System Dynamics Modeling of Ransomware Incidents

Marcus Miller[a]* and Dr Navid Ghaffarzadegan[a]

[a]*Industrial and Systems Engineering, Virginia Tech, Blacksburg, Virginia, USA*

Correspondence details: *Marcus Miller, Email: marcusm83@vt.edu

Dr Navid Ghaffarzadegan, Email: navidg@vt.edu

Marcus Miller – Marcus is a PhD candidate in Industrial and Systems Engineering at Virginia Tech focusing on management systems engineering. A retired United States Air Force colonel with leadership, staff, and engineering experience, he served as a sales leader for an IT solution firm after retirement from the Air Force and is currently a systems/project engineer for a defense contractor. Marcus earned an M.S. in National Security Studies from the National War College, a M.S. in Electrical Engineering from the University of Illinois – Urbana Champaign, and a B.S. in Electrical Engineering from the US Air Force Academy.

Dr Navid Ghaffarzadegan – Navid is an associate professor in the Department of Industrial and Systems Engineering at Virginia Tech. His research interests include systems sciences and applications of system dynamics modelling in various managerial and policy contexts such as service enterprises, higher education, science policy, and health policy. Navid's research has been supported by various organizations such as NIH, and corporates such as Dell, Inc. Navid is currently the Associate Editor of the System Dynamics Review. He is the winner of various awards including the College of Engineering's excellence award for outstanding new Assistant Professors. Prior to joining Virginia Tech, Navid was a postdoctoral researcher at MIT, Engineering Systems Division. He earned a Ph.D. in Public Policy (System Dynamics) from State University of New York at Albany, an M.B.A., Management (System Dynamics) from Sharif University of Technology, and a B.S. in Mechanical Engineering from Sharif University of Technology.

Abstract

Ransomware threatens damaging economic, social, and other real-world consequences. This is especially grave for certain sectors of the economy that provide critical services and handle sensitive data – and may not be well-prepared to defend against hackers accessing their networks and holding data or operations at bay until a ransom is paid. We show that system dynamics modeling can be applied to baseline the ransomware ecosystem, explain past patterns, and provide insight into policy decisions. Simulation showed improvement by increasing incident reporting, reducing reporting delays, and strengthening passive defenses. We also identify suggestions for future research.

Keywords: Ransomware, cybersecurity, system dynamics modeling, hacker gangs, ransomware gangs, ransomware as a service

System Dynamics Modeling of Ransomware Incidents

Introduction

Cyber-attacks threaten corporate operations and finances, personal security and privacy, the functioning of the global economy, the resilience of national infrastructures, and overall confidence in government and social relationship (Jaikaran, 2021; King & Gallagher, 2020; Portman & Peters, 2021).

A specific form of cyber-attacks, ransomware, defined as an activity where "criminals remotely compromise computer systems and demand a ransom in return for restoring and/or not exposing data" (Ransomware Task Force, 2021), poses the threat of widespread damaging economic, social, and other real-world consequences (Liska, 2021; Ransomware Task Force, 2021; Rudis, 2022; Wuest, 2022). With a 74% increase from 2020 to 2021 in worldwide costs of ransomware (SonicWall, 2022) and a 35% increase in the average ransom payment from 2021 to 2022 (Coveware, 2023) ransomware has gained attention as an urgent global issue (Barlet, 2023; Page, 2022). The threat of ransomware is particularly concerning for the relatively undefended sectors burdened with legacy IT capabilities – principally health care, education, and municipal governments – that also handle and retain sensitive data and play an important role in the welfare and functioning of society (Poulsen & Evans, 2021; Warner, 2022).

The ransomware ecosystem involves an array of actors, stakeholders, tools, techniques, and business models competing for valuable digital assets traversing networks and stored in organizational data bases, on-premises or in the cloud. The actors and stakeholders – asset bearing organizations, IT and cyber security professionals, hacker gangs along with their affiliates and supporting infrastructure providers, law enforcement and insurance underwriters – must constantly consider the benefits and costs in capability investments, defensive or offensive. And the defenders must also consider the operational and financial risks of forsaking those investments or of securing third-party insurance arrangements to transfer the risk of ransomware.

Global governments and the private sector are rushing to combat ransomware (Ransomware Task Force, 2021) with promising progress and but still unclear attribution of success to those actions (Chainalysis Team, 2023; Comizio et al., 2023; Coveware, 2022d; Greig, 2023; Lyngaas, 2023). Greater holistic insight into effects, second order effects, and the overall solution trade-space, including technical, legal, and business, can help shape governments' priorities, policies, and actions in response to this global problem (Comizio et al., 2023; Robles-Carrillo & García-Teodoro, 2022a).

Cyberspace may be virtual, but it is home to real-world, inherently global problems. As more human activities and supporting structures move online, we must adapt to change and address challenges that arise in this virtual environment. While cyberspace is a complex system or system of systems, the right tools and techniques can be leveraged to guide society's adaptation and intervention. As will be shown in this paper the application of system dynamics modeling can help shape policies for a better future that can be less threatened by nefarious actors in cyberspace. This paper seeks to explain how system dynamics modeling can be used to baseline the global ransomware ecosystem, explain past patterns, and provide insight into future policy decisions.

Research Problem

Ransomware Threat

Table 1 lists several key ransomware threat details and statistics for the United States and worldwide. While by some measures the pace of attacks and the damage experienced may have alleviated some in 2022, it is still a major concern and early evidence of 2023 data suggests a return to the previous highs. Regardless, it remains a top concern for leaders of large, medium, and small businesses and organizations in all sectors, cybersecurity professionals, law enforcement, government leaders at all levels, and insurance providers.

Table 1 Ransomware Threat Summary

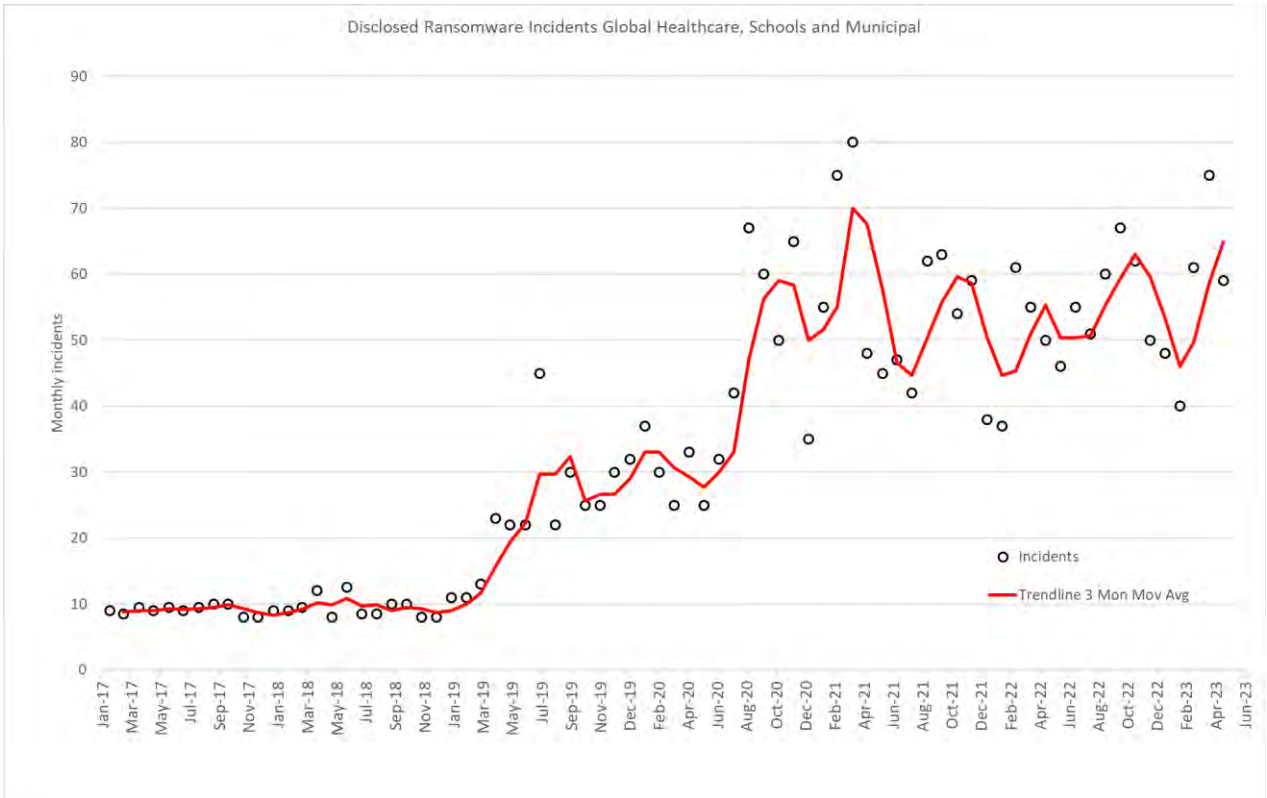
Data Characterizing Extent and Impact of Ransomware	Year	Source Citation
Ransomware is the fastest growing cybercrime model	2022	(Brooks, 2022)
Ransomware attacks increased 80% YoY	2022	(Page, 2022)
Global cost of ransomware increased 74% YoY	2021	(Claroty, 2020)
Average ransom payment was $408,644 a 26% QoQ increase (Q4)	2022	(Coveware, 2023)
US financial institutions report seeing $1.2B in ransom payments	2021	(Vicens, 2022)
Ransom payments account for just 15% of the total cost of an attack	2021	(Blosil, 2022)
Total global annual cost of ransomware damage $20B	2021	(Chang, 2023)
90% of organizations hit by ransomware saw impact on operations	2021	(Sophos, 2022)
~37% of global organizations were victims of ransomware attacks	2021	(Snape, 2022)
80% of critical infrastructure entities were attacked by ransomware	2021	(Singleton et al., 2020)
Government organizations account for 13% of ransomware attacks	2021	(Sobers, 2022)
66% of healthcare organizations had at least one ransomware attack	2021	(Sophos, 2022)
US hospitals/public health account for 25% of reported ransomware	2023	(Benvenisti, 2022)
44% of ransomware attacks against healthcare disrupted delivery ops	2022	(Vijayan, 2023)
Healthcare industry hit by ~$25B cumulative costs from ransomware	2019	(SafeAtLast, 2022)
45M people were impacted by attacks on the healthcare sector	2021	(Warner, 2022)

Global statistics paint one picture of a serious concern, but the recent anecdotal evidence of ransomware incidents, especially in healthcare, education, and municipal governments is even more compelling.

- According to news reports of an “unprecedented” attack, CommonSpirit Health, the second largest non-profit hospital chain the US with 140 hospitals and 1000 care sites situated across 21 states experienced a suspected ransomware attack in Fall 2022 impacting electronic health records, ambulance services, and appointment scheduling (Starks, 2022b).
- An attack on IT services provider Advanced in 2022 left the UK’s NHS scrambling after it was forced to cancel appointments and rely on pen and paper for notes (Page, 2022).
- A breach of Australian health insurance giant Medibank in 2022 resulted in hacker access of nearly 10M customer records and almost 500K patients’ health claims data (Page, 2022).
- An email intrusion led to a ransomware attack on Ireland’s public-health infrastructure with devastating consequences in Spring 2021 (Krebs, 2021b).
- A ransomware attack in Sep 2020 on Universal Health Services, one of the largest U.S. hospital chains, halted computer access at ~250 hospitals, emergency rooms and outpatient centers. While a ransom wasn’t paid, it still cost $67M for a weeks’ long recovery (Poulsen & Evans, 2021).
- As a result of WannaCry, the first major global ransomware attack in 2017, UK’s NHS faced a $100M recovery costs with disruptions in 80 hospitals impacting 19,000 patients (Starks, 2022b).

- An attack on the Los Angeles Unified School District in Fall 2022 resulted in a 500 GB leak of sensitive student data (Page, 2022).
- Lincoln College, an historically black university, was forced to close in 2022 after 157 years blaming both COVID-19 and ransomware attacks (Chung, 2022).
- Long Island was forced to conduct business 1990s style for over two months in Fall 2022 with no online systems beyond FAX and phones – a "cybermorass" (Maslin Nir, 2022).

Figure 1 depicts the growth of ransomware attacks against healthcare, education, municipal governments annually from 2017 through mid-year 2023, illustrating a high rate of growth till late 2021, a short period of high volatility followed by a steady high level of incidents through May 2023. This trend data is unique to these three sectors. The source for this trend data is RecordedFuture.com (a cybersecurity analysis company).

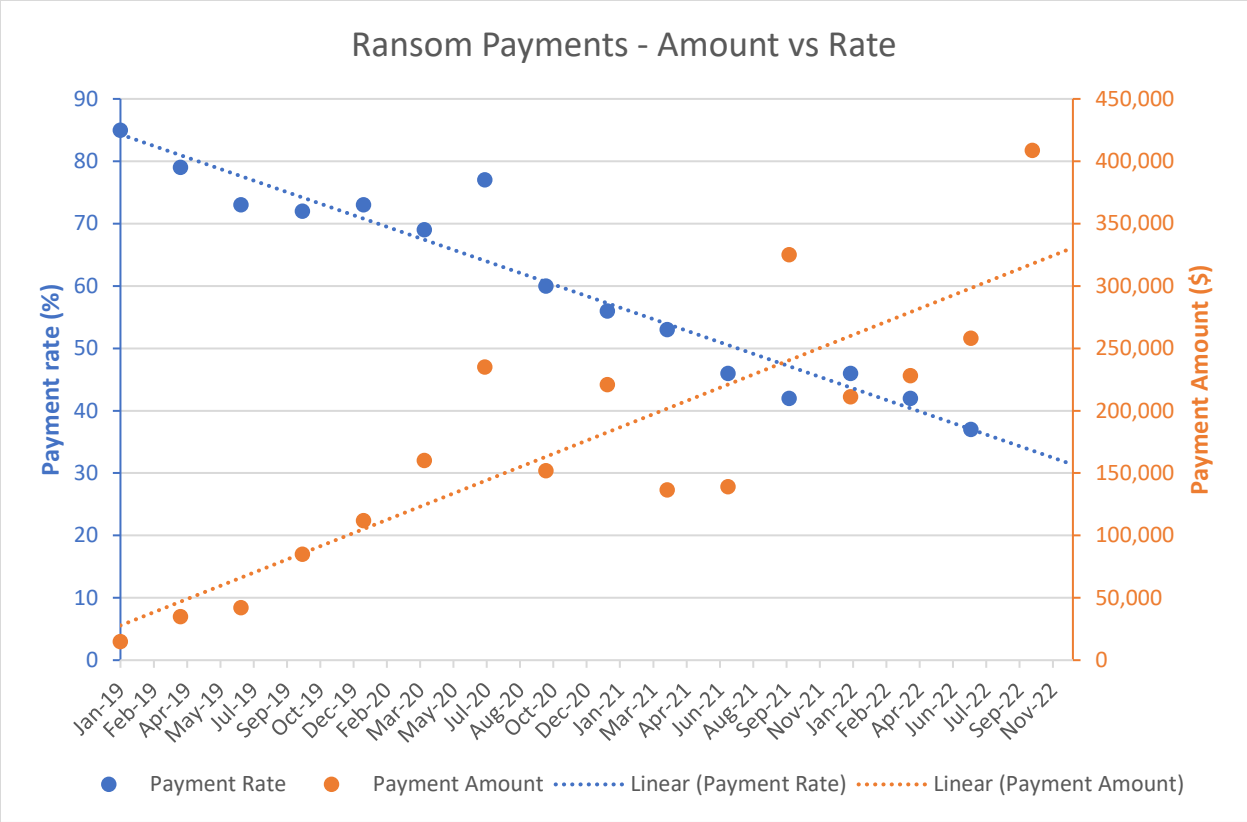


Source: (Janofsky, 2023; Liska, 2022)

Figure 1 Ransomware Attacks Against Healthcare, Education, and Municipal Governments

The growth and variation in reported ransomware incidents starting in March 2019 as seen in Figure 1 could be due to any number of factors or developments but those are best explored in detail after an explanation of the ransomware ecosystem.

Figure 2 shows the trend data for ransom payments from Jan 2019 through Dec 2022.



Source: (Coveware, 2022c)

Figure 2 Ransom Payment Rate versus Average Ransom Payment

The diverging trends in ransom payment rates and average ransom payments since January 2019 (Figure 2) also pose a perplexing and critical situation demanding investigation and policy responses. In this paper we will probe this problem set, the key statistics that characterize this problem, the underlying factors, and the impact of potential policy actions.

Ransomware Ecosystem

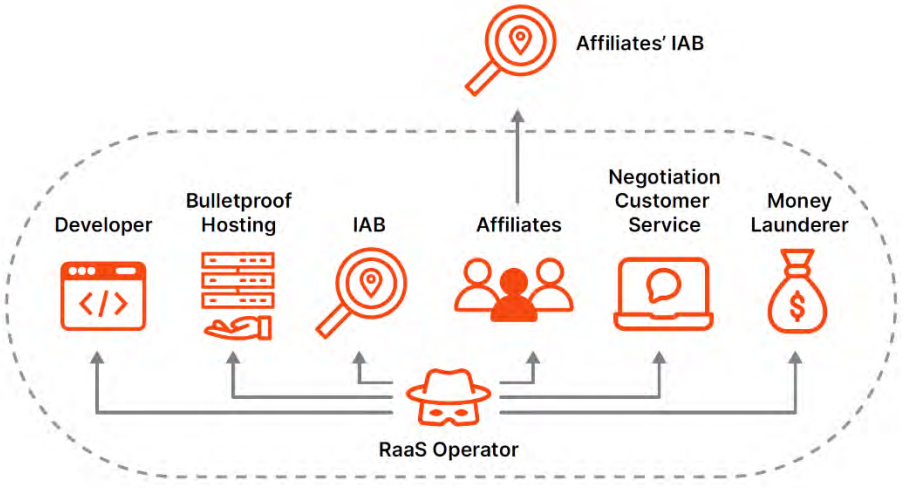
Before elaborating on the problem statement, research objectives, and research methods for this paper we will examine this problem and the underlying ecosystem in greater detail. While this section and the supporting appendix is not meant to be a comprehensive survey of the ransomware problem it should provide a high-level summary needed to help understand later elements of our research.

As noted in the previous section, ransomware is a serious threat to the cyber ecosystem and the activities existing in it or supported by it. It is also multifaceted, highly complex, and devious. The connective links, relationships, and influences are many and varied. Appendix A offers extensive detail on the ransomware ecosystem, but a brief overview is provided in the following.

Potential targets are organizations with a business/operational/customer-facing presence online or supporting activities accessible via private information technology networks and data storage networks typically connected to the internet. Over the last decade organizations have been increasingly leveraging cloud-based business applications and data storage in lieu of their own corporate or private networks. The central premise of the ransomware ecosystem is that organizational data stored or accessible online is ultimately vulnerable to network intrusion and unauthorized access. Once inside the network, hackers can encrypt the organization's data to prevent use or access of the data or operational assets (software)

until a ransom is paid. The victim may choose to pay the ransom and potentially receive the decryption key or refuse the ransom. If the decryption key is not obtained or provided the organization must either rebuild the data assets, software applications, and/or network infrastructure from scratch or from information assets stored in a secure, independent location. Following the attack, regardless of ransom resolution, the victim may or may not report the incident to law enforcement authorities. Additionally, the victim may or may not have had insurance coverage for cybersecurity events or malfeasance that could be applied in the event of a ransomware incident (Collier, 2021; Liska, 2021; Livinston, 2022).

At the crux of the ecosystem are the hacker groups or gangs. These loosely aligned global teams receive some level of support or enablement from the governments of Russia, Iran, and/or North Korea. Key factors behind the ability of these criminal organizations to generate and sustain ransomware attacks include gang member expertise, hacker tools, data encryption techniques, supporting infrastructure, payment infrastructure, business models, alliances, and means of covert coordination. The types of Hacker activities include: develop strains, prioritize targets, surveil targets, probe networks, attempt intrusions, access data, encrypt data, and announce possession and ransom demands (Al-rimy et al., 2018; Baker, 2022; Collier, 2021; Dudley & Golden, 2022a; Farhat & Awan, 2021). The emergence of ransomware as a service (RaaS) business model lowered the threshold for technical expertise required to conduct ransomware attacks and thus expanded the pool of criminal operatives in this arena, while reducing the overall cost to execute an attack through repeatable, extensible processes (Baker, 2022; Beaman et al., 2021; Coveware, 2022a; Hacquebord et al., 2022; Kok et al., 2019; Liska, 2021; Meland et al., 2020; O'Kane et al., 2018; *Ransomware as a Service: Understanding the Cybercrime Gig Economy and How to Protect Yourself | Microsoft Security Blog*, n.d.; *The Ransomware Ecosystem - RaaS, Extortion, Cryptocurrency*, n.d.; Richardson & North, 2017). Figure 3 highlights the key elements of the ransomware hackers' infrastructure, based on the RaaS business model, including attack vector developers, hosting infrastructure, internet access brokers (IAB), partner affiliates (traditional hacker gangs), negotiation services/portals, and payment infrastructure (usually Bitcoin based) (Liska, 2021).



Source: (Liska, 2021)

Figure 3 Ransomware Attack Elements for a Ransomware as a Service Infrastructure

Organizations with less attack surface and strong cyber defenses, can deter hackers and reduce the likelihood of successful attacks (Livinston, 2022; Robles-Carrillo & García-Teodoro, 2022a). Basic cyber security hygiene and the implementation of the latest software patches are also key. Cyber defenses include the employment of cybersecurity tools, network monitoring and reaction processes, and end user

awareness of hacker techniques and recommended actions. Cybersecurity capabilities can be either in-house or leveraged from third parties (Trim & Upton, 2016). Prior to attacks firms may also take specific ransomware mitigation and recovery measures to reduce severity, duration, and total cost of ransomware events (Richardson & North, 2017).

Once an organization is attacked, its data encrypted and ransom demanded, the victim may opt to pay the ransom and hope that the decryption keys are provided, or refuse demands, mitigate damages from any unauthorized release, and recover operations from backups or rebuilding the infrastructure and applications (Dudley & Golden, 2022a). Key metrics that assess the overall scope and scale of the problem include incident reporting rate, incident reporting delay, ransom payment rate, average payment amounts, total costs of ransomware attacks, and sectors and asset size of victim organizations (Chang, 2023; Cook, 2022; Insikt-Group, 2023; Livinston, 2022).

The ecosystem also includes the insurance industry providing unique ransomware or cybersecurity coverage protection, private sector non-profit or for-profit anti-ransomware organizations/partnerships, plus local and national law enforcement activities backed up by government cybersecurity agencies (Dudley & Golden, 2022b; Haughey, 2022; Johnson, 2023; Robles-Carrillo & García-Teodoro, 2022a). Insurance coverage is a key part of the ecosystem enabling and supporting victims in negotiating with ransomware gangs, enforcing cybersecurity protection standards as part of acquiring coverage, and providing victims with the financial backing to recover operations and business losses if ransom demands are not paid (Pratt, 2022; Woods, 2023a).

Problem Statement

The complexity of the ransomware ecosystem defies easy understanding and problem solving (Ransomware Task Force, 2021). A variety of factors can impact the extent and severity of ransomware and decision makers need to precisely understand how policy choices impact outcomes. Certain solutions may appear obvious, but the underlying dynamics and potential ramifications across the complex system need to be fully understood.

For example, the slowdown in ransomware incidents against healthcare, education, and municipal governments starting in Q3 2021 shown in Figure 1 is uniquely perplexing as the change could be due to any number of factors. Figure 3 shows the trend data in Figure 1 again, this time with notes to explain or hypothesize behavior in certain periods. Periods of interest include the consistent rapid growth starting in March 2019 potentially coinciding with the increased use of ransomware as a service (Baker, 2022; Coveware, 2022a) and recognition of these sectors as particularly vulnerable (Branch et al., 2019; Coveware, 2022c; Jalali & Kaiser, 2018; Poulsen & Evans, 2021; Ransomware Gangs' Favorite Targets, 2022), the growth in online activity and remote work during the start of Covid-19 in the spring of 2020 (Beaman et al., 2021; LaBerge et al., 2020), and then the peak of incidents in late 2021 and 1H/2022 followed by increasing variability. Hypotheses for this variation include the distractions and divergent priorities arising from the developing or start of the Ukraine War, the drastic drop in the price of Bitcoin, the elimination of several dominant hacker groups, heightened risk of law enforcement activity, continued reductions in ransom payment rates, and dislocations in crypto payment methods (Gillum, 2022; Kim, 2022; Marks, 2022; Starks, 2022a, 2023a; Uberti, 2021; Waldman, 2022). However, by early 2023, it was clear that the ransomware hacker gangs were still quite active, and that ransomware remained a threat (Editorial Board, 2023; Insikt-Group, 2023; Janofsky, 2023; Newman & Burgess, 2023; Sakellariadis, 2023; Starks, 2023a, 2023b).

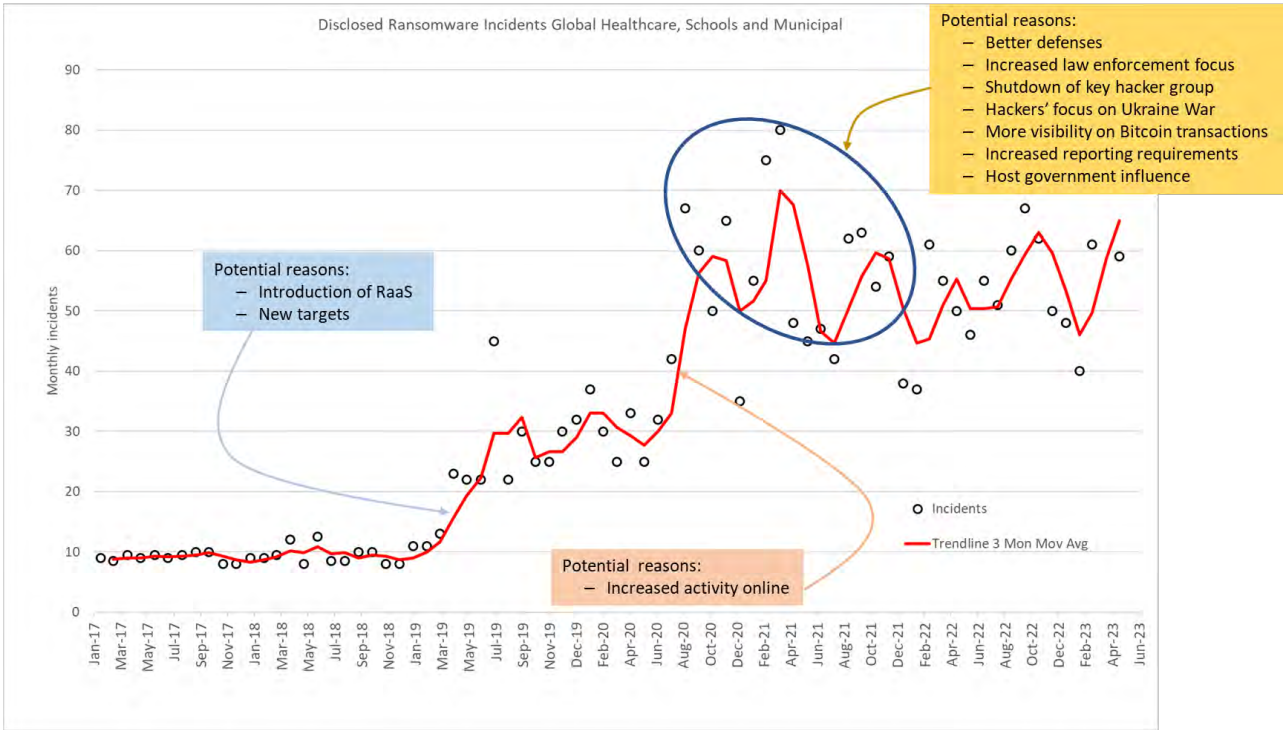


Figure 4 Reported Ransomware Incidents with Behavior Highlights

Governments across the globe seek to reduce or mitigate this problem. However, solid understanding of the problem should precede or at least accompany action. Given the wide variety of factors involved in this complex arena and the range of reasonable policy actions, what is behind the recent volatility in the reported incident data and which policies have the most potential going forward? Thus, our problem statement: *Given the unexplained variation in recent ransomware trend data, are government policy decisions and actions successful in reducing the problem and what other approaches have promise?*

Research Objective

Given the research problem discussed above, the objective of this research is two-fold. First, we seek to better explain the pattern of ransomware incidents reporting from 2017 to mid-year 2023. The changes in time series data (growth, variation, static) can be grouped into distinct epochs, perhaps with unique reasons that can be traced back to specific underlying variables and changes in their parameters. Second, we will assess the impact of current government and private sector actions on the ransomware problem and craft a mechanism to reliably predict the impact of potential policies and actions.

Our research will leverage systems thinking methodologies – and specifically system dynamics modeling and simulation. The focus Is on the use of data, data analysis, and modeling in support of major cyber security decisions by decision makers. We aim to show that system dynamics modeling can be a useful mechanism to help understand this complex cybersecurity problem and bound the range of effective solutions.

In this effort we examine trend data, investigate measures of key variables, model relationships, and simulate both the current baseline and future scenarios for the problem of ransomware. Based on modeling and simulation, we will assess both current measures being employed and potential policy decisions to improve results/outcomes in this arena.

Research Method

System Dynamics Modeling

Ransomware is a complex problem involving many dimensions, actors, decision makers, stakeholders, operational and mission/business equities, and intricate relationships and dependencies. Fortunately, systems thinking offers value in understanding the environment, factors, and interactions for complex socio-economic problems. Accordingly, this research effort will develop, validate, and apply systems thinking and system dynamics modeling to the ransomware problem scenario.

We employ system dynamics modeling against this problem set because this technique has proven effective in examining solutions to complex social, managerial, and economic systems through a holistic a view of systems' organizational structures, decomposed elements, key variables, and major processes (Forrester, 1961, 2022; Sterman, 2000).

Moreover, system dynamics modeling has been previously applied to cybersecurity modeling. By examining prominent research involving cyber security and system dynamics modeling we can understand what has been accomplished, what appears to be most useful and applicable, and where gaps remain as to our interests. One focus of prior research concerns modeling the complexities of deploying and maintaining cybersecurity capabilities of an organization, specifically the key challenges or obstacles in capability development, how these capabilities may be established and evolved, and how they might erode over time (Jalali & Kaiser, 2018). System dynamics modeling also proved useful in a simulation game to help decision-makers overcome biases in capability development and address specific challenges of deployment delays and threat uncertainties (Jalali et al., 2019). System dynamics modeling has also been used to simulate the actual behavior of a complex information system network with cybersecurity protections (Kannan & Swamidurai, 2019). Another focus area of system dynamics modeling regards insider threats, addressing mostly the root causes leading to heightened risk and potential mitigation approaches (D. Andersen et al., 2004; Martinez-Moyano et al., 2008; Yang & Wang, 2011) The last focus area applies systems thinking with comprehensive system dynamics models to examine the value of investments in cybersecurity and optimize the firm's investment strategies (Nazareth & Choi, 2015; Oosthuizen et al., 2019). While these three models restricted the system boundaries to those factors under the firm's control, they could be starting point(s) for a model focused on responses to the ransomware threat.

Development and Simulation Approach

We examined a specific cyber security threat – ransomware in health care, education, and local government sectors – and applied systems thinking to explain the pattern of incidents and examine different policy scenarios. Our approach is detailed in Table 3. Information from technical reports, government documents, and cybersecurity threat updates were gleaned to create a detailed conceptual perspective of the ransomware ecosystem and its behavior. We built a simulation model that could be used to understand and evaluate a variety of potential policies and interventions to address this threat. After validating and calibrating the model with real world data, we adjusted parameters associated with alternative policy scenarios to estimate, understand, and evaluate the potential change in outcomes. Besides understanding policy implications in our simulation-based what-if analysis, we also want to confirm the causes and identify any unintended consequences of the proposed policies. Ultimately, our objective is to explore proper policies that can help minimize long-term threats and costs of ransomware.

Table 2 Development and Simulation Approach

Major Activity	High Level Description	Specific Actions
Problem Framing	Investigate and define the ransomware problem and ecosystem	Identify and scope the ransomware problem
		Identify major problem indicators and how those have changed over time; collect time series data
		Identify key actors and stakeholders in the ransomware ecosystem and understand their roles and equities
		Identify the factors or variables associated with the problem; collect time series data
		Examine the major actions taken or proposed to address the ransomware problem
		Conceptualize system structure in a level diagram
		Review prior system dynamics research in cybersecurity
Dynamic Hypotheses and Causal Structure	Create a structure to visualize relationships, causes, and effects in the ransomware ecosystem	Develop hypotheses of causes, effects, and feedback loops
		Create causal structure of the key aspects of the ransomware ecosystem
		Define potential feedback loops to explain balancing and reinforcing actions
		Set model boundaries and categorize variables as endogenous or exogenous
Model Formulation	Create a model that simulates key relationships and feedback mechanisms in the ransomware ecosystem	Leverage previous causal diagram as foundation for simulation model
		Establish system structure - identify and associate “stocks” and “flows”
		Iteratively build and test model, key sections at a time
		Develop feedback loops to explain balancing and reinforcing actions; verify correct performance
Model Calibration	Optimize model parameters	Review classification of variables constant and dynamic and as exogenous and endogenous
		Document average and min-max ranges of existing data for key variables
		Iteratively calibrate parameters of key variables to create best fit of model outputs with historical time series data
Model Validation	Ensure model adequately simulates real-world as reflected in available data	Compare simulated model outputs (stocks and dynamic variables) with available data
		Run simulations of baseline futures
Policy Analysis	Apply the model to examine and predict effectiveness of policy decisions	Identify potential policy scenarios
		Run simulations of potential policy scenarios
		Compare simulations with baseline futures
		Assess success of alternative policy initiatives
		Document and explain results

`

Since the problem framing step was discussed in the previous section, the remaining portion of this paper will cover the development of our system dynamics model of ransomware, specifically its creation, verification, validation, and simulation, followed by its application to analysis of specific policies.

Model Overview

The model follows from the information summarized in Table 2 introduced previously and starts with a diagram showing the structure, relationships, and influences between the key elements in the ecosystem. Key elements of this diagram include ransomware incidents (actual & reported), targeted assets, payment infrastructure, hacker gangs, cyber defense systems, government, and insurance agencies.

The following discussion explains the system dynamics model used to simulate the ransomware ecosystem. The model strives to capture as many of the key real-world factors as practical. This section describes the structure, functionality, and operational behavior of the model section by section. The ultimate purpose of this portion of the paper is to explain, rationalize, and verify each key element of the model. The following lists the reinforcing and balancing feedback loops in the model. We will build out the model step by step and explain the role of each feedback loop.

Reinforcing Loops

R1 – Revenue Drives Growth

R2 – Insurance Pays Hackers

R3 – More Incident Reporting Drives Insurance

R4 – Digital Asset Growth

Balancing Loops

B1 – Risk Response

B2 – Attack Hackers

B3 – Capacity Adjustment

B4 – Insurance Covers Damage

B5 – Public Report Obligation

B6 – Insurance Mandates Cyber Protections

B7 – Price Adjustment

B8 – Target Adjustment

B9 – Insurance Pays Out More

B10 – Defenses Mitigate Attack Damages

Figure 5 shows the first level of the ransomware system dynamics model.

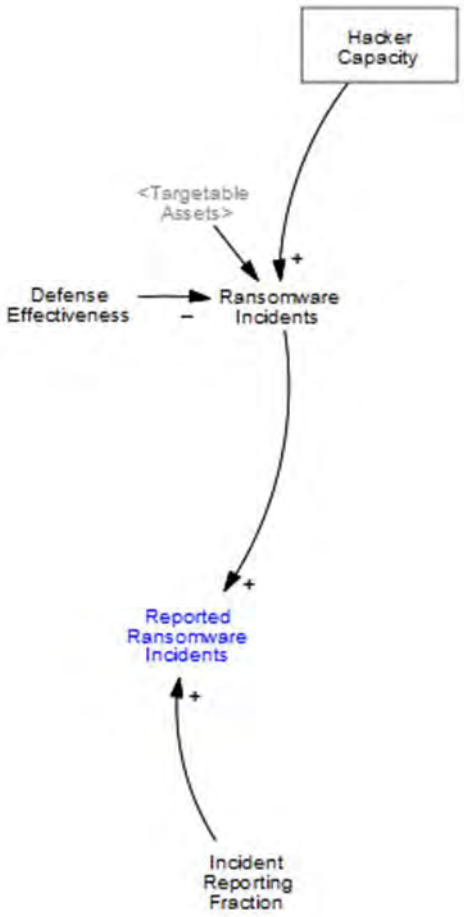


Figure 5 Ransomware Model Build 1

This initial buildup figure shows the creation of ransomware incidents resulting from the interaction of hacker capabilities and defense effectiveness. Ransomware incidents are core to the rest of the model as it drives revenue needed for future capabilities as well as sets the risk framework underlying defense capability development. The equation for ransomware incidents is expressed as follows:

Ransomware Incidents = (1 – Defense Effectiveness) * Min (Hacker Capacity, Targetable Assets)

This is the core equation in the model. Ransomware Incidents is the output of Defense Effectiveness, Hacker Capacity and Targetable Assets. Incidents result if targeted digital assets are not covered by the firm or organization's defense capabilities. With this equation the model generates incidents tempered by the effectiveness of defenses, the level of targetable assets, and the capacity of the hacker gangs to sustain attacks.

The addition of defense capabilities as seen in Figure 6, Model Build 2, involves two balancing loops.

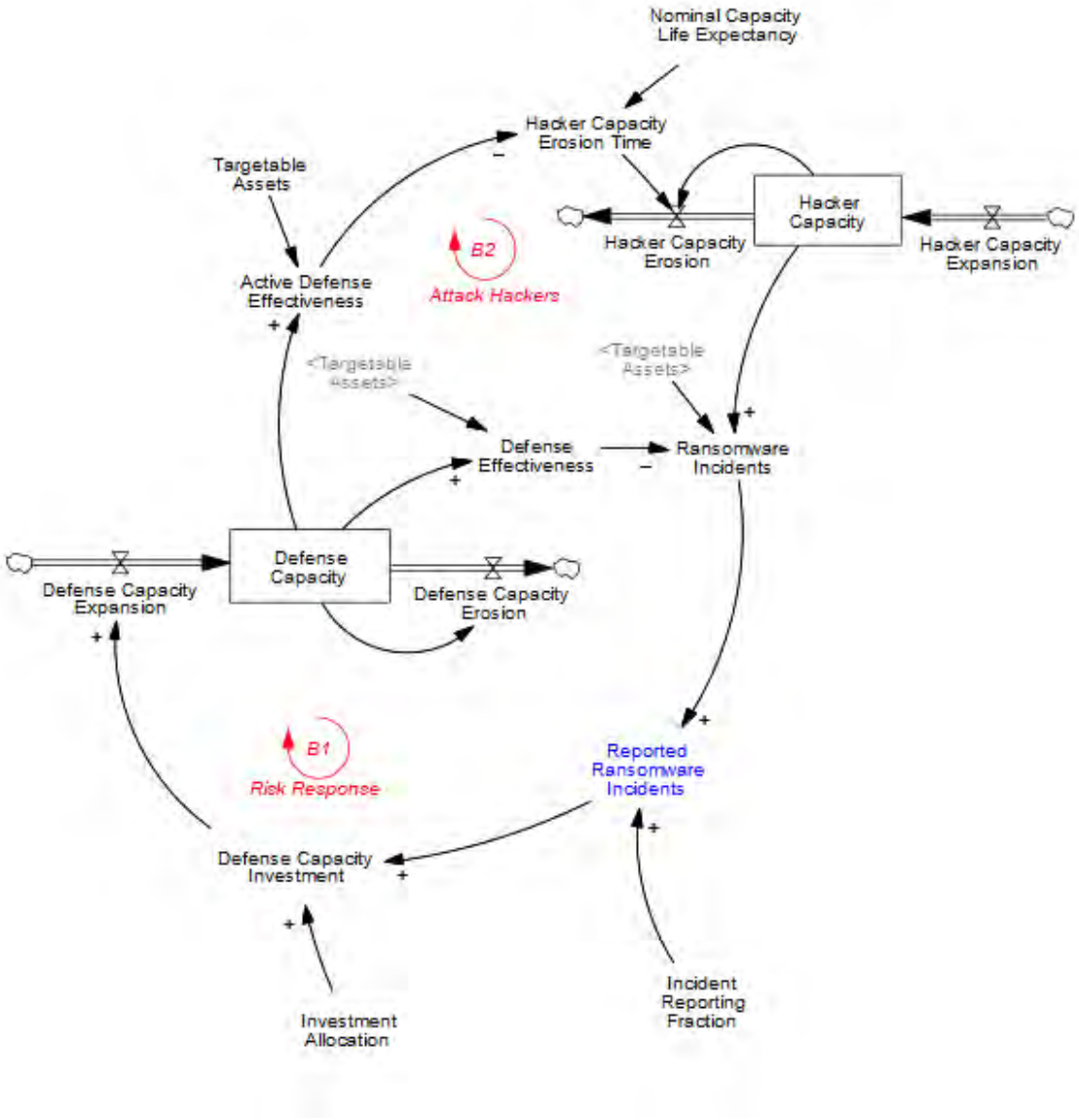


Figure 6 Ransomware Model Build 2

The firm/organization's response to learning of "reported" ransomware incidents is the growth of defense capabilities to cover the digital assets (or the targetable assets). Targetable assets can also be viewed as the full set of attack vectors (or attack surface) presented to a hacker by digital assets, with the expectation that any one digital asset has several independently targetable attack vectors. This first balancing loop (B1) is the corporate/organizational response to the perceived risk of ransomware (reported incidents) to deploy passive cybersecurity measures, including software updates related to vulnerabilities, technical tools, and operational processes to monitor networks and deploy defenses, increased cybersecurity workforce strength, mitigation and recovery measures, and end user threat awareness and education.

The second balancing loop (B2) is the role of active defenses, that is the efforts by governments and third parties to hack (offensive cyberattacks), arrest, or otherwise disrupt the hacker gangs, affiliate partners,

supporting infrastructure, and payment channels. In this model those active defense efforts are accounted for by reducing the life expectancy or erosion time of hacker capacity.

In Figure 7, Model Build 3, we see the growth of hacker capacity as enabled by the revenue available from the ransom proceeds.

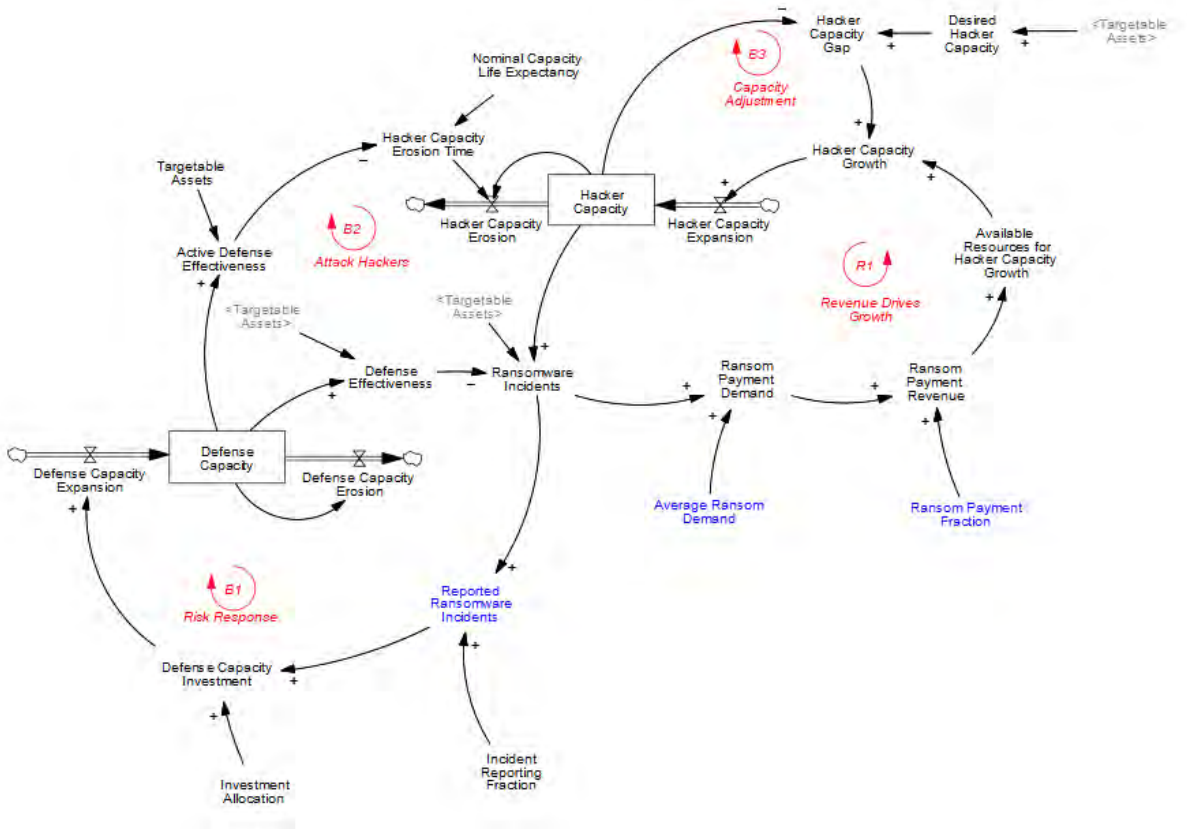


Figure 7 Ransomware Model Build 3

Revenue is a function of the number of successful attacks (incidents), average ransom demanded for each incident, and the fraction of victims paying ransoms. Hacker capacity growth is determined by the available revenue, the fraction of the revenue reinvested by the hacker gangs in ransomware attacks, and the average cost to develop and deploy an attack.

The incorporation of hacker capabilities into the model involves two loops, a reinforcing loop (R1) where available revenue drives growth of hacker capabilities and a balancing loop (B3) that adjusts hacker capacity to the opportunity represented by targetable assets.

The growth of ransomware attacks (as seen in the reported incidents and ransom payments) and the overall cost of those attacks drives cyber insurance market (R3).

In Figure 8, Model Build 4, we see the first two impacts or loops due to the cyber insurance coverage held by the potential targets or owners of the digital assets.

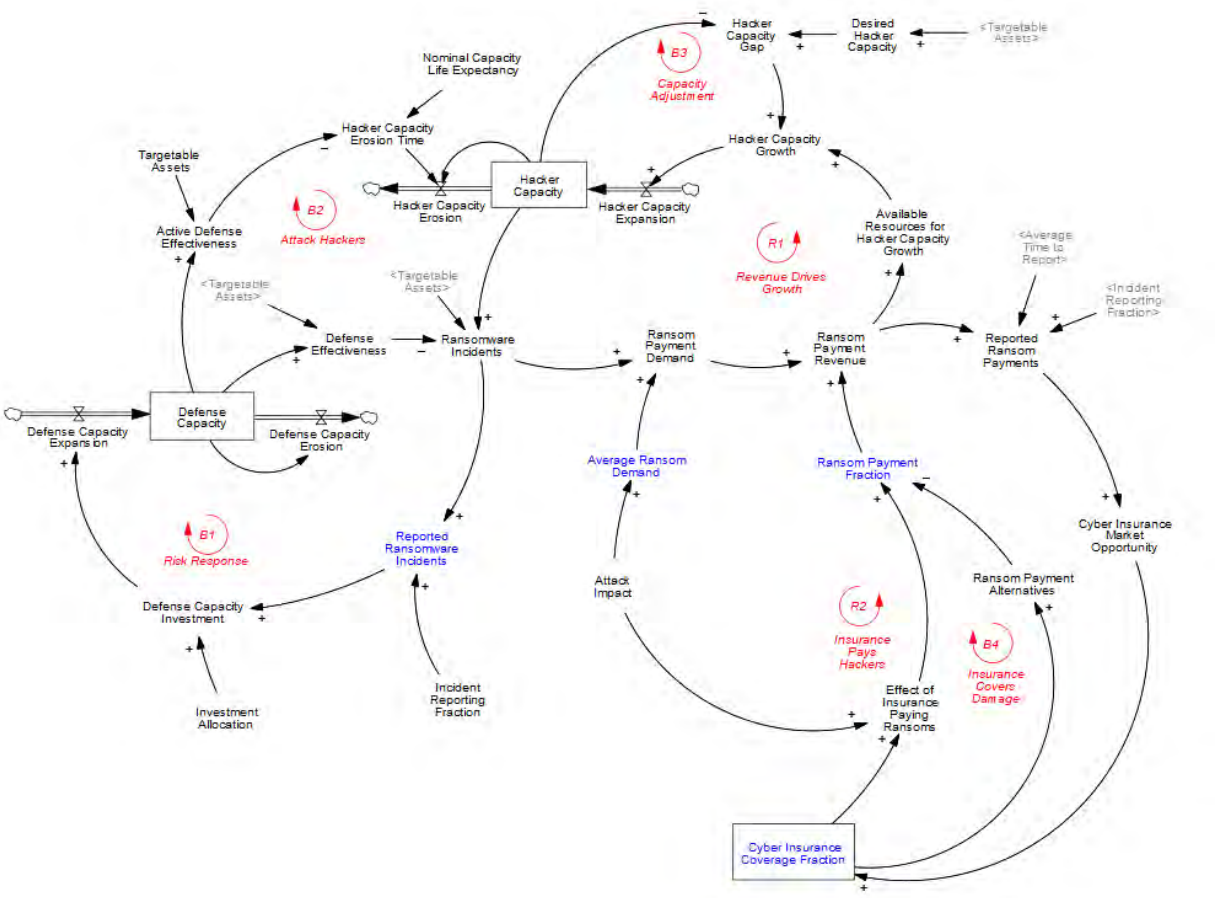


Figure 8 Ransomware Model Build 4

Cyber insurance has several effects on the ransomware ecosystem. First, cyber insurance provides the victim with the funds and third-party negotiation services to pay the ransom demands of the hackers (R2).

Second, cyber insurance can cover the damage of ransomware attacks (B4), including rebuilding networks and data bases and covering lost business revenue, often precluding the victims' need to pay ransom demanded by the hackers. Hence, here we see the inherent dichotomy of cyber insurance coverage – insurance makes it both easier to pay ransoms and reduces the need for victims to pay ransoms.

The third and fourth effects of cyber insurance are seen in Figure 9, Model Build 5.

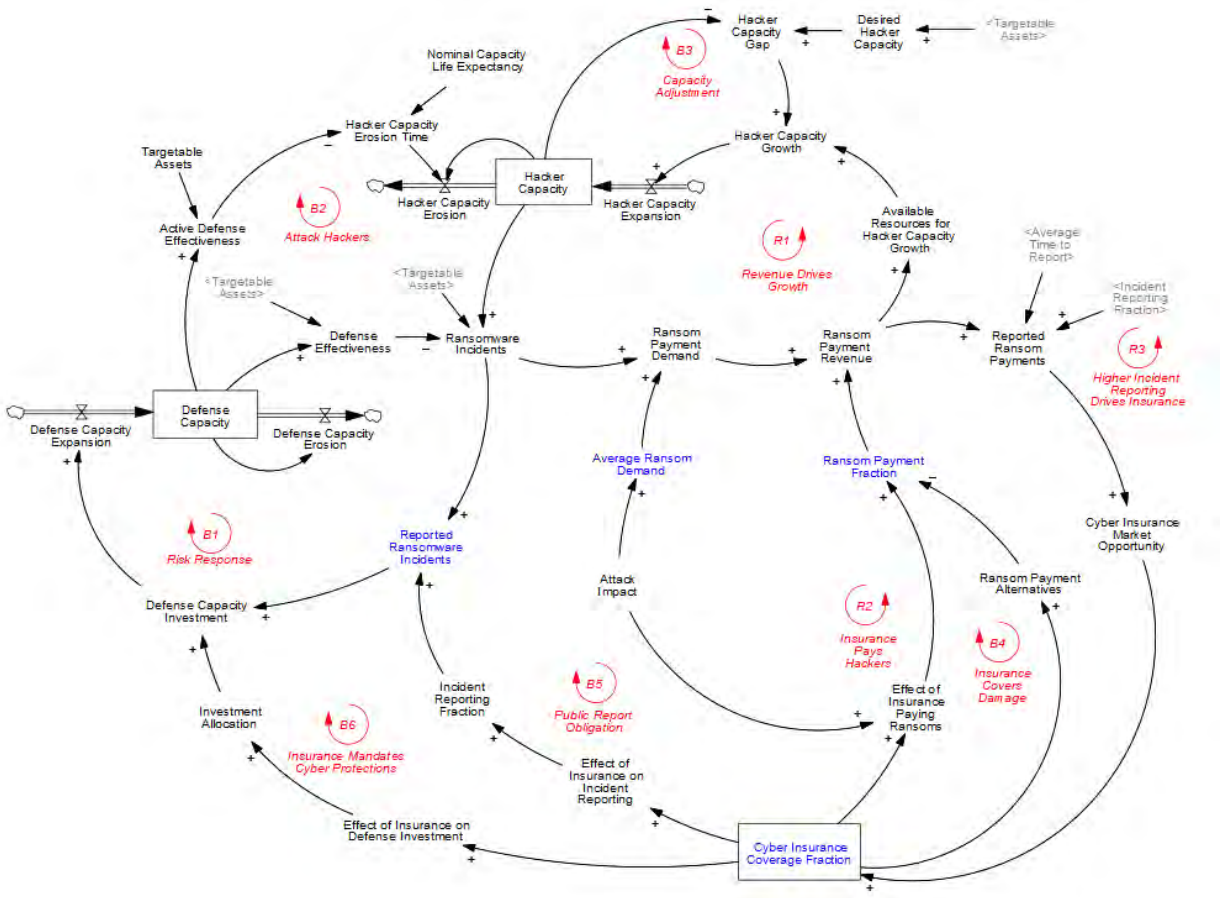


Figure 9 Ransomware Model Build 5

Third, filing cyber insurance claims often involves an incident reporting obligation (B5) ultimately increasing the overall fraction of incidents reported. Fourth, and most importantly, as part of the process to acquire cyber insurance the covered party must typically show some level of basic defensive protection measures employed – specifically, user awareness/education programs, intrusion detection tools, and recover/mitigation plans, in order to obtain coverage (B6). As an extended effect of higher incident reporting, the feedback look R3 emerges as higher reporting drives increased perceived need for cyber insurance coverage for firms and organizations that see themselves at risk.

In Figure 10 we see the additional effects of the dynamic change in the fraction of victims paying ransom to the hacker gangs. If payment rate decreases, the hackers then demand more money to attain the same revenue (B7) and will go after larger, more lucrative targets (B8). And with those larger targets and more impactful attacks, the demands for ransom are higher, and the potential damages are greater, and the effort needed to recover more massive and time consuming, leading to even higher insurance payouts, in ransoms or damage/recovery claims (B9). This figure also shows the final feedback loop regarding the impact that defenses have on the ability of victims to mitigate the impact of a ransomware attack and recover without paying a ransom to the hackers (B10).

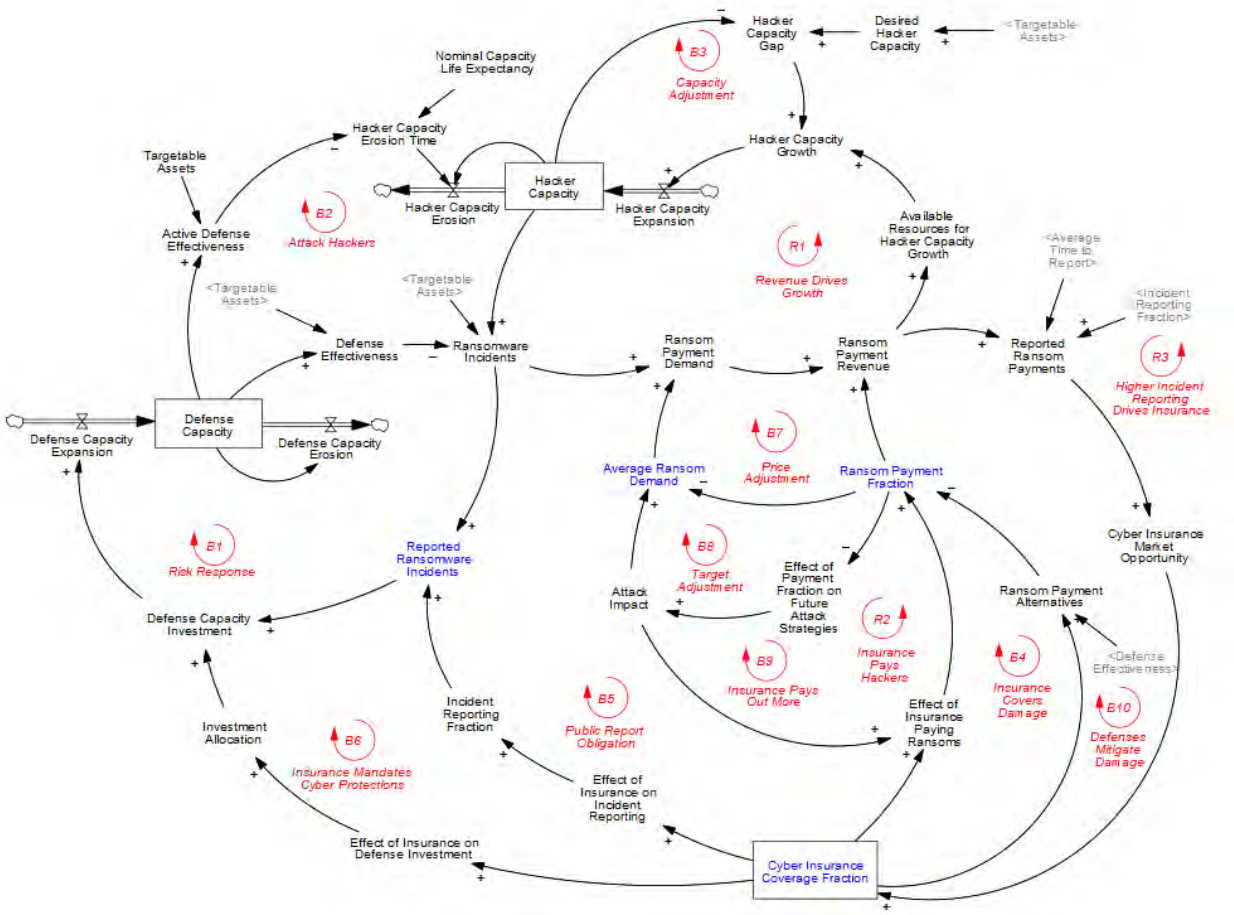


Figure 10 Ransomware Model Build 6

Figure 11, our final build, describes the model in its entirety. An added aspect for this figure is the Digital (or online) Assets of the firm or organization. The variable Targetable Assets reflects that any one line of business online may present hackers with several different attack vectors. Appendix B shows an additional version with minor constants and variables included.

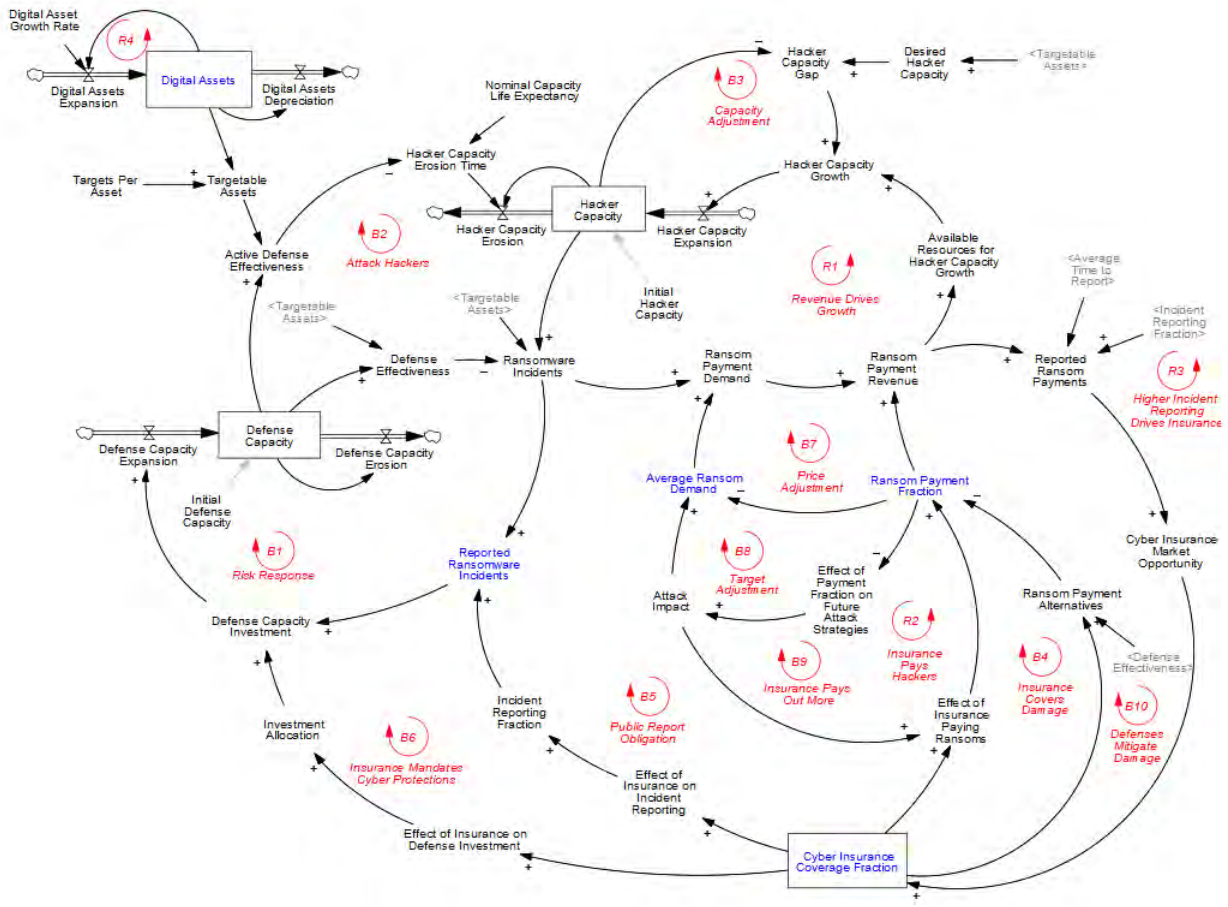


Figure 11 Full Ransomware Stock-and-Flow Simulation Model

We used Vensim DSS software to create and simulate this model. Appendix C lists the equations used in this model. The full data set needed to replicate this model is included in the supplemental material for this paper.

Variables and Parameters

Several variables were introduced in the previous model build diagrams. Table 3 summarizes the variables and parameters incorporated in this model.

Table 3 Key Variables and Parameters

Variable	Units	Category					Value
		Exogenous	Endogenous	Stock	Key Interest	Policy Candidate	
General Ecosystem							
Digital Assets	Assets		X	X			Equation, 100
Digital Assets Expansion	Assets/Month		X				Equation
Digital Assets Growth Rate	Dimensionless/Month	X					0.0243
Digital Assets Depreciation	Assets/Month						Equation
Assets Life Expectancy	Month	X					48
Targets per Asset	Dimensionless	X					5.01959
Targetable Assets	Assets		X				Equation
Ransomware Incidents	Successful Attacks/Month		X		X		Equation
Reported Ransomware Incidents	Successful Attacks/Month		X		X		Equation
Baseline Incident Reporting Fraction	Dimensionless	X					0.15
Incident Reporting Fraction	Dimensionless	X	X		X	X	Equation
Average Time to Report	Month	X			X	X	4
Ransom Payment Demand	Dollars/Month		X				Equation
Ransom Payment Revenue	Dollars/Month		X				Equation
Baseline Payment Fraction	Dimensionless						0.760206
Ransom Payment Fraction	Dimensionless	X			X	X	Equation
Average Ransom Demand	Dollars/Successful Attack	X			X		Equation
Baseline Ransom Demand	Dollars/Successful Attack	X					199430
Time to Perceive Payment Rate	Month	X					3
Defense Element							
Baseline Investment	Dimensionless	X					0.37254
Investment Allocation	Dimensionless		X				Equation
Defense Capacity Investment	Assets		X				Equation
Defense Capacity Expansion	Assets/Month		X				Equation
Defense Capacity Expansion Time	Month	X					2
Defense Capacity	Assets		X	X	X		Equation
Defense Capacity Initial	Assets		X				24.3986
Defense Capacity Erosion	Assets/Month		X				Equation
Defense Capacity Erosion Time	Month	X					24
Workforce per Defense Capability	People/Asset	X					10104.3
Normal Hiring		X					1.5M
Cybersecurity Workforce	People		X		X		Equation
Defense Effectiveness	Dimensionless		X		X		Equation
Active Defense Priority	Assets/Mon	X				X	0.75
Active Defense Effectiveness	Dimensionless		X		X	X	Equation
Hacker Element							
Average Capacity Development Cost	Dollars/Attack	X					11322.8
Reinvestment Fraction	Dimensionless	X					0.416256
Resources for Capacity Growth	Dollars/Attack		X				Equation
Desired Hacker Capacity	Attacks		X				Equation
Hacker Capacity Growth	Attacks		X				Equation
Hacker Capacity Expansion	Attacks/Month		X				Equation
Hacker Capacity Expansion Time	Month	X					10.651
Hacker Capacity	Attacks/Month		X	X	X		Equation
Hacker Capacity Initial	Attacks/Month						39.42
Hacker Capacity Erosion	Attacks/Mon	X					Equation
Hacker Capacity Erosion Time	Month		X				Equation
Nominal Capacity Life Expectancy	Month	X					11.9023

Insurance Element							
Cyber Insurance Coverage Fraction	Dimensionless			X	X		Equation, 0.26
Time to Acquire Policy	Month	X					18
Effect on Defense Investment	Dimensionless		X				Equation
Investment Effect Significance	Dimensionless	X					0.388278
Effect on Incident Reporting	Dimensionless		X				Equation
Reporting Effect Significance	Dimensionless	X					0.3
Reported Ransom Payments	Dollars		X	X			Equation
Cyber Insurance Market Opportunity	Dollars		X				Equation
Policy Coverage Scaling	Dollars	X					10.96M
Nominal Industry Size	Dimensionless	X					0.39052
Ransom Payment Alternatives	Dimensionless		X				Equation
Payment Alternative Effect Significance	Dimensionless	X					0.476735
Effect of Insurance Paying Ransoms	Dimensionless		X				Equation
Insurance Payout Effect Significance	Dimensionless	X					.213207
Effect of Payment % on Attack Strategies	Dimensionless		X				Equation
Attack Impact	Dimensionless		X	X			Equation, 0.1
Attack Impact Effect Significance	Dimensionless		X	X			0.545405

Data sources and references are provided in the supplemental material.

Figure 12 below depicts the real-world trend data for four key variables used to the verify the accuracy of the model and its parameters, ransom payment fraction, average ransom payments, cyber insurance coverage and the size of the cybersecurity workforce.

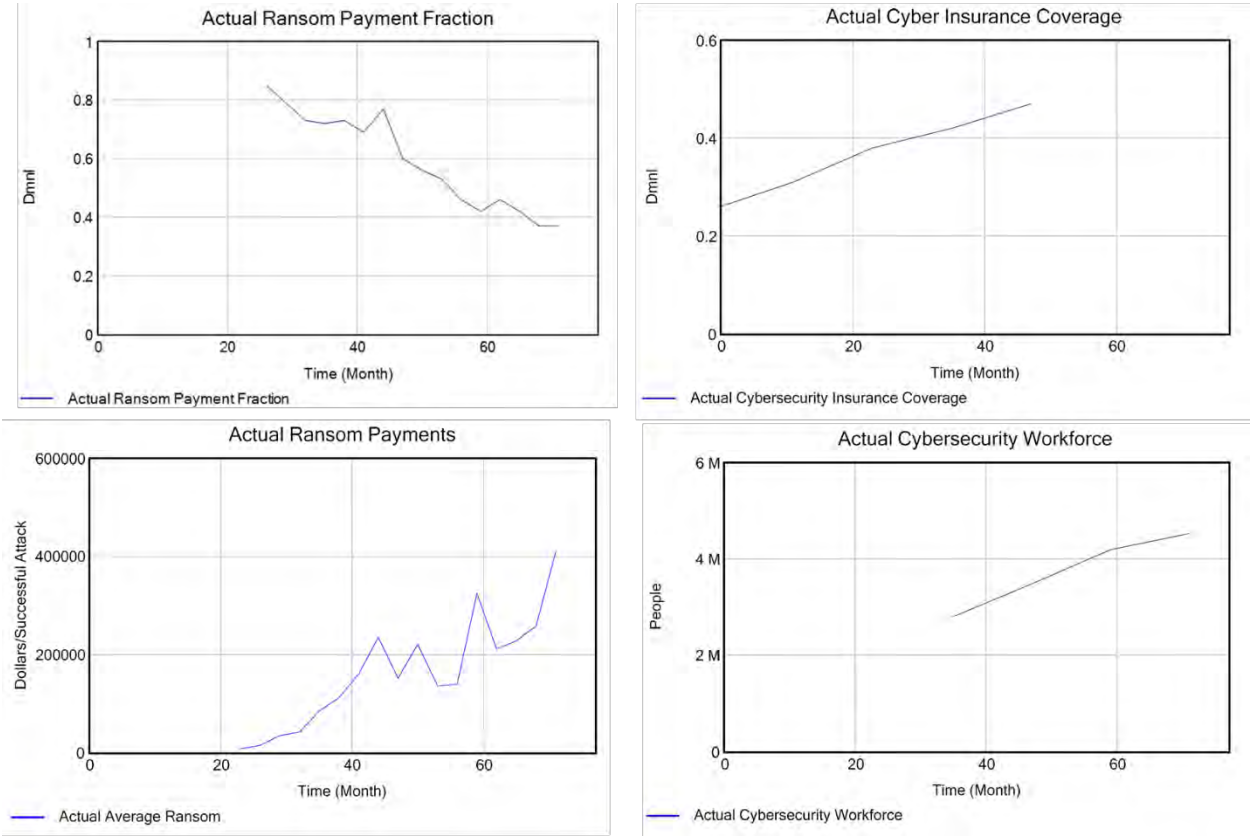


Figure 12 Real-World Trend Data – Ransom Payment Fraction, Ransom Payments, Cyber Insurance Coverage, and Cybersecurity Workforce Size

Model Verification and Validation

As part of the process to develop this model we took verification and validation steps to ensure the model aligned with real world understanding of the ransomware ecosystem behavior and was relevant and useful to assess policy alternatives in this space. Real world time series data was used for digital assets, reported ransomware incidents, ransom payment rate, average ransomware payment, cyber security insurance coverage, and cybersecurity workforce. Parameter values were manually and then automatically calibrated (using Vensim optimization) for the best fit between the simulated and actual data. We also observed several patterns of behavior that contribute to our overall confidence in the model. In each case the variable relationships and equations deliver logical, expected results as the parameters are modified. For example, the level of digital assets moderates or bounds (upper) ransomware incidents, attacks will grow quickly without defenses, more attacks fund even more attacks, reduced per attack development costs (enabled by more investment) increases hacker capacity, increasing incident reporting levels and reduced reporting timeframes drives increased investment in cybersecurity and eventually greater defense capabilities.

To validate this model, we need to be able to compare reported ransomware incidents over the period 2017 through mid-year 2023. The real-world data used here is the same used in Figure 1 and represents reported incidents from the three sectors of healthcare, education, and municipal government. As seen in Figure 13, showing a comparison of the simulated data with real-world data, the calibrated model's output closely tracked real-world data on ransomware incidents.

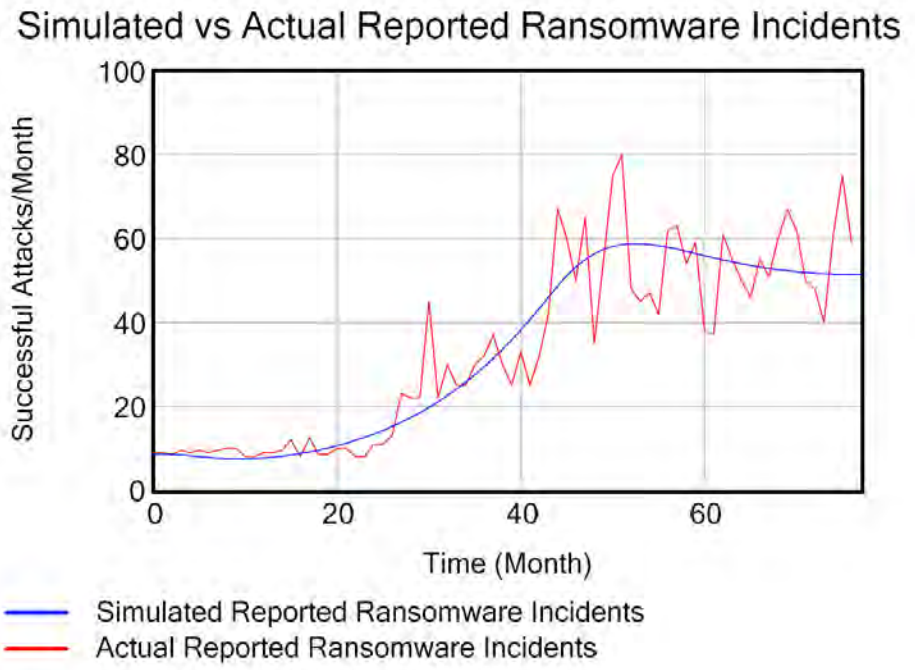


Figure 13 Comparison of Simulated to Actual Reported Ransomware Incidents (Jan 2017 to May 2023)

In Figure 14 the same follows for ransom payment fraction, average ransom payments, cyber insurance coverage fraction, and size of cybersecurity workforce.

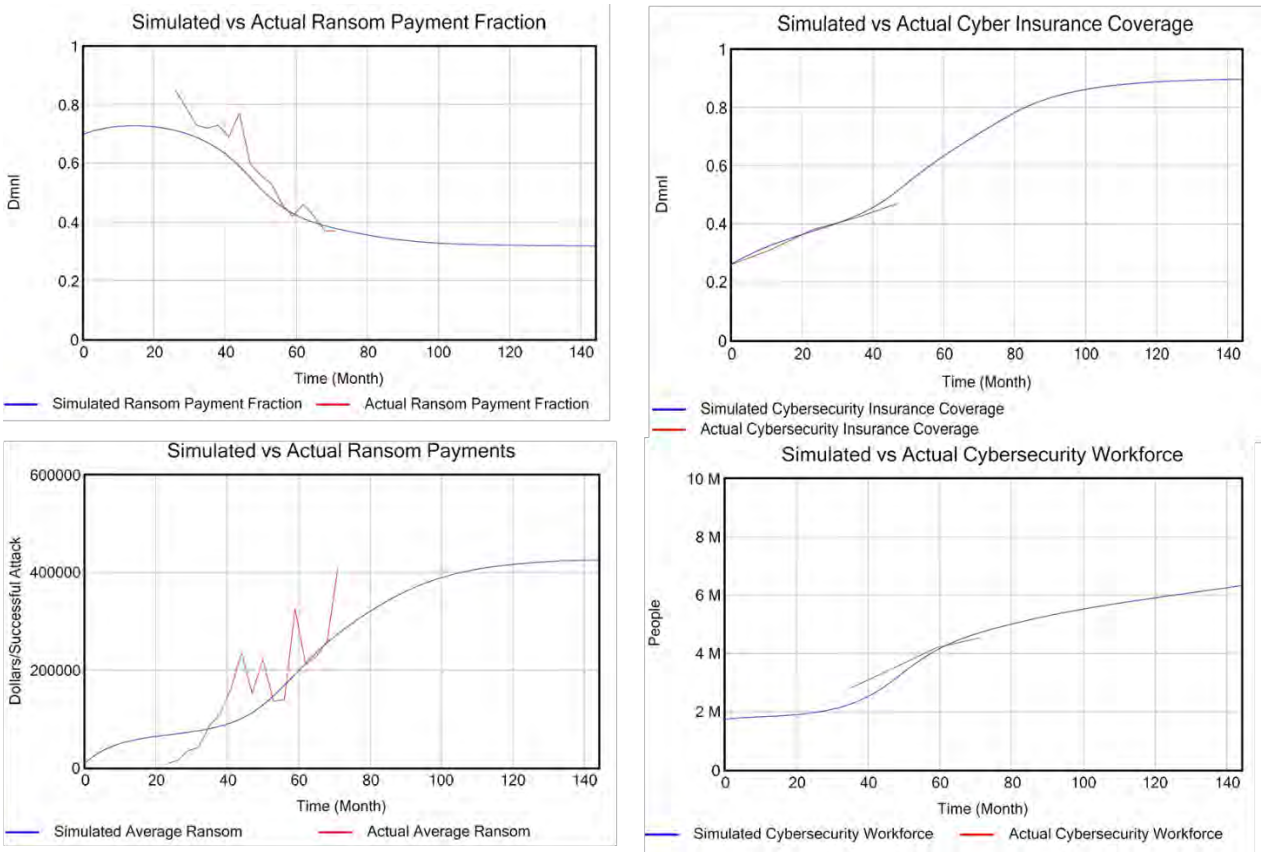


Figure 14 Comparison of Simulated to Actual Ransom Payment Fraction, Average Ransom Payments, Cybersecurity Insurance Coverage, and Cybersecurity Workforce Size

Policy Scenarios

The policy scenarios included in our analysis partially address the Federal government's role in combating ransomware. While the Ransomware Task Force (2021) (Starks, 2023b) identifies a full list of actions ongoing and in consideration, we selected several that were feasible to implement in our model. The general intent of each of these scenarios is to evaluate whether increased emphasis in these lines of effort would yield positive or synergistic results on the overall problem. This set of policy scenarios is realistic and relevant to today's policy framework options as each is either being considered and openly discussed, if not actively being implemented or encouraged. The key measure of merit in this simulation model for policy scenarios is ransomware incidents, albeit a manufactured measure as the actual incident data is unknown due to the lack of full reporting by ransomware victims. That lack of reporting leads us to the first policy scenario.

Scenario 1: Increase the reporting of ransomware incidents (and reduce the time to report.) The low rate of reporting of ransomware incidents has been noted as an issue (Marks, 2022; Menn et al., 2023; Ransomware Task Force, 2021; Shanklin, 2023). Moreover, it is difficult to estimate the real rate as the lack of reporting itself obscures reality. For this scenario we will model a 20% increase in the incident reporting rate after month 80 to observe the impact that increased reporting would have on the rest of the ecosystem and assess the ultimate value of policy measures in this area (Barlet, 2023; O'Donnell-Welch, 2022; Ransomware Task Force, 2021; Rudis, 2022). The model already incorporates the effect of

insurance coverage on incident reporting. In the real world, this policy change could employ Federal and state standards, penalties, and even incentives to try to increase reporting. Necessarily associated with a mandate in incident reporting is the reporting timeframe (Barlet, 2023). Hence, as part of this scenario we will also include the effect of a 50% reduction in the average time to report an event, from 4 to 2 months, also at month 80 in the model timeline.

Scenario 2: Reduce the ransom payment fraction. For reported incidents this already appears to be a positive trend (Coveware, 2022c) and this trend data is included in the model. For this scenario we will simulate an additional 30% reduction in the ransom payment rate after month 80, effectively hitting the lower bound set in the model. In the real world, this policy measure would employ Federal and state standards, clarification of existing sanctions against deals specific entities, threat of civil or criminal penalties, better data and network backups, prohibitions (internal or external) against insurance receipts used for ransom payments, and post-attack technical support to victims to decrypt the encryption on their data to encourage victim to avoid paying ransom demands (Barlet, 2023; Dudley & Golden, 2022a; Editorial Board, 2023; Ransomware Task Force, 2021; Robles-Carrillo & García-Teodoro, 2022a; Rudis, 2022; Tidy, 2023; Zorz, 2022).

Scenario 3: Strengthen passive defenses. This policy scenario adds a 50% increase in the baseline investment allocation at month 80. Specific measures that could be taken to affect this change might involve increased threat awareness, which in turn drives greater recognition and understanding that ransomware is an immediate, serious, and addressable threat drives action in the cybersecurity industry and in the targeted firms to reduce attack surfaces, develop technical solutions, correct vulnerabilities, and educate end users on their role in preventing network intrusions. The specific actions to effect greater threat awareness are varied but must be directed to specific high-risk sectors to make a difference (Barlet, 2023; Mascellino, 2023; McKinsey, 2023; Ransomware Task Force, 2021; Richardson & North, 2017; Rudis, 2022).

Scenario 4: Enhance active defenses. Recent news and documentaries report on several successful law enforcement campaigns (in some cases assisted by private entities) to infiltrate hacker gang networks, recover encryption keys, and disrupt or eliminate hacker gangs and their supporting infrastructure and staff (Collier, 2021; Coveware, 2022b; Dudley & Golden, 2022; Menn et al., 2023; Ransomware Task Force, 2021; Shakir, 2023). It is important to recognize that these activities take resources, expertise, and time to put in place. This policy scenario doubles down on these active defense actions and reflects both a higher level of effort and well as a wider array of specific types of actions taken. In our model, this level of effort is captured in the variable “active defense priority” which sets a threshold or baseline of current defense capability to establish those activities that degrade hacker capacity. This scenario implements a change in this variable by a 50% level of effort increase at month 80 in the timeline.

Scenario 5: Combination of the above. While it may not be appropriate, feasible, or prudent to implement all policies at the same time, for simplicity we combined all four into a single scenario. On the other hand, a concerted government approach to reducing or mitigating ransomware should not be pursued in a piecemeal fashion as some policies may be mutually supportive.

Table 4 summarizes the five policy scenarios simulated in this model. While in the model these policy scenarios are implemented at month 80, in the real-world these measures would be phased in over 3-12 months. Also, the specific changes for investment allocation and active defense priority may not have clear real-world equivalents.

Table 4 Ransomware Policy Scenarios (Implemented at Month 80)

Policy Scenario	Short Title	Parameter Changes
1	Increase incident reporting rate and reduce time to report	20% increase in reporting rate; 50% decrease in reporting time
2	Reduce ransom payment rate	Reduction by 30%
3	Strengthen passive defenses	Increase investment allocation by 50%
4	Enhance active defenses	Raise active defense priority by 50%
5	Combination of all 4	

Results

Simulations were run both without and with policy interventions. Before showing the results of the policy scenarios, we offer the baseline forecast for reported ransomware incidents as well as an overall trend comparison of hacker capacity and defense capacity against targeted assets.

Baseline Forecast

As seen in Figure 15, without additional policy interventions or exogenous changes the model predicts that ransomware incidents will continue to increase going forward through the end of the simulation at month 144 (or end of 2029). This suggests a continuing problem worthy of policy intervention.

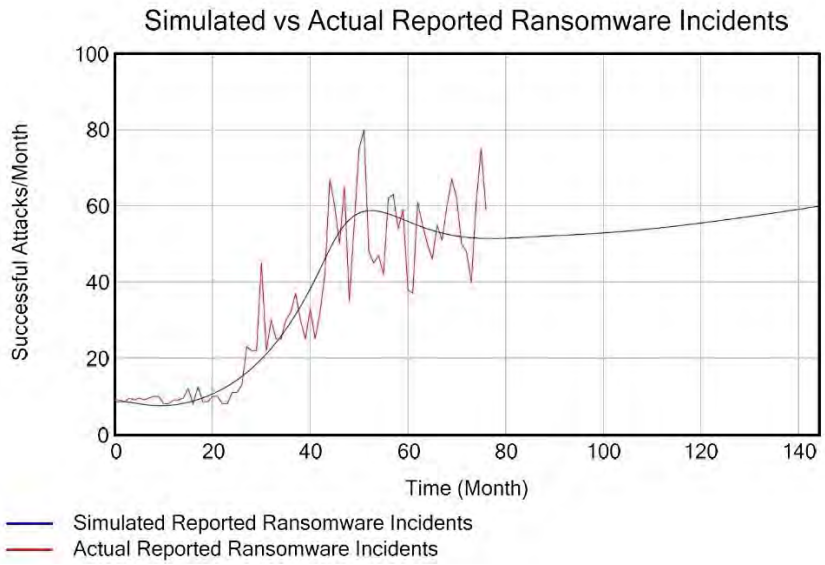


Figure 15 Baseline Simulation – Reported Ransomware Incidents

Figure 16 below shows the simulated trend data for hacker capacity and defense capacity. Targetable digital assets serves as an upper bound on hacker capacity as well as an objective reach for defense capacity. Even with defense capabilities exceeding hacker capacity over much of the simulation period, targetable assets are still left uncovered and thus hacker efforts are successful in generating ransomware incidents.

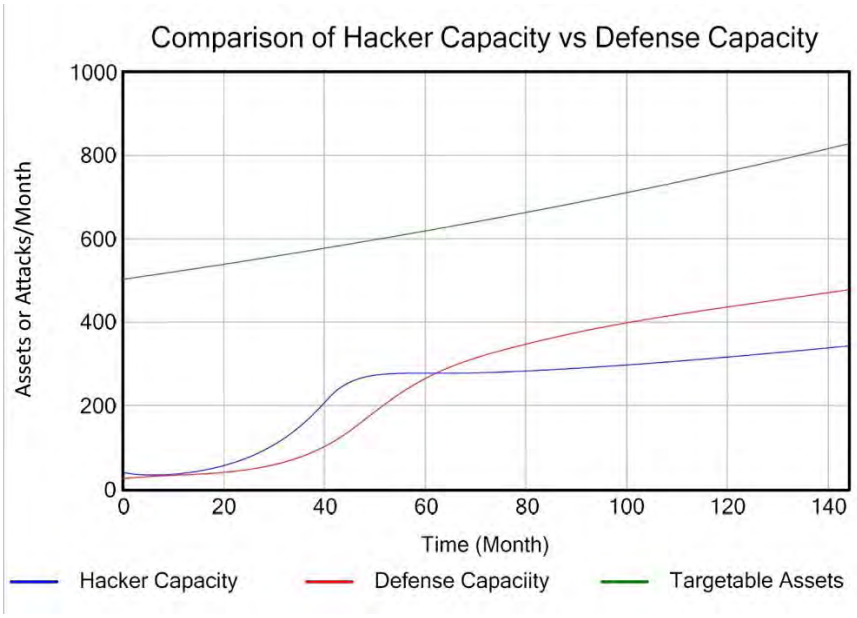


Figure 16 Comparison of Hacker Capacity vs Defense Capacity and Targetable Assets

Assessment of Policy Scenarios

The results of the policy simulations indicate positive results for four of five scenarios as seen in Figures 17, 18, 19, 20, 21, and 22. Note that the policy application time is at month 80 (o/a Sep 2023).

Up to this point our study has focused on reported ransomware incidents, as that's the primary trend data that shows the core problem. However, since one or more of the policy measures strive to increase the fraction of incidents that are reported, we will focus on estimated ransomware incidents in lieu of a reported data or forecasts of reported data. In Figure 17 we show a comparison of estimated (or simulated) ransomware incidents and reported ransomware incidents to show the basic relationship between the two. In Figure 18 we show the impact of Policy Scenario 1 on simulated ransomware incidents. Going forward for the remaining policy scenarios we will show just ransomware incidents. Figures 17 and 18 clearly show the impact of policies regarding incident reporting and reporting timelines.

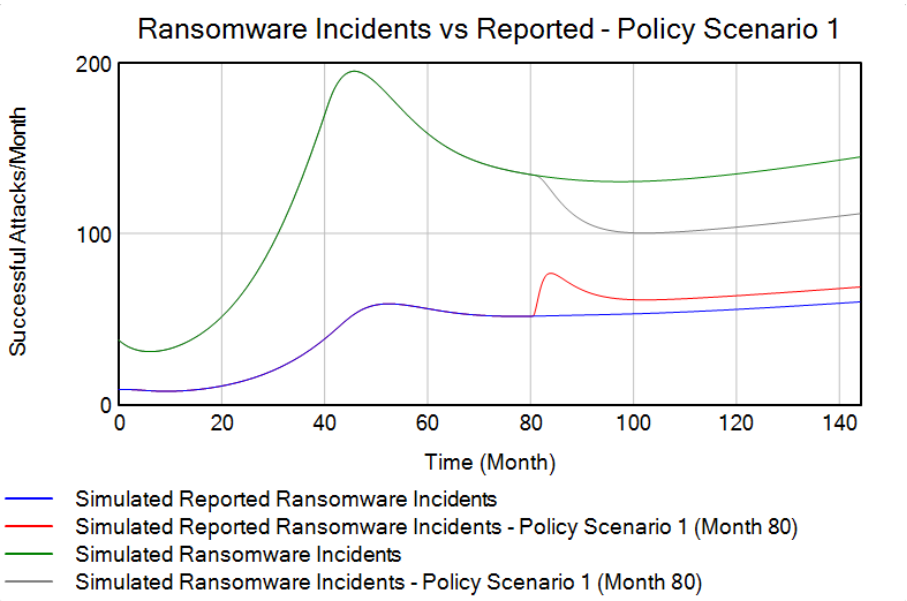


Figure 17 Policy Scenario 1 – Improved Incident Reporting and Time to Report (Comparing True and Reported Ransomware Incidents)

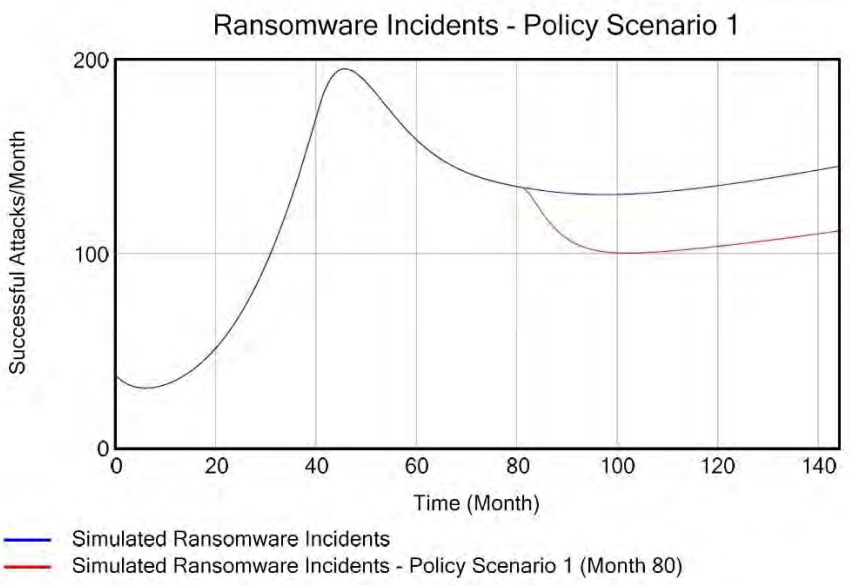


Figure 18 Policy Scenario 1 – Improved Incident Reporting and Time to Report

In Figure 19 we add illustrations of the impacts of Policy Scenarios 2, 3, 4, and 5. For Policy Scenario 2 – Reduce Ransom Payment Fraction on ransomware incidents, the curve shows negligible impact on ransomware incident forecasted trend data. For Policy Scenario 3 – Strengthen Passive Defenses on ransomware incidents, the curve shows a substantial impact on the projected data over time. For Policy Scenario 4 – Enhance Active Defense on ransomware incidents, the curve shows minimal impact. For Policy Scenario 5 – Combination of All Policy Scenarios on ransomware incidents, as expected, the curve shows a substantial impact of the combination of all four policy scenarios on ransomware incidents.

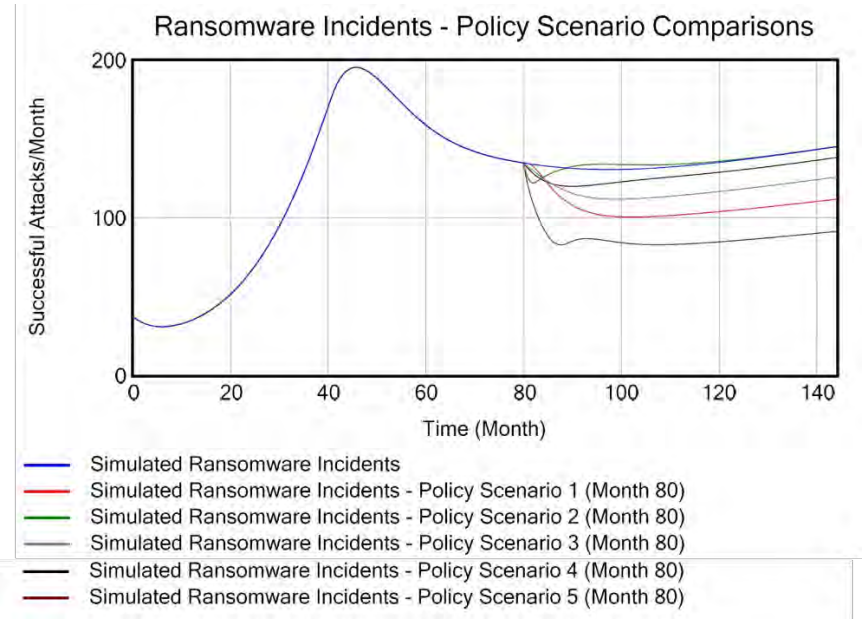


Figure 19 Ransomware Incidents Under All Policy Scenarios

Scenario 1, increased incident reporting and reduced reporting timelines, behaved as expected. The policy measure ultimately provides firm/organization leaders and cybersecurity practitioners with more precise and timely understanding of the real threat and thus drives changes in cyber defense posture and potentially active defense activities as well. Scenario 1 could be put in place by government mandates, industry/commercial standards, and tighter enforcement of insurance policies. The theory of Scenario 2 is that removing resources from the hacker ecosystem by limiting the payment rate would consequently reduce the funds available to reinvest in new capacity. However, with fewer victims paying ransom the simulation reacted with higher ransom demands and more lucrative targets, in a rather abrupt manner. Scenario 3, increased passive defenses, had a positive result but incidents continue to increase just at a lower level. Scenario 4, enhanced active defense (including offensive actions against hacker groups – "hack the hackers"), produced results but not at the expected level as hackers quickly regenerate capabilities diminished by law enforcement. In a rough comparison of focusing on passive defenses (Scenario 3) versus active defenses (Scenario 4), passive appears more effective. Scenario 5, the combination of all four policy scenarios, performed positively as expected.

Figure 20 shows the impact of Policy Scenario 5 (all policies) against the key trend data we introduced earlier – ransom payment fraction, average ransom demand, cybersecurity insurance coverage, and cybersecurity workforce size. As seen in the graphs the inclusive policy scenario behaved as expected from the perspective of each of the four trend data charts.

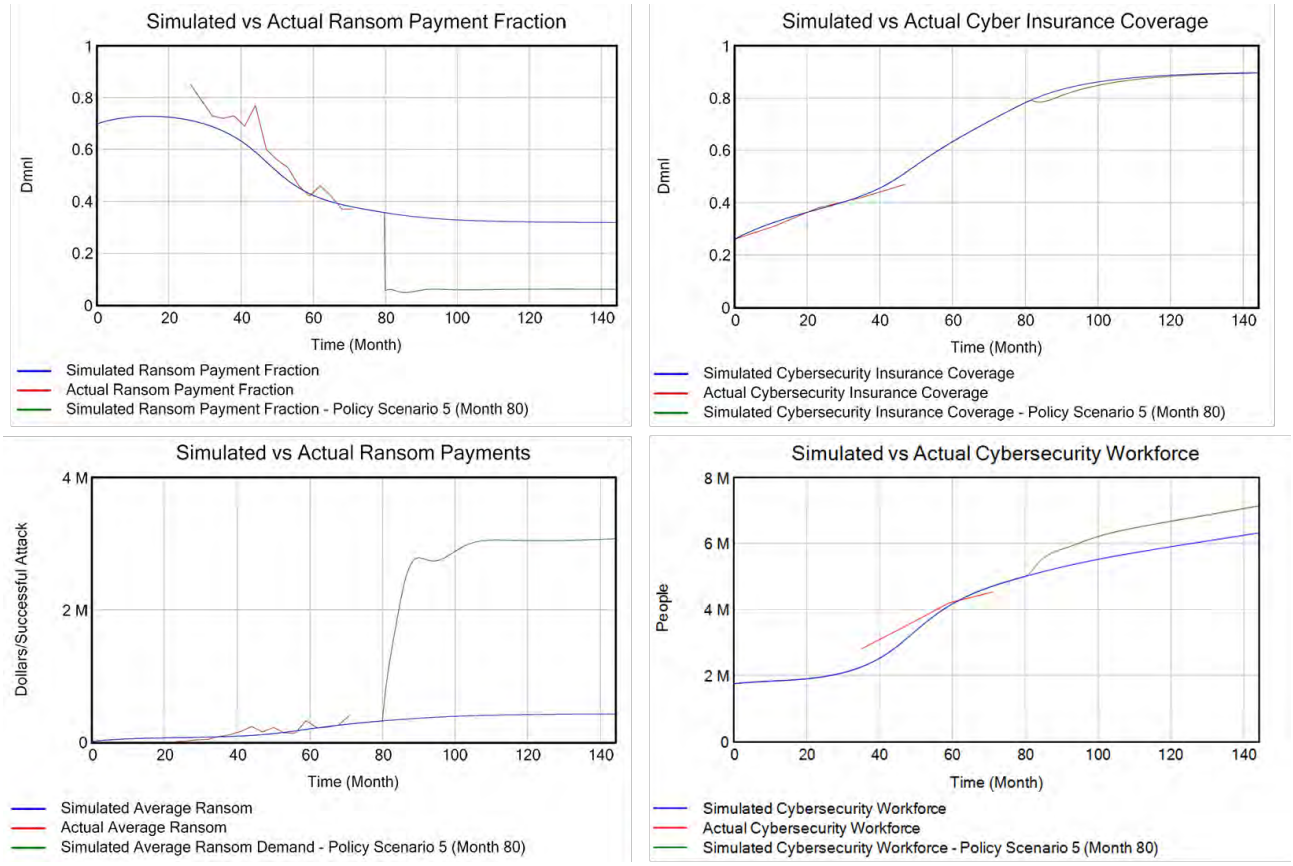


Figure 20 Policy Scenario 5 - Ransom Payment Fraction, Average Ransom Payments, Cybersecurity Insurance Coverage, and Cybersecurity Workforce Size

Appendix D provides additional time series views of key variables in the model for both the base run and Policy Scenario 5.

To better understand and validate the policy scenarios we ran a counterfactual simulation where the proposed policies are implemented when the problem first arises. Figure 21 shows the policy impact against ransomware incidents if each policy were simultaneously implemented in Feb 2018 (month 14). The graph suggests that the policy scenarios as implemented in the model have some level of validity.

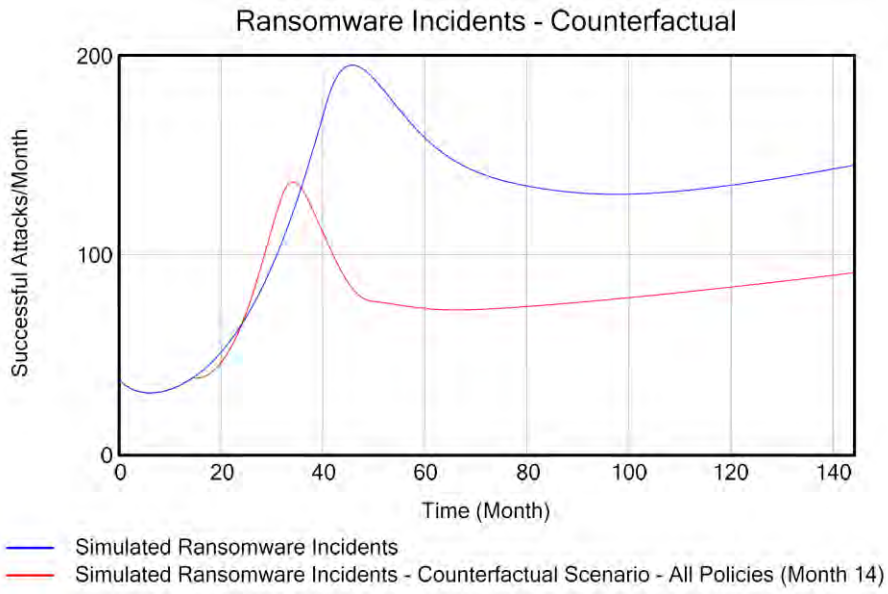


Figure 21 Ransomware Incidents - Counterfactual Policy Implementation

Discussion and Conclusions

We built a model to simulate the effects of policy decisions on ransomware incidents. We researched the ransomware ecosystem to understand the structure, variables, and parameters values. We verified and validated this model by comparison against real world time series data. We then applied this model to examine alternative policy actions that governments could employ to reduce the extent and severity of ransomware.

The results of simulating alternative policy actions suggest that government intervention, notionally at the Federal level, can positively impact this complex problem. The model evaluates policy actions focused on four key areas: increasing the incident reporting fraction and reducing the time to report an incident (Scenario 1); further reducing the ransom payment rate (Scenario 2); strengthening passive defenses (Scenario 3), and further enhancing active defenses including law enforcement activities (Scenario 4). While government intervention already appears to be having an impact on the ransomware problem, our conclusion is that further improvement in incident reporting metrics and in strengthening passive defenses will have the highest confidence results. According to our simulation results, further attempts to reduce the fraction of victims paying ransom will have the negative result of increasing the ransom payment demanded since the hacker gangs are revenue seeking. However, more investigation of these four policy scenarios through system dynamics modeling and other policy evaluation methods is clearly warranted.

Despite interesting, promising, and useful results, our initial modeling and simulation efforts involve some limitations and unexplored threads that offer opportunities for improvements in the model and further policy investigations.

First, while we have captured the main elements involved in the ransomware ecosystem, we may not be fully accounting for important variables or their weight in our model and may be missing subtle aspects of the various feedback loops in the ecosystem. The best approach to address such weaknesses would be

to base the model on direct input from subject matter experts during the problem formulation stage and initial development of the causal diagram. Although our model was based on a thorough analysis of current events, publicly available data, and policy recommendations, gathering input direct from subject matter experts could still help identify additional variables, qualify the feedback relationships, and validate the current model (D. F. Andersen & Richardson, 1994; Felipe Luna-Reyes et al., 2006).

Data for the key parameter in the simulation of this model, reported ransomware incidents, applies exclusively to the global health care, education, and municipal government sectors. The remaining data sets come from the ransomware and cybersecurity ecosystem at large. Recognizing that all sectors, actors (hackers or defenders), and online targets and their vulnerabilities are not the same across the cybersecurity and ransomware ecosystems, the second improvement in the model would be to gather and apply sector specific data. While our current modelling efforts may oversimplify or neutralize some of these sector differences, the result on the model's validity may not be measurably affected. However, with more complete data sets and parameters for specific sectors of interest – in this case, healthcare, education, and/or local government, the model and simulations could be specifically constructed to address unique challenges or dynamics of individual sectors. Furthermore, with the right data sets, this model could be extended to other sectors than those explored in this research effort with the aim of investigating the difference in the impact of policy scenarios.

Third, the model includes several exogenous variables that in the real world dynamically interact with other factors in the ecosystem. A more complete and valid model would incorporate these key variables as endogenous to fully capture the relationships across the ecosystem. Potential variables to include as endogenous include active defense priority, average development cost, and reinvestment fraction.

Fourth, several important aspects of the ransomware ecosystem should be added to or enhanced in this model to make it more comprehensive and correct.

- Methods to improve incident reporting metrics in the sector of interest, to include specific incentives or mandates, should be incorporated as the nuances of those various approaches will ultimately determine the extent of success.
- Similarly, greater fidelity in the types of defensive capabilities, mitigation or recovery methods, and alternatives for active defenses should be incorporated into the model.
- The RaaS business model underpins much of the current success of the ransomware threat and is a core part of today's ransomware ecosystem. While complex in many respects, it retains much of the qualities and impact that "as a service" models have in the "legal" IT domain, especially partner and process openness, clearly assigned roles, inherent flexibility in scale and targets, and accelerated pace of change (Hacquebord et al., 2022; Insikt-Group, 2023; Meland et al., 2020). At a minimum the fluid aspects of the business model and its impact on the reducing the cost to deploy ransomware capabilities would be a useful improvement. In fact, a separate system dynamics model could be developed just to explore the financial, innovative, market, and operational aspects of the RaaS business model.
- The effect of cyber insurance on enabling the payment of ransoms, conversely offering an alternative to paying ransoms, promoting higher reporting of ransomware incidents, and driving greater investments in cyber defenses are well incorporated into the model. However, risk tradeoffs and calculus in the organizations' decisions to purchase insurance or in the insurance

firms premium rate setting are not well addressed and yet are key factors behind this element of the ecosystem (DeKorte, 2019; Eling & Schnell, 2016; Granato & Polacek, 2019; Woods, 2023b).

- An important reason to avoid paying ransoms is the defensive measures, mostly taken in advance, to mitigate the impact of a successful ransomware attack. These measures include redundant or backup data storage, networks, and applications (Comizio et al., 2023; Robles-Carrillo & García-Teodoro, 2022). While the current version of the model does account for defensive enablers of ransom payment alternatives, greater fidelity in the level of mitigations and impact avoidance would offer a more robust model.
- Technology is a key element in this ecosystem. Technology creates the ecosystem in which the targeted assets reside. Technology creates the vulnerabilities, to include zero day exploits, that the hacker gangs exploit and the tools they leverage. Besides creating vulnerabilities, technology also enables corrective actions to patch vulnerabilities, monitor networks for intrusions, and block or remove hacker penetrations. Thus, the relative pace of hacker and defensive innovations stands as fundamental in understanding which side will remain ahead in this competition (Hacquebord et al., 2022; *How Are Ransomware Gangs Evolving Their Expansion and Attack Strategy?*, 2022; Meland et al., 2020). While the current model accounts for the pace of incorporating defensive and offensive capabilities, it considers those exogenous variables rather than factors influenced by priorities, policies, practices, and level of effort applied by key actors in the ecosystem and thus recognized endogenously. Overall, the time phased processes of attack development and execution could be better described in the model.
- Even with the means to access (or generate) technological innovations, employ modern business models, and reconstitute organizations in an agile fashion, hacker gangs and their infrastructure remain ultimately vulnerable to attack and disruption themselves (Comizio et al., 2023; Temple-Raston & Glueck, 2023). While the current model reflects the ability of active defenses to undermine or attrit hacker capabilities at large, the model lacks most key nuances in hacker organizational behavior. In fact, like the prior note about RaaS, a separate system dynamics model could be devised just to explore the vulnerabilities and resilience of hacker gangs and their infrastructure.
- The prioritization of ransomware targets based on size, likelihood of exploitable vulnerabilities, expected payoff, and risk of attracting increased attention from law enforcement are important, yet not fully incorporated aspects of the ecosystem (Gillum, 2022; Insikt-Group, 2023; Meland et al., 2020; Menn et al., 2023; NAIC, 2022; O'Kane et al., 2018; Starks, 2023a, 2023b; Uberti, 2021).

Beyond inclusion of more aspects of the ransomware ecosystem a more comprehensive and complete model should be able to assess the additional policy scenarios discussed below.

First, we should model governmental efforts to increase the transparency of Bitcoin exchanges, on the same level as the global banking system, making it easier to recover ransom payments and induce greater risk or deterrence in an otherwise reliable and covert payment infrastructure (Comizio et al., 2023; Ransomware Task Force, 2021; Robles-Carrillo & García-Teodoro, 2022; Rosenzweig, 2021).

Second, include measures to more discretely assess the potential impact and ramifications of increased efforts to disrupt the priority, focus, security, and cohesiveness of the hacker groups, individually or collectively, by hacking back, crippling supporting infrastructure, and infiltrating networks to recover decryption keys (Collier, 2021; Dudley & Golden, 2022a, 2022b). As mentioned previously, important in

this arena would also be modeling the resilience and vulnerabilities of hacker gangs and the RaaS business model (Baker, 2022; Krebs, 2021a; Sabin, 2023).

Third, we suggest modeling the impact of increased government resource allocation, beyond what's being directed today, to address this problem. Potential areas for greater government funding include law enforcement cybersecurity expertise and staffing, direct support to victims to aid in recovering from ransomware attacks, and increased R&D spending on defensive technologies and tools specifically designed to predict, detect, and block ransomware intrusions and attacks (Beaman et al., 2021; Dudley & Golden, 2022b; Kamil et al., 2022; Kok et al., 2019; McIntosh et al., 2022).

Ransomware is a serious global threat, not just in the arenas of healthcare, education, and local government, but for wider business and personal activities conducted online. It is a global problem that demands serious and concerted effort by governments, industry, non-governmental sectors, and academia. Policy decisions in this arena should be informed by data and decision makers need to know that their policies are precisely targeted, cost-effective, value-added, and free of unintended consequences. Moreover, since initiatives to tackle the cybersecurity threat can consume substantial public funds and divert the attention of agencies' staffs, decision makers need to recognize the impacts and benefits of those efforts.

This study indicates that government focus in areas that increase visibility of the immediate threat and other incentives to drive higher investments in defensive capabilities will result in the highest impact in combating ransomware. Moreover, measures focused on reducing the fraction of victims paying ransoms may not yield the expected results due to the revenue seeking behavior of hacker gangs. While these are not novel ideas for policy makers, the use of simulation tools to help understand the impact and ramifications of these government intervention vectors ultimately provides deeper insight and stronger justification. Ultimately the role of threat awareness as a trigger for corporate and government action, including both passive and active defenses and insurance coverage, stands out as instrumental in addressing this international problem.

This paper contributes to the academic and practical understanding of the ransomware problem as well as the overall cybersecurity threat and the range of government responses and interventions. By employing systems thinking with causal analysis, feedback loops and simulation, this research offers a means by which decision makers can better understand the range of factors underlying the ransomware problem and influencing Federal agency responses. A holistic, systems model of the ransomware environment capturing actors, motivations, business models, enablers, and both offensive and defensive capabilities, can offer a means by which decision makers can better understand the range of factors underlying the ransomware problem and the potential for influencing results through government responses. This study contributes to the relatively small but expanding body of research on system dynamics modeling in the field of cybersecurity. This paper also validates that system dynamics modeling can be effectively employed to gain insight on complex cybersecurity problems that threaten human activities online. To our knowledge, this study is the first to document a system dynamics model of ransomware and thus offers new insights into the methodology for examining a socio-economic and security challenge in cyberspace, as well as implications for policy makers. Our ability to effectively adapt and intervene to address real world problems of ransomware and future cybersecurity threats can help shape a safer and more productive online environment.

Reference List

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, *74*, 144–166. https://doi.org/10.1016/J.COSE.2018.01.001

Andersen, D., Cappelli, D. M., Gonzalez, J. J., Mojtahedzadeh, M., Moore, A. P., Rich, E., Sarriegui, J. M., Shimeall, T. J., Stanton, J. M., Weaver, E. A., & Zagonel, A. (2004). *Preliminary System Dynamics Maps of the Insider Cyber-threat Problem*. http://www.cert.org/research/sdmis/

Andersen, D. F., & Richardson, G. P. (1994). *Scripts for Group Model Building Center for Technology in Government*.

Bach, M. P., & Ceric, V. (2007). Developing system dynamics models with "step-by-step" approach. *Journal of Information and Organizational Sciences*. https://www.researchgate.net/publication/28811323

Baker, K. (2022, February 7). *Ransomware as a Service (RaaS) Explained*. CrowdStrike Cybersecurity 101. https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

Barlet, G. (2023, March 11). *US cyber strategy is missing accountability and a ransomware moonshot*. The Hill. https://thehill.com/opinion/cybersecurity/3895342-us-cyber-strategy-is-missing-accountability-and-a-ransomware-moonshot/

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers and Security*, *111*. https://doi.org/10.1016/j.cose.2021.102490

Benvenisti, R. (2022, October 26). *FBI and CISA Issue Joint Ransomware Alert For All Healthcare Facilities*. The Lackwood Scoop. https://thelakewoodscoop.com/news/fbi-and-cisa-issue-joint-ransomware-alert-for-all-healthcare-facilities/

Blosil, J. (2022, October 24). *Ransomware cost: Measuring the true cost of a ransomware attack*. NetApp Blog. https://www.netapp.com/blog/ransomware-cost/

Branch, L. E., Eller, W. S., Bias, T. K., McCawley, M. A., Myers, D. J., Gerber, B. J., & Bassler, J. R. (2019). Trends in Malware Attacks against United States Healthcare Organizations, 2016-2017. *Global Biosecurity*, *1*(1), 15. https://doi.org/10.31646/GBIO.7

Brooks, C. (2022, June 3). Alarming Cybersecurity Stats for Mid Year 2022. *Forbes*. https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=508b79347864

Chainalysis Team. (2023, January 19). *Ransomware Revenue Down As More Victims Refuse to Pay*. Chainalysis Blog. https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/

Chang, J. (2023). *119 Impressive Cybersecurity Statistics: 2023 Data & Market Analysis*. Financesonline.Com. https://financesonline.com/cybersecurity-statistics/

Chung, C. (2022, May 9). Lincoln College in Illinois to Close, Hurt by Covid and Ransomware Attack. *New York Times*. https://www.nytimes.com/2022/05/09/us/lincoln-college-illinois-closure.html

Claroty. (2020). *The Global State of Industrial Cybersecurity*. https://claroty.com/resources/reports/the-global-state-of-industrial-cybersecurity

Collier, B. (2021, September 8). The Secret Vulnerability of Cybercriminals: Burnout. *Wall Street Journal*. https://www.wsj.com/articles/secret-weakness-of-cybercriminals-they-are-bored-11631051849

Comizio, V. G., Corn, G., Deckelman, W., Hopkins, K., & Hughes, M. (2023). *Combating Ransomware: One Year On*. https://digitalcommons.wcl.american.edu/research

Cook, S. (2022, October 6). *Ransomware Statistics & Facts for 2018-2022*. Comparitech. https://www.comparitech.com/antivirus/ransomware-statistics/

Coveware. (2022a, January 27). *Ransomware as a Service Innovation*. Coveware. https://www.coveware.com/blog/2022/1/26/ransomware-as-a-service-innovation-curve

Coveware. (2022b, February 3). *Law enforcement pressure forces ransomware groups to refine tactics in Q4 2021*. Coveware Quarterly Ransomware Report. https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021

Coveware. (2022c, May 3). *Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting*. Coveware Ransomware Quarterly Report. https://www.coveware.com/blog/2022/5/3/ransomware-threat-actors-pivot-from-big-game-to-big-shame-hunting

Coveware. (2022d, July 28). *Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022*. Coveware Ransomware Quarterly Report. https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022

Coveware. (2023, January 20). *Improved Security and Backups Result in Record Low Number of Ransomware Payments*. Coveware Quarterly Report. https://www.coveware.com/blog/2023/1/19/improved-security-and-backups-result-in-record-low-number-of-ransomware-payments

Crowdstrike. (2022, October 10). *A Brief History of Ransomware*. CrowdStrike Cybersecurity 101. https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/

DeKorte, R. (2019). *Cybersecurity Insurance: Toward a more effective marketplace*. Utica College.

Dudley, R., & Golden, D. (2022a). *The Ransomware Hunting Team*. Farrar, Straus and Giroux.

Dudley, R., & Golden, D. (2022b, November 6). Why the F.B.I. Is So Far Behind on Cybercrime. *The New York Times*. https://www.nytimes.com/2022/11/06/opinion/ransomware-fbi.html

Editorial Board. (2023, February 8). How to fight back against ransomware hackers. *The Washington Post*. https://www.washingtonpost.com/opinions/2023/02/08/how-fight-back-against-ransomware-hackers/

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *Journal of Risk Finance*. https://doi.org/10.1108/JRF-09-2016-0122

Farhat, D., & Awan, M. S. (2021, June 28). A Brief Survey on Ransomware with the Perspective of Internet Security Threat Reports. *9th International Symposium on Digital Forensics and Security, ISDFS 2021*. https://doi.org/10.1109/ISDFS52919.2021.9486348

Felipe Luna-Reyes, L., Martinez-Moyano, I. J., Pardo, T. A., Cresswell, A. M., Andersen, D. F., & Richardson, G. P. (2006). Anatomy of a group model-building intervention: building dynamic theory from case study research. *Dyn. Rev*, *22*, 291–320. https://doi.org/10.1002/sdr

Forrester, J. (1961). *Industrial Dynamics* (2013th ed.). Martino Publishing.

Forrester, J. (2022). *Principles of Systems*. System Dynamics Society.

Gillum, J. (2022, November 22). Ransomware gangs shift tactics, making crimes harder to track. *The Seattle Times*. https://www.seattletimes.com/business/ransomware-gangs-shift-tactics-making-crimes-harder-to-track

Granato, A., & Polacek, A. (2019). The growth and challenges of cyber insurance. *Chicago Fed Letter*. https://doi.org/10.21033/CFL-2019-426

Greig, J. (2023, March 19). *Pro-Russia hackers are increasingly targeting hospitals, researchers warn*. The Record: Recorded Future News. https://therecord.media/killnet-ddos-hospitals-healthcare-russia

Griffiths, C. (2022, December 1). *The Latest 2022 Ransomware Statistics*. AAG-IT. https://aag-it.com/the-latest-2022-ransomware-statistics-updated-october-2022/

Hacquebord, F., Hilt, S., & Sancho, D. (2022). *The Near and Far Future of Ransomware Business Models*.

Haque, S., Eberhart, Z., Bansal, A., & McMillan, C. (2022). A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. *Association for Computing Machinery*. https://doi.org/10.1145/nnnnnnn.nnnnnnn

Harford, I. (n.d.). The history and evolution of ransomware. In *Tech Target*. Retrieved December 31, 2022, from https://www.techtarget.com/searchsecurity/feature/The-history-and-evolution-of-ransomware

Haughey, C. (2022, November 11). *How the U.S. Government is Fighting Back Against Ransomware?* Security Intelligence. https://securityintelligence.com/articles/us-gov-fighting-ransomware/

How are Ransomware Gangs Evolving their Expansion and Attack Strategy? (2022, May 22). SISA Infosec.Com. https://www.sisainfosec.com/blogs/how-are-ransomware-gangs-evolving-their-expansion-and-attack-strategy/

Insikt-Group. (2023). Threat Analysis 2022 Annual Report. In *Recorded Future*. www.recordedfuture.com

Jaikaran, C. (2021). *Federal Cybersecurity: Background and Issues for Congress*. https://crsreports.congress.gov

Jalali, M. S., & Kaiser, J. P. (2018a). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *J Med Internet Res 2018;20(5):E10059 Https://Www.Jmir.Org/2018/5/E10059*, *20*(5), e10059. https://doi.org/10.2196/10059

Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *Journal of Strategic Information Systems*, *28*(1), 66–82. https://doi.org/10.1016/j.jsis.2018.09.003

Janofsky, A. (2023). *Ransomware tracker: The latest figures [May 2023]*. Recorded Future. https://therecord.media/ransomware-tracker-the-latest-figures?utm_medium=email&_hsmi=258324964&_hsenc=p2ANqtz-_f6M0oNAnJL79teCkwM3fhqOjH-9p97ZHGAYD2_KwFbWFmJPQ0rVsYP69fXEnNFicq71xDEKyB74B_iIvh5o6lUmc_h-2ynQmtVZRLdTcCz1cjqVo&utm_content=258324964&utm_source=hs_email

Johnson, O. (2023, February 24). *CISA Leader Tells MSPs Cyber Insurance Market 'Fueled Rise In Ransomware.'* CRN. https://www.crn.com/news/channel-news/cisa-leader-tells-msps-cyber-insurance-market-fueled-rise-in-ransomware

Kamil, S., Siti Norul, H. S. A., Firdaus, A., & Usman, O. L. (2022). The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges. *2022 International Conference on Business Analytics for Technology and Security, ICBATS 2022*. https://doi.org/10.1109/ICBATS54253.2022.9759000

Kannan, U., & Swamidurai, R. (2019). Empirical Validation of System Dynamics Cyber Security Models. *IEEE SouthestCon*. https://ieeexplore.ieee.org/document/9020607

Kim, C. (2022). *Ransomware attacks decline amid crypto downturn*. Axios.Com. https://www.axios.com/2022/07/27/ransomware-attacks-decline-amid-crypto-downturn

King, A., & Gallagher, M. (2020). *Cyberspace Solarium Commission Final Report*. https://www.solarium.gov/

Kok, S. H., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). Ransomware, Threat and Detection Techniques: A Review. *International Journal of Computer Science and Network Security*, *19*(2), 136.

Krebs, B. (2021a, August 5). *Ransomware Gangs and the Name Game Distraction*. Krebs on Security. https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/

Krebs, B. (2021b, December 13). *Inside Ireland's Public Healthcare Ransomware Scare*. Krebs on Security. https://krebsonsecurity.com/2021/12/inside-irelands-public-healthcare-ransomware-scare/

LaBerge, L., O'Toole, C., Schneider, J., & Smaje, K. (2020). COVID-19 digital transformation & technology. In *McKinsey*. https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

Liska, A. (2021). *Ransomware: Understand. Prevent. Recover.* Actual Tech Media. www.actualtechmedia.com

Liska, A. (2022). *Ransomware*. https://www.recordedfuture.com/research

Livinston, Z. (2022, December 1). *Main Targets of Ransomware Attacks & What They Look For*. ESecurity Planet. https://www.esecurityplanet.com/threats/what-ransomware-attackers-look-for/

Lyngaas, S. (2023, January 31). *Ransomware: New US strategy prioritizes victims but could make it harder to catch cybercriminals*. CNN Politics. https://www.cnn.com/2023/01/31/politics/ransomware-disruption-hive-cybercrime/index.html

Marks, J. (2022, March 24). Officials are still in the dark on ransomware. *The Washington Post: Cybersecurity 202*. https://www.washingtonpost.com/politics/2022/03/24/officials-are-still-dark-ransomware/

Martinez, I. J., & Richardson, G. P. (2001, July). Best Practices in System Dynamics Modeling. *The 19th International Conference of the System Dynamics Society*.

Martinez-Moyano, I. J., Rich, E., Conrad, S., Andersen, D. F., & Stewart, T. R. (2008). A behavioral theory of insider-threat risks: A system dynamics approach. *ACM Transactions on Modeling and Computer Simulation*, *18*(2). https://doi.org/10.1145/1346325.1346328

Mascellino, A. (2023, March 4). CISA Unveils Ransomware Notification Initiative. *Infosecurity Magazine*. https://www.infosecurity-magazine.com/news/isa-unveils-ransomware/

Maslin Nir, S. (2022, November 28). *How a Cyberattack Plunged a Long Island County Into the 1990s*. The New York Times. https://www.nytimes.com/2022/11/28/nyregion/suffolk-county-cyber-attack.html

McIntosh, T., Kayes, A. S. M., Chen, Y. P. P., Ng, A., & Watters, P. (2022). Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions. In *ACM Computing Surveys* (Vol. 54, Issue 9). Association for Computing Machinery. https://doi.org/10.1145/3479393

McKinsey. (2023). *What is cybersecurity?* https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-cybersecurity?

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers and Security*, *92*. https://doi.org/10.1016/j.cose.2020.101762

Menn, J., Stein, P., & Schaffer, A. (2023, January 26). *Hive ransomware gang shut down by FBI, AG Merrick Garland says*. The Washington Post. https://www.washingtonpost.com/national-security/2023/01/26/hive-ransomware-fbi-doj/

NAIC. (2022, December 20). *Ransomware*. Center for Insurance Policy and Research. https://content.naic.org/cipr-topics/ransomware

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information and Management*, *52*(1), 123–134. https://doi.org/10.1016/j.im.2014.10.009

O'Donnell-Welch, L. (2022, July 22). *U.S. Government Grapples With Cyber Incident Reporting Pain Points*. Decipher. https://duo.com/decipher/cyber-incident-reporting-pain-points-a-government-push-and-public-perception

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *IET Networks*, *7*(5), 321–327. https://doi.org/10.1049/iet-net.2017.0207

Oosthuizenl, R., Pretorlus, L., Moutonl, F., & Molekoal, M. (2019). Cyber Security lnvestment Cost-Benefit lnvestigation Using System Dynamics Modelling. *International Conference on Cyber Warfare and Security*. https://www.proquest.com/docview/2198531577?pq-origsite=gscholar&fromopenview=true

Page, C. (2022, November 18). *Ransomware is a global problem that needs a global solution*. Tech Crunch. https://techcrunch.com/2022/11/18/combatting-ransomware

Portman, R., & Peters, G. (2021). *Federal Cybersecurity America's Data Still at Risk*. https://www.hsdl.org/?abstract&did=857006

Poulsen, K., & Evans, M. (2021, June 10). The Ruthless Hackers Behind Ransomware Attacks on U.S. Hospitals: 'They Do Not Care.' *WSJ*. https://www.wsj.com/articles/the-ruthless-cyber-gang-behind-the-hospital-ransomware-crisis-11623340215

Pratt, M. (2022, December 6). *What you should know when considering cyber insurance in 2023*. CSO Online. https://www.csoonline.com/article/3681852/what-you-should-know-when-considering-cyber-insurance-in-2023.html

Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself | Microsoft Security Blog. (n.d.). Retrieved July 2, 2023, from https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

Newman, L., & Burgess, M. (2023, July 12). Ransomware Attacks Are on the Rise, Again. *Wired*. https://www.wired.com/story/ransomware-attacks-rise-2023/

Ransomware gangs' favorite targets. (2022, September 31). Help Net Security. https://www.helpnetsecurity.com/2022/08/31/ransomware-attack-patterns/

Ransomware Task Force. (2021). *Combating Ransomware - A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force*. https://securityandtechnology.org/ransomwaretaskforce/

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, Mitigation and Prevention. *International Management Review*, *13*(1). https://digitalcommons.kennesaw.edu/facpubs/4276

Robles-Carrillo, M., & García-Teodoro, P. (2022). Ransomware: An Interdisciplinary Technical and Legal Approach. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/2806605

Rosenzweig, P. (2021, August 31). Opinion _ There's a Better Way to Stop Ransomware Attacks. *The New York Times*.

Roumani, M., Fung. Chun Che, & Choejey, P. (2015). Assessing Economic Impact due to Cyber Attacks with System Dynamics Approach. *International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*. https://ieeexplore.ieee.org/document/7207084

Rudis, R. (2022, July 12). *RTF Year Two: New Map; New Data: Same Mission*. Institute for Security + Technology. https://securityandtechnology.org/blog/rtf-year-two-new-map-new-data-same-mission/

Sabin, S. (2023, February 24). *Russia's cybercrime underground is starting to recover from Ukraine war disruptions*. Axios. https://www.axios.com/2023/02/24/russian-cybercrime-rebound-ukraine?utm_source=pocket_saves

SafeAtLast. (2022). *22 Shocking Ransomware Statistics for Cybersecurity in 2021*. https://safeatlast.co/blog/ransomware-statistics/#gref

Sakellariadis, J. (2023, May 23). *Ransomware comes back with a vengeance*. Politico. https://www.politico.com/newsletters/weekly-cybersecurity/2023/05/15/ransomware-comes-back-with-a-vengeance-00096869

Shakir, U. (2023, January 27). *FBI takes down Hive ransomware network*. The Verge. https://www.theverge.com/2023/1/27/23574257/fbi-us-justice-department-seizes-hive-ransomware-network-servers

Shanklin, W. (2023, January 26). *DOJ says it disrupted a major global ransomware group*. Endgadget. https://www.engadget.com/hive-ransomware-doj-fbi-disruption

Singleton, C., Kiefer, C., & Villadsen, O. (2020, October 30). *Ransomware 2020: Attack Trends Affecting Organizations Worldwide*. SecurityIntelligence.Com. https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/

Snape, G. (2022, October 5). *Data breaches are costing more – what companies need to know*. Fintech News. https://www.fintechnews.org/data-breaches-are-costing-more-what-companies-need-to-know/

Sobers, R. (2022, May 20). *89 Must-Know Data Breach Statistics [2022]*. Varonis.Com. https://www.varonis.com/blog/data-breach-statistics

SonicWall. (2022). *Mid-Year Update: 2022 SonicWall Cyber Threat Report*.

Sophos. (2022). *The State of Ransomware 2022*. https://www.sophos.com/en-us/content/state-of-ransomware

Starks, T. (2022a, August 17). Is the drop in ransomware numbers an illusion? *The Washington Post*. https://www.washingtonpost.com/politics/2022/08/17/is-drop-ransomware-numbers-an-illusion/

Starks, T. (2022b, October 6). An 'unprecedented' hospital system hack disrupts health-care services. *The Washington Post*. https://www.washingtonpost.com/politics/2022/10/06/an-unprecedented-hospital-system-hack-disrupts-health-care-services/

Starks, T. (2023a, March 30). Think ransomware gangs won't thrive this year? Think again, experts say. *The Washington Post*. https://www.washingtonpost.com/politics/2023/03/30/think-ransomware-gangs-wont-thrive-this-year-think-again-experts-say/

Starks, T. (2023b, May 23). Influential task force takes stock of progress against ransomware. *The Washington Post*. https://www.washingtonpost.com/politics/2023/05/05/influential-task-force-takes-stock-progress-against-ransomware/

Sterman, J. (2000). *Business Dynamics Systems Thinking and Modeling for a Complex World*. McGraw Hill Education.

Temple-Raston, D., & Glueck, G. (2023, May 16). *Knocking down Hive: How the FBI ran its own ransomware decryption operation*. Recorded Future. https://therecord.media/hive-ransomware-decryptors-fbi-bryan-smith-interview-click-here

The Ransomware Ecosystem - RaaS, Extortion, Cryptocurrency. (n.d.). Retrieved July 2, 2023, from https://ransomware.org/what-is-ransomware/the-importance-of-cryptocurrency-raas-and-the-extortion-ecosystem/

Tidy, J. (2023, January 19). *Cyber-crime gangs' earnings slide as victims refuse to pay*. BBC News. https://www.bbc.com/news/technology-64323980

Trim, P., & Upton, D. (2016). Cyber Security Culture : Counteracting Cyber Threats through Organizational Learning and Training. *Cyber Security Culture*. https://doi.org/10.4324/9781315575681

Uberti, D. (2021, May 25). High-Profile Hacks Leave Ransomware Gangs with Unwanted Publicity. *WSJ*. https://www.wsj.com/articles/high-proile-hacks-leave-ransomware-gangs-with-unwanted-publicity-11621935000

Vicens, A. (2022, November 1). *Ransomware costs top $1 billion as White House inks new threat-sharing initiative*. CyberScoop. https://wwhttps://www.cyberscoop.com/ransomware-payments-cost-treasury/w.cyberscoop.com/ransomware-payments-cost-treasury/

Vijayan, J. (2023, February 13). *Healthcare in the Crosshairs of North Korean Cyber Operations*. DarkReading. https://www.darkreading.com/attacks-breaches/healthcare-in-the-crosshairs-of-north-korean-cyber-operations

Waldman, A. (2022, July 21). *NCC Group observes a drop in ransomware attacks -- for now*. TechTarget. https://www.techtarget.com/searchsecurity/news/252523029/NCC-Group-observes-a-drop-in-ransomware-attacks-for-now

Warner, M. (2022). *CyberSecurity is Patient Safety*.

Woods, D. W. (2023). A Turning Point for Cyber Insurance. *Communications of the ACM*, *66*(3), 41–44. https://doi.org/10.1145/3545795

Wuest, C. (2022, August 25). *Ransomware dominates the threat landscape*. Help Net Security. https://www.helpnetsecurity.com/2022/08/25/ransomware-dominates-threat-landscape/

Yang, S. C., & Wang, Y. L. (2011). System Dynamics Based Insider Threats Modeling. *International Journal of Network Security & Its Applications*, *3*(3), 1–14. https://doi.org/10.5121/ijnsa.2011.3301

Zorz, Z. (2022, August 31). *Should ransomware payments be banned? A few considerations*. Help Net Security. https://www.helpnetsecurity.com/2022/08/31/should-ransomware-payments-be-banned-considerations-video/

Appendix A – Ransomware Ecosystem

As noted in the main text, ransomware is a serious threat to the cyber ecosystem and the activities existing in it or supported by it. It is also multifaceted, highly complex, and devious. The connective links, relationships, and influences are many and varied. The following table seeks to simplify this complex ecosystem. While this table is the authors' work, it was shaped by a variety of source material, academic, historical, governmental, and public news. We refer the reader to the following rich set of sources: (Al-rimy et al., 2018; Baker, 2022; Beaman et al., 2021; Cook, 2022; Coveware, 2022a; Crowdstrike, 2022; Dudley & Golden, 2022a; Farhat & Awan, 2021; Griffiths, 2022; Haque et al., 2022; Harford, n.d.; Haughey, 2022; Insikt-Group, 2023; Kamil et al., 2022; Kok et al., 2019; Krebs, 2021a; Liska, 2021; Livinston, 2022; Meland et al., 2020; O'Kane et al., 2018; Ransomware Task Force, 2021; Richardson & North, 2017; Rudis, 2022; Sophos, 2022; Starks, 2023b).

This table captures the essential characteristics of the ecosystem. Using the prism of five different levels, it shows the difference between the six major stakeholder groups. The five levels are I. Motivation, II. Cyber Tools and Infrastructure, III. Economics, Business Models, and Payment Infrastructure, IV. Alliances and Partnerships, and V. Operating Environment and Rules. The six major or active stakeholders are Hacker Gangs, Targeted Entities, Cybersecurity Industry and Workforce, Insurance Sector, National Governments (Democracies), and Law Enforcement and Cybersecurity Agencies.

The causal diagrams and system dynamics model we create and explain in this study are founded upon this basic understanding of the ecosystem.

Table A-1 High-Level View of Ransomware Ecosystem

Ransomware Ecosystem						
Level	**Hacker Gangs**	**Targeted Entities (Corporations, Non-Profits, Schools,**	**CyberSecurity Industry and Workforce**	**Insurance Sector**	**National Governments (Democracies)**	**Law Enforcement and Government CyberSecurity**
Level V. Operating Environment and Rules	Benign operating environment (mostly) Few bounds on behavior or targets Host government support Target decisions (sector, size, pWin)	Digital transformation Online customer-facing presence Connected supplier interactions Connected backoffice support Networked organizational data COOP, backup and recovery plans Defensive cyber measures only Option to report incidents Option to pay ransoms	General prohibitions against hack back Industry standard best practices	Federal and state governance Ransom negotiation guidelines	Balance free markets and mandates Respect for freedoms in cyberspace Respect for privacy in cyberspace International norms for free nations	Criminal justice codes Infrastructure takedowns Hacker gang infiltration/disruptions Indictments, arrests and prosecutions Competing priorities
Level IV. Alliances and Partnerships	Coordination on the Dark Web RaaS brands and affiliates Sharing targets data Sharing attack vectors and techniques Community cohesiveness Agility to rebrand and transform	Trade, industry, sector associations Post-attack support gov and private	Industry associations Information sharing alliances Open web sites, portals, and blogs	Insurance agency cooperatives Access to private consultants	International partnerships Industry lobbying (cybersecurity and sectors) Sponsor task forces and intiatives	Cross agency partnerships International partnerships Public-private partnerships Interagency task forces Elite ransomware consultants
Level III. Economics, Business Models and Payment Infrastructure	Profitability Reinvestment decisions Financial support to illegal activities Illicit, covert, hidden payment infrastructure Ransomware as a Service model	Increasing business activity online Sector priority for cybersecurity Cost of deploying new defensive tools Insurance coverage and risk decisions Ransom payment tradeoffs Alternatives to paying ransom	Cyber workforce supply & demand Investments based on ROI calculations	Risk calculus Premium calculations Policy limitations	Financial regulation of crypto currencies	Ability to trace financial transactions Ability to recover ransom payments
Level II. Cyber Tools and Infrastructure	Network surveillance tools Network intrusion tools Techniques to encrypt data Secure, reliable, economic infrastructure Ease of deployment and operation Speed of deployment	Overall attackable surface Vulnerability awareness and fixes Cyber hygiene / baseline standards Sector priority for cybersecurity Cost of deploying new defensive tools Independent network/data backups User awareness, training & compliance	Cyber defense R&D opportunities Cyber defense business development Emerging tools (predict, detect, block) Techniques to recover decryption keys	Best practices Underwriting standards Technical inspection of client networks Ops ssessment of client processes Holistic protection	National level investments in cyber R&D NIST standards CISA leadership, oversight, coordination	Cyber surveillance / intelligence Techniques to disrupt hacker networks Agents with organic cyber skills Training to improve cyber skills R&D, acquisition, and deployment
Level 1. Motivation	Financial gain Cybersuperiority complex Competitive sport Break the rules and not get caught Gang cohesiveness Priority of work Recruiting and retention	Buiness/mission continuity Customer service Avoid financial disruption or loss Reputation of the organization Protect privacy of customer data	Financial gain Remaining current Competitive sport (to a lessor degree)	Financial gain Support client needs Reputation of the firm Enable client privacy	National level problem awareness Political pressures to act Political will to invest resources Political will to make tough choices Competing pressures for attention	Protection of citizen Agent professionalism and zeal Track record of successful cases Priority of work Competitive sport (in some cases) Agency wins and publicity

Appendix B – Full System Dynamics Model Structure

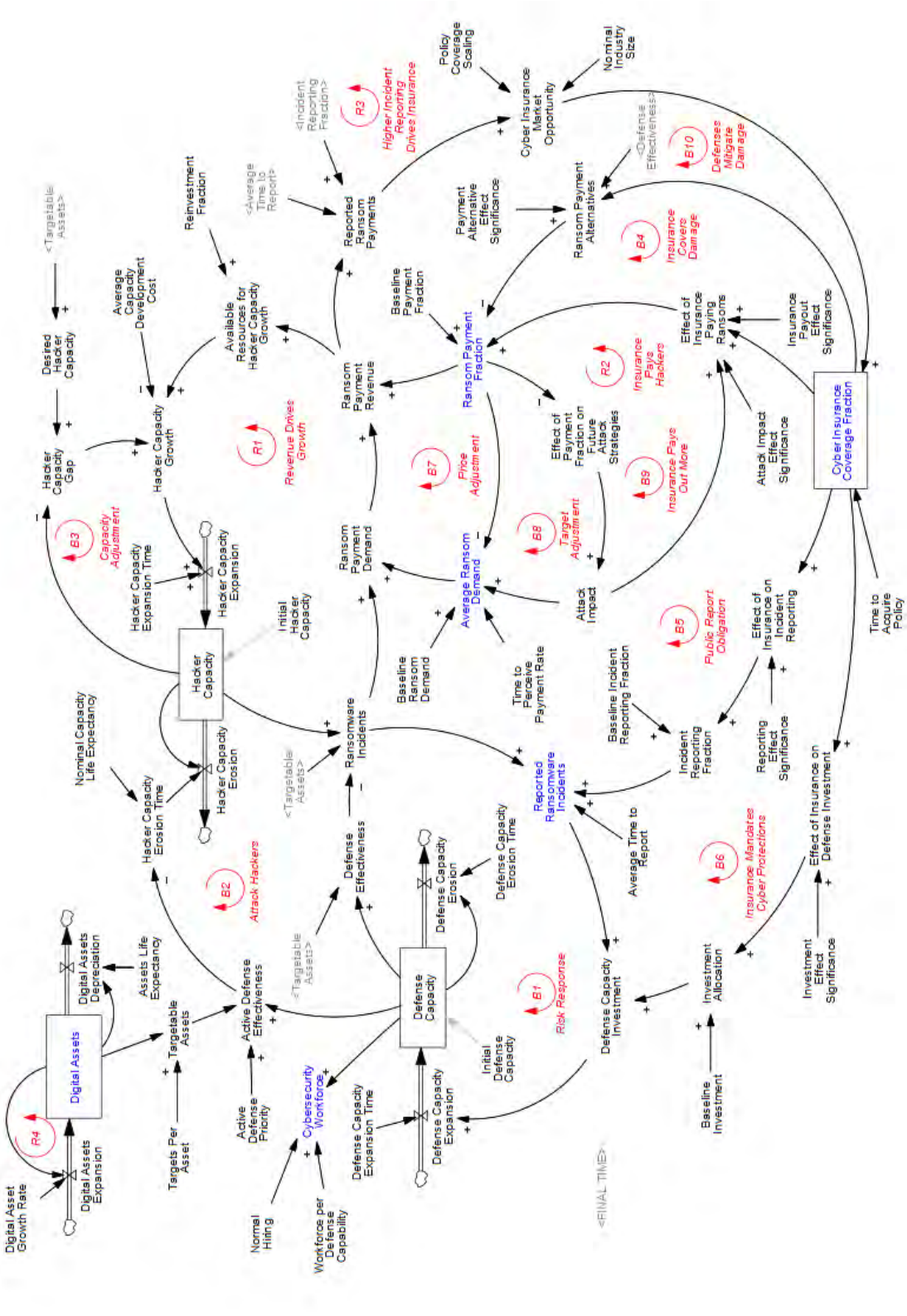


Figure C-1 Full System Dynamics Model Structure

Appendix C – List of Equations

Ransomware Incidents = (1 - Defense Effectiveness)*MIN(Targetable Assets, Hacker Capacity)

Reported Ransomware Incidents = SMOOTH3(Ransomware Incidents*Incident Reporting Fraction, Average Time to Report)

Defense Capacity Investment = Reported Ransomware Incidents*Investment Allocation

Investment Allocation = MIN(0.9, Baseline Investment + Effect of Insurance on Defense Investment)

Incident Reporting Fraction = MIN(0.9, Baseline Incident Reporting Fraction + Effect of Insurance on Incident Reporting)

Defense Effectiveness = MIN(1, Defense Capacity/Targetable Assets)

Active Defense Effectiveness = MIN(0.9, (Defense Capacity/Targetable Assets)*Active Defense Priority)

Hacker Capacity Erosion Time = Nominal Capacity Life Expectancy*EXP(-Active Defense Effectiveness)

Hacker Capacity Gap = MAX(Desired Hacker Capacity-Hacker Capacity, 0)

Hacker Capacity Growth = MIN(Hacker Capacity Gap, Available Resources for Hacker Capacity Growth/Average Capacity Development Cost)

Available Resources for Hacker Capacity Growth = Ransom Payment Revenue*Reinvestment Fraction

Ransom Payment Demand = Ransomware Incidents*Average Ransom Demand

Ransom Payment Revenue = Ransom Payment Demand*Ransom Payment Fraction

Reported Ransom Payments = SMOOTH3(Incident Reporting Fraction*Ransom Payment Revenue, Average Time to Report)

Cyber Insurance Market Opportunity = MIN(0.9, Reported Ransom Payments/Policy Coverage Scaling + Nominal Industry Size)

Cyber Insurance Coverage Fraction = SMOOTHi(Cyber Insurance Market Opportunity, Time to Acquire Policy, 0.26)

Effect of Insurance on Defense Investment = Cyber Insurance Coverage Fraction*Investment Effect Significance

Effect of Insurance on Incident Reporting = Cyber Insurance Coverage Fraction*Reporting Effect Significance

Effect of Insurance Paying Ransoms = MIN(0.9, (Cyber Insurance Coverage Fraction*Insurance Payout Effect Significance) + Attack Impact Effect Significance*Attack Impact)

Ransom Payment Fraction = Baseline Payment Fraction + Effect of Insurance Paying Ransoms-Ransom Payment Alternatives

Average Ransom Demand = SMOOTHi(Baseline Ransom Demand/Ransom Payment Fraction*Attack Impact, Time to Perceive Payment Rate, 8000)

Ransom Payment Alternatives = Cyber Insurance Coverage Fraction*Payment Alternative Effect Significance + Defense Effectiveness

Effect of Payment Fraction on Future Attack Strategies = 1 - Ransom Payment Fraction

Attack Impact = SMOOTHi (Effect of Payment Fraction on Future Attack Strategies, 12, 0.1)

Appendix D – Additional Model and Policy Verification

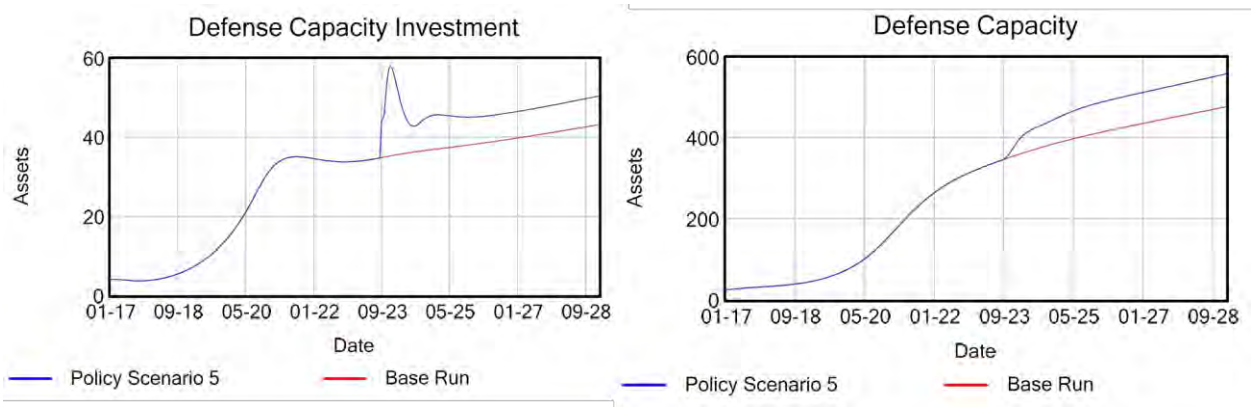


Figure E-1 Investment and Defense Capacity – Policy Scenario 5

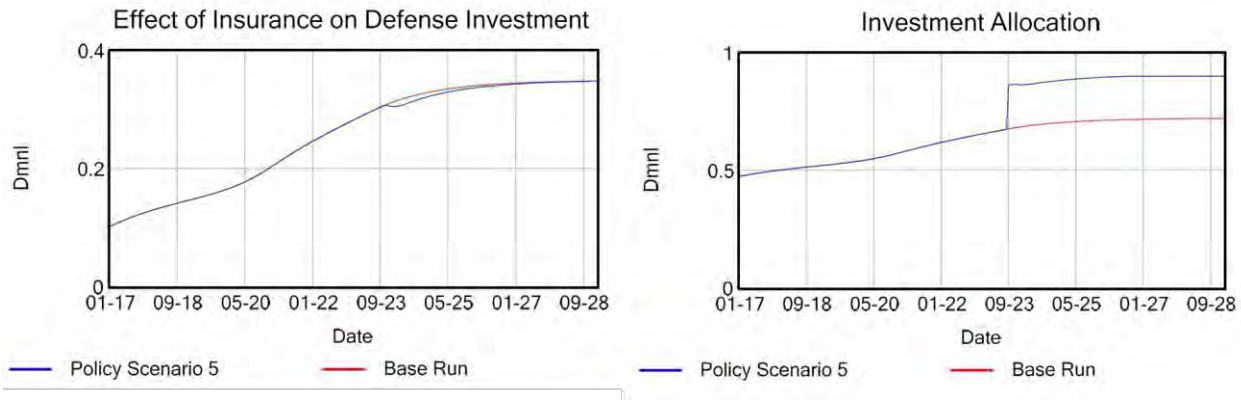


Figure E-2 Effect of Insurance on Investment and Investment Allocation – Policy Scenario 5

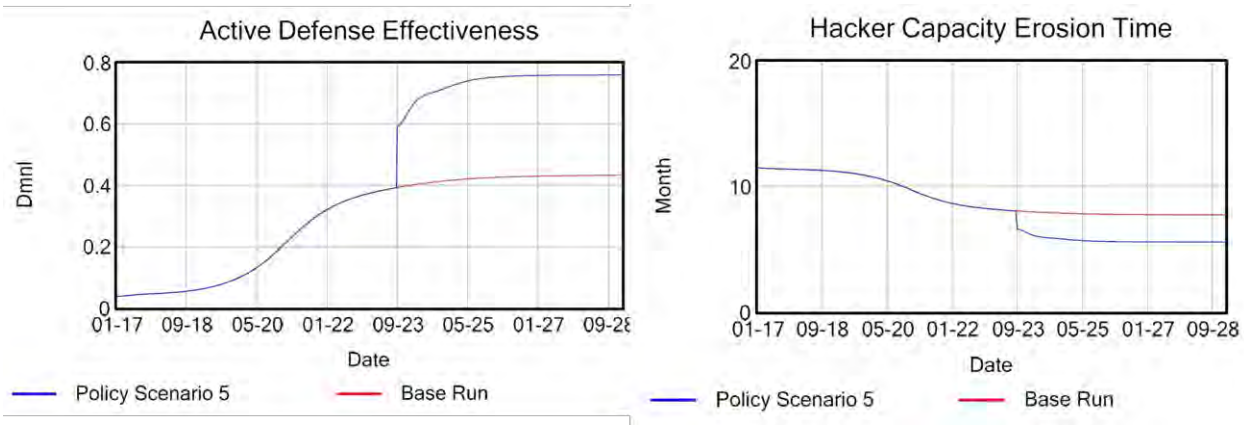


Figure E-3 Active Defense Effectiveness and Hacker Capacity Erosion Time – Policy Scenario 5

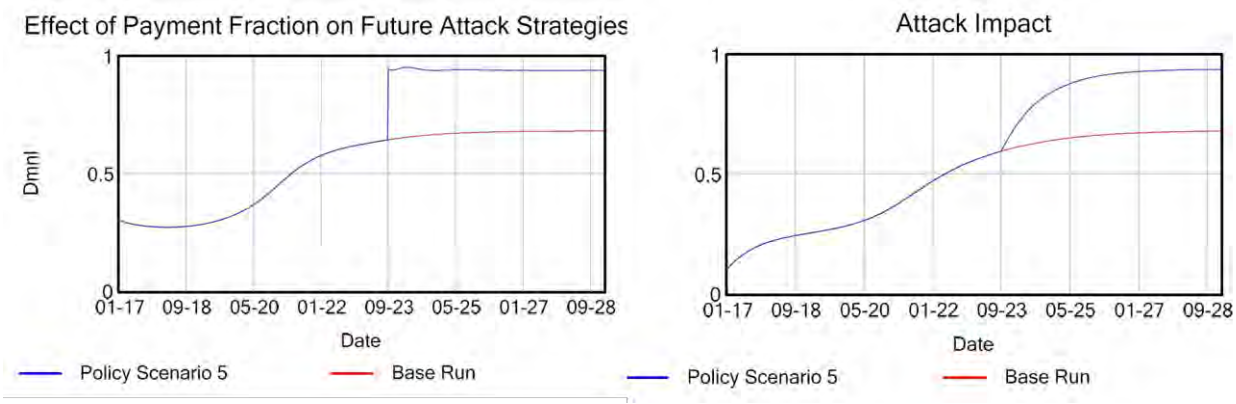


Figure E-4 Effect of Payment Fraction on Attack Strategies and Attack Impact – Policy Scenario 5

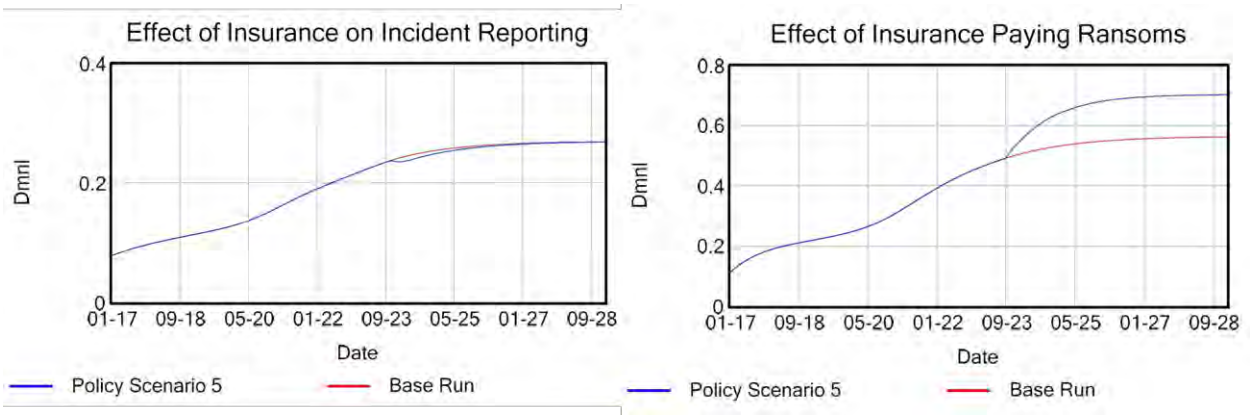


Figure E-5 Effect of Insurance on Incident Reporting and on Paying Ransoms – Policy Scenario 5

Appendix E – Supplemental Material

Vensim File Code

Parameter Data File