognizing emergent properties	Recognizing/ identifying interconnections and feedback	Understanding the relationship between feedback and behavior, including delays	Understanding the difference between rates and levels	Using general systems principles to explain an observation	Describing connections in mathematical terms, using both qualitative and quantitative variables	Using simulation to test hypotheses and develop policies
Assaraf and Orion 2005	X	X	X		X		
Cavaleri, Raphael, and Filletti 2002	X	X	X	X	X	X	X
Checkland and Haynes 1994	X						
Costello, 2001	X	X	X				
Draper 1993	X	X	X	X	X	X	X
Deaton and Winbrake, 1999	X	X	X				
Espejo 1994	X	X					X
Forrester 1994	X						
Kali, Orion and Eylon 2003	X	X				X	X
Kasperidus, Langerfelder, and Biber 2006			X	X		X	
Maani and Maharaj 2002	X	X	X			X	X
Maani and Maharaj 2004	X	X	X			X	X
Meadows 1991	X	X	X	X	X		
Ossimitz 2000	X	X	X				X
Potash and Heinbokel 1997			X	X		X	
Richmond 1991	X	X	X			X	
Richmond 1993	X	X	X	X	X	X	X
Richmond 1994	X	X	X	X	X		
Richmond 1997	X	X	X			X	X
Stuntz, Lyneis, and Richardson 2001	X	X	X			X	X
Sweeney and Sterman 2000		X	X	X		X	

The inclusion of systems thinking in project management has been explored by many researchers (Siriram, 2017), although gaps still exist in this nascent field. Systems thinking has begun to appear in cybersecurity literature generally; however, a paucity of literature exists in the application of systems thinking to ransomware. Yan (2020) provides systems theories and methods for addressing cybersecurity challenges, discounting current cybersecurity models that do not add clarity and provide the holistic nature provided by a systems thinking approach. Knobloch (2019) highlighted issues with the inability of organizational leaders to address behavioral factors for both diffusing and sustaining best practices in healthcare for an initiative called the Systems Engineering Initiative creating a model for reducing infections.

A comprehensive view of the set of networks and information systems used by government agencies, enterprises, critical infrastructure providers, and public administrations is lacking and much needed (Armenia, et. al., 2019). Armenia et al. (2019) sought to extend the focus of cybersecurity issues across the organization, from the executive level to the implementation and operational levels. They further suggest joining the risk categories into a causal mapping of a general process-structure, providing a common ground for discussion at all organizational levels (Armenia, et al., 2019). Given these observations, we suggest that the following research questions are worthy of further exploration:

Research question 1: Can systems thinking thwart and/or protect against ransomware attacks?

Research question 2: Does a hybrid approach to systems thinking address the potential for ransomware and future technology usage driven attacks?

An initial approach to addressing these research questions would be to include case studies and/or grounded theory, ideally contrasting organizations using a systems (hybrid) approach to ransomware attacks with organizations that do not take that approach. These research approaches could then be expanded/tested with larger-scale surveys of numerous organizations of various sizes and industries to test the generalizability of any earlier research findings.

Future considerations and recommendations

While there are many challenges in the ever-changing ransomware threat landscape, we suggest that systems thinking be considered as a key component of cybersecurity modeling to find, characterize, understand, evaluate, and predict cybersecurity ransomware more specifically. A foundational understanding regarding ransomware and attack trends were also highlighted in addition to suggesting systems approach for deterrence. The systems thinking approach is interdisciplinary and shows promise in project management literature to provide a layered framework in coordination with other cybersecurity tools and frameworks outlined. A systems thinking approach can and should be taught in organizations for employees at all levels to understand their role within the overall system regarding regards to cybersecurity behaviors.

Ransomware is not just a financial threat to organizations and individuals. In this regard the National Security Agency Cybersecurity Director notes: “Our adversaries are targeting all levels of U.S. Government, critical infrastructure, industry, academia, private citizens and our allies. This is a shared threat that requires us all to work as a coalition with a common goal.” (Joyce, in National Security Agency, 2022, p 3). This quote not only highlights the wider threats posed by ransomware (and cybersecurity threats in general) but also emphasizes the need for a collaborative approach to dealing with such threats. The systems approach that we proposed is ideally positioned as a framework for such collaboration as it identifies both the impacts and interconnectedness of key actors within the realms of ransomware.

References

Armenia, S., Ferreira Franco, E., Nonino, F., & Spagnoli, E. (2019). Towards the definition of a dynamic/systemic assessment for cyber security risks through a systems thinking approach. *Proceedings of the 61st Annual Meeting of the ISSS - 2017 Vienna, Austria*, *2017*(1). https://journals.isss.org/index.php/proceedings61st/article/view/3198

Arnold, R. D., & Wade, J. P. (2015). A definition of systems thinking: A systems approach. *Procedia Computer Science*, *44*, 669–678. https://doi.org/10.1016/j.procs.2015.03.050

Barker, W., Scarfone, K., Fisher, W., & Souppaya, M. (2021). Cybersecurity Framework Profile for Ransomware Risk Management (NIST Internal or Interagency Report (NISTIR) 8374 (Draft)). *National Institute of Standards and Technology.* Retrieved as https://www.aha.org/system/files/media/file/ 2021/06/nist-cybersecurity-framework-profile-for-ransomware-risk-management-6-2021.pdf

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, *111*, 102490.

Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network Security, 2016*(9), 5-9.

Brooks, C. (2021). More alarming cybersecurity stats For 2021!. *Forbes,* October 24, 2021. https://www.forbes.com/sites/chuckbrooks/2021/10/24/more-alarming-cybersecurity-stats-for-2021-/?sh=17b1f02d4a36 on March 16, 2022.

J. -C. Cheng, N. -Y. Lee, C. Chi and Y. -H. Chen, "Blockchain and smart contract for digital certificate," *2018 IEEE International Conference on Applied System Invention (ICASI)*, 2018, pp. 1046-1051, doi: 10.1109/ICASI.2018.8394455.

Collier, R. (2017). NHS ransomware attack spreads worldwide. *Canadian Medical Association Journal, 189*(22), 786-787.

Crowdstrike (2022). *2022 global threat report.* https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2022GTR.pdf.

Cybersecurity and Infrastructure Security Agency and Others (2022, February 9). 2021 trends show increased globalized threat of ransomware. Joint Cybersecurity Advisory. https://media.defense.gov/2022/Feb/09/2002935687/-1-1/0/2021_TRENDS_SHOW_INCREASED_GLOBALIZED_THREAT_OF_RANSOMWARE_20220209.PDF

Dickson, F., & Kissel.C. (2021). IDC's 2021 Ransomware study: Where you are matters! *IDC Research.* https://www.idc.com/getdoc.jsp?containerId=US48093721

FireEye (2020). Cyber trendscape. https://www.fireeye.com/offers/rpt-cyber-trendscape.html

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? *Review of Financial Studies*, *32*(5), 1798-1853. https://doi.org/10.1093/rfs/hhz015

Genç, Z. A., Lenzini, G., & Sgandurra, D. (2021). Cut-and-mouse and ghost control: Exploiting antivirus software with synthesized inputs. *Digital Threats: Research and Practice, 2*(1), 1-23.

Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computers & Security, 24*(1), 31-43.

Kerner, S.M. (2022). Ransomware trends, statistics and facts in 2022. https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts#:~:text=Ransomware%20statistics%20for%202021%20and%202022&text=Approximately%2037%25%20of%20global%20organizations,January%20to%20July%2031%2C%202021 on March 16, 2022.

Knobloch, M. J., Thomas, K. V., Musuuza, J., & Safdar, N. (2019). Exploring leadership within a systems approach to reduce health care–associated infections: A scoping review of one work system model. *American Journal of Infection Control*, *47*(6), 633–637. https://doi.org/10.1016/j.ajic.2018.12.017

McIntosh, T., Kayes, A. S. M., Chen, Y. P. P., Ng, A., & Watters, P. (2021). Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. *ACM Computing Surveys (CSUR)*, *54*(9), 1-36.

National Institute of Standards and Technology (2018, April 16), Framework for improving critical infrastructure cybersecurity.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Security Agency (2022). 2021 NSA Cybersecurity year in review. https://media.defense.gov/2022/Feb/03/2002932462/-1/-1/0/2021_NSA_CYBERSECURITY_YEAR_IN_REVIEW.PDF

Osborne, C. (2021). Updated Kaseya ransomware attack FAQ: What we know now. https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/ on March 16, 2022.

Pagán, A., & Elleithy, K. (2021). A multi-layered defense approach to safeguard against ransomware. *2021 IEEE 11th Annual Computing and Communication Workshop and Conference Proceedings*, 942-947.

Pérez-Sánchez, A., & Palacios, R. (2022). Evaluation of local security event management system vs. standard antivirus software. *Applied Sciences, 12*(3), 1-18.

Pranggono, B., & Arabo, A. (2020). Covid-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2). https://doi.org/10.1002/itl2.247

Ransomware.org (2022). Ransomware defined: Breaking down ransomware. https://ransomware.org/what-is-ransomware

Reshmi, T. R. (2021). Information security breaches due to ransomware attacks-a systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100013.

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review, 13*(1), 10-21.

Richmond, B. (1991) Systems thinking. Four key questions. Watkinsville, GA: High Performance Systems.

Richmond, B. (1994). Systems thinking/system dynamics: Let's just get on with it. *System Dynamics Review*, *10*(2-3), 135–157. https://doi.org/10.1002/sdr.4260100204

Rieck, K., Holz, T., Willems, C., Düssel, P., & Laskov, P. (2008). Learning and classification of malware behavior. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment.* Berlin, Germany.

Segura, J. (2016). Citadel: a cyber-criminal's ultimate weapon? Malwarebytes Labs, March 30, 2016. https://blog.malwarebytes.com/threat-analysis/2012/11/citadel-a-cyber-criminals-ultimate-weapon/ on March 16, 2022.

Siriram, R. (2017). A hybrid (soft and hard) systems approach to project management. *International Journal of Industrial Engineering*, *4*(6), 1–16. https://doi.org/10.14445/23499362/ijie-v4i6p101

Stave, K., & Hopper, M. (2007, July). What constitutes systems thinking? A proposed taxonomy. In *25th international conference of the system dynamics Society*.

Sokolov, K. (2021). Ransomware activity and blockchain congestion. *Journal of Financial Economics, 141*(2), 771-782.

Tailor, J. P., & Patel, A. D. (2017). A comprehensive survey: Ransomware attacks prevention, monitoring and damage control. *International Journal of Research and Scientific Innovation, 4*, 116-121.

Thomas, J., & Galligher, G. (2018). Improving backup system evaluations in information security risk assessments to combat ransomware. *Computer and Information Science, 11*(1), 14-25.

Thomas, J. E. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business and Management, 13*(6).

Verizon (2021). Data breach investigations report. https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis.

Yan, D. (2020). A Systems thinking for cybersecurity modeling. *arXiv preprint arXiv:2001.05734*.