




| Whitepaper

A RISK ASSESSMENT FOR RANSOMWARE PREVENTION IN OPERATIONAL TECHNOLOGY (OT) ENVIRONMENTS

November 2021

Tom Winston, Ph.D.
Director, Intelligence Content
Dragos, Inc.

 info@dragos.com


 [@DragosInc](https://twitter.com/DragosInc)

TABLE OF CONTENTS

Abstract 3

Overview 4

Ransomware is a Serious Problem..... 5

Risk Assessment in Connected Systems 6

Complex Systems Approach to Ransomware 7

How are IT and OT Systems Considered Complex?..... 8

More Context 10

A Complex Systems Solution for a Complex Problem in Simple Terms 11

Methodology..... 12

Generalized Formula for Each Function 13

Optimization in the System..... 13

Further Thoughts on this Approach..... 14

Simulated Examples 14

How to Assess Values of Security Implementations 16

Conclusion 16

Further Research..... 17

References 17

ABSTRACT

Ransomware has become the primary attack vector for many industrial organizations during 2021. Incidents like Colonial Pipeline, Honeywell, and JB Foods showed the world that even when industrial control systems are not specifically the target, ransomware attacks on enterprise IT systems which are integrated with operational technology (OT) cause major disruptions. This paper considers a novel approach to conducting a risk assessment in such environments to produce a quantifiable value representing an organization's risk exposure.

Ransomware not only creates unusable file systems, but it can also halt processes, stop production, disrupt distribution, and can cost millions of dollars and cause weeks long headaches for victims. By dumping data to dedicated leak sites ransomware gangs can release intellectual property and personally identifiable information (PII). The techniques are varied, but they have common themes, accessing the infrastructure through known vulnerabilities. Once adversaries achieve initial access, they execute other programs to gain a foothold in critical enterprise IT systems and can move laterally to OT systems. Victims must pay the ransom to regain access to their file systems and regain control of their processes that use the file systems. Victims must decide the best course of action for their organization.

Best practices, and better "cyber hygiene" have proven ineffective against the blended approaches ransomware adversaries employ. The research in this paper explores a solution to securing environments that is rooted in complex systems analysis and advanced mathematics, presented in a way that stakeholders can use immediately. In this approach we avoid much of the differential calculus that underpins it, to make this paper more easy to read and digest across a wide variety of industries.

OVERVIEW

You have probably heard the phrase, “cyber never sleeps.” Unfortunately, this credo is 100 percent correct. Not only does “cyber” (a reference to cyber attack vectors) never sleep, but it also constantly evolves and constantly surprises. During the first half of 2021, the average remediation cost of ransomware cyber attacks has doubled to approximately \$1.85 million¹. The Energy, Oil, Gas and Utilities sectors typically has the most difficult to update infrastructure, and thus has the greatest propensity to pay the ransom². This includes downtime, people hours, device costs, network costs, lost opportunities, ransom paid, etc.

Unlike other cyber attacks or breaches that are sometimes difficult to quantify, ransomware attacks have a very specific value assigned to them, typically based on the adversary’s background and the analytical research of the organization’s cyber attack insurance. Organizations can use cyber attack insurance to pay for ransomware attacks, and actuaries calculate the value of an organization’s infrastructure and charge a premium based on that value. According to Dragos Research³, out of all the Industrial Control Systems (ICS) sectors in 2021, ransomware groups targeted the manufacturing industry more than any other. Dragos has compiled data on Dedicated Leak Sites (DLS) leveraged by ransomware actors to analyze trends for June and July regarding the Manufacturing Sector. Of 56 ICS-related DLS postings identified by Dragos in June and July, 29, or 52%, were regarding the Manufacturing Sector. Of these 26, the most commonly posted manufacturing sub-sectors were Automotive (21%), Technology (14%), and metal components (14%). Nineteen out of

26 postings were made by Conti or Lockbit 2.0; notably, Manufacturing Sector targets made up 75% of Lockbit 2.0’s ICS postings. While Conti primarily targets firms in English-speaking nations, their victims were located globally. Lockbit 2.0 posted information regarding firms in eight different countries around the world. Dragos assesses with moderate confidence that ransomware trends are likely to continue shifting as groups are taken offline, pursued by law enforcement, reformed, and reprioritized; however, DLS data provides some insight into the current activity of ransomware groups that can be leveraged by defenders to better protect their organizations⁴.

The ransoms range from hundreds to tens of millions of United States dollars. Stepping back and taking a look at the psychology of risk avoidance, aversion, and protection can help us to better understand the underpinnings of this phenomenon – not just “how this is happening,” but perhaps most importantly “why this is happening.”

RANSOMWARE IS A SERIOUS PROBLEM

During the first six months of 2021 adversaries ransomed many manufacturing organizations including Molson Coors, Honeywell, JBS S.A., and of course Colonial Pipeline. In every instance, blurred lines between Information Technology (IT) and Operational Technology (OT) contributed to the vulnerability of these companies to ransomware. The ransomed companies have a very difficult decision to make in short order: How do we restore operations, how can we quickly and easily stop the money hemorrhage, and how can we keep our shareholders happy? These questions are among the myriad questions facing ransomed organizations.

According to a body of open-source reporting, many of these organizations have paid the ransoms only to find that their systems do not function properly, even after the ransomware groups release the decryption keys. According to Sophos, victims only got 65% of data back on average after paying the ransom⁵.

Ransomware adversaries capitalize on a perfect storm of antecedent conditions including weak boundaries between OT and IT, poorly understood interactions between systems

and systems of systems, and remote access schemas put in place to serve work from home pandemic needs. This research in no way, shape, or form is decrying the security posture of any organization. However, it attempts to address the ransomware problem in a piecemeal and logical manner that will provide some basis for an overall security rating to help reduce the impact of ransomware. From a technical standpoint, ransomware adversaries gain initial access through corporate IT infrastructure, and in some instances are able to negatively impact OT infrastructure through lateral movement mechanisms. While it's true that organizations will never be able to stop 100% of attacks, including ransomware, this methodology hopes to greatly reduce the impact an attack may have on an organization.

Ransomware adversaries use a blended approach to compromise an organization and demand ransoms that require victims to pay for the keys used to decrypt the file systems the adversaries compromise. Ransomware adversaries also use the threat of the release of the unencrypted Personally Identifiable Information (PII) or other sensitive corporate information (presumably exfiltrated before encrypting the file systems) to dump leak sites on the dark web. This has happened time and again throughout the first half of 2021. Victims have little recourse to restore functionality to their systems but to pay the ransoms. This has become a point of debate as well – which is not covered by the scope of this paper.

RISK ASSESSMENT IN CONNECTED SYSTEMS

It is easy to understand how many actions, or lack thereof, can change risk levels for those undertaking the actions. In a like manner, it is relatively simple to make a few assumptions about the lack of safety online. However, protection online varies from person to person, and from organization to organization. Protection Motivation Theory (PMT), as posited by Rogers (1975)⁶ describes a framework used to explain people's behavior to protect themselves against risk in a health context. Later researchers⁷ have applied PMT to protective behaviors in the context of cybercrime⁸. Analysts have observed a real, appreciative rise in ransomware targeting industrial organizations and according to a 2020 Dragos whitepaper⁹, many of the incidents have resulted in disruption to industrial operation. The idea of risk acceptance does not easily explain the recent spate of ransomware attacks. Risk acceptance occurs when a business or individual acknowledges that the potential loss from a risk is not great enough to warrant spending money to avoid it. The ransomware attack vectors are not always straightforward, and their impact is not always well understood. The impact is different among IT and OT assets in an organization. According to a variety of open sources, ransomware adversaries use publicly available information to determine the cost of the ransom to a given organization. This cost is usually substantial, but the risk of losing days, weeks, or even potentially months of manufacturing, distribution, and delivery is far greater.

This presents a complex system optimization problem to the victims. There are upfront costs associated with typical risk avoidance measures which include:

- **SECURITY CONTROLS**
 - Defense in depth methodologies such as segmented networks
 - A clear understanding of how OT and IT interact
- **IMPLEMENTATION**
 - Auditing
 - Secure access controls
 - Secure remote access controls
 - Updated software and hardware across IT and OT spectra
- **HYGIENE**
 - Strategic security plans to adjust to changing needs of the organizational IT and OT

Organizations must balance the up-front cost of these measures against exposure to ransomware attack vectors (unpatched vulnerabilities), and eventual ransoms if the first holds true. Complex systems are systems where the behavior is intrinsically difficult to model due to the dependencies, competitions, relationships, or other types of interactions between their parts, or between a given system and its environment. There is much math devoted to this area of inquiry, and we will avoid the abstract nature of such problems in this paper to stay on point.

The field of Game Theory¹¹ examines how decisions that one player makes affect (negatively or positively) the future decisions of other players in the game. Evolutionary Game Theory (EGT) predicts behaviors where there may not be any overall intention on the decisions made by the players in the game. Game Theory posits those decisions made by others in the game and how they affect the individual decisions made by any one player. This relates well to the conundrum posed by ransoms and ransomware. Where EGT falls though is that it

assumes players will make decisions based on evolutionary, stable strategies, or behaviors that persist in a population once they are found to be prevalent. Relating EGT to the complex series of events that lead to a ransomware attack is perhaps a stretch, and indeed relating biological science to the ransomware paradigm may also be a stretch. However, it should be noted that as EGT is a complex system of interactions that lead to further interactions, the antecedent conditions in organizations plagued with ransomware are actually no different.

COMPLEX SYSTEMS APPROACH TO RANSOMWARE

There is very little research that considers ransomware from the complex systems optic. Ransomware is successful due to a lack of understanding about how systems of things interact with systems of other (different) things. Complex systems are systems where modeling is complicated by the dependencies, relationships, or other “interactions” between parts of one system, and parts of another. This is a scientific approach that investigates how relationships between a system’s parts give rise to its collective behaviors, and how the system interacts and forms relationships with its environment. The study of complex systems regards collective, or system-wide, behaviors as the fundamental object of study. For this reason, complex systems can be understood as an alternative paradigm to reductionism, which attempts to explain systems in terms of their constituent parts and the individual interactions between them¹². The IT/OT divide is not actually relevant for this research because in practice

this is generally a blurred line. The vast majority of ransomware starts in the IT of organizations, and only a few cases have had the built-in capability to directly affect OT assets (EKANS, for example).

HOW ARE IT AND OT SYSTEMS CONSIDERED COMPLEX?

Grossly generalizing IT and OT systems as complex is not appropriate without some explanation of how this research considers them and how they meet some of the characteristics of complex systems. First, it helps to consider how many complex systems people interact with on a daily basis: financial markets, weather, politics, community dynamics, etc. can all be considered complex systems. Identifying the quantifications of complex systems is not obvious. A broad body of research associates three, five, or even seven characteristics to what defines a complex system. For the purposes of this research, the following characterize complex systems: Emergence, non-linearity, limited predictability, effects of small changes leading to large events, evolutionary dynamics, self-organization, and fundamental uncertainty¹³.

EMERGENCE

The interactions of the various elements in these systems constitute the behavior of the system as a whole. Whether in the IT or the OT, the way these elements are connected (or isolated) dictates the complexity of the system. Models that describe and define specific layers and levels between IT and OT infrastructure may not apply, if even only for the sake of discussion. The sum of the parts is not just greater than its whole, but its operations are susceptible to minor perturbations (see “small changes...” below).

NON-LINEARITY

While it is true that process-specific applications may have measurable setpoints that fall into linear patterns, the interaction of these controllers with other devices in the system may not necessarily exhibit this behavior. The IT/OT interactions as a whole may successfully measure discrete events (e.g. intrusions or attempts), it is not generally the case that such perturbations in the IT systems have any measurable effect in the OT systems. If they do, they may or may not be measured.

LIMITED PREDICTABILITY

Considering the myriad of defense in depth topics that comprise most IT security discussions, security as a whole is difficult to predict because antecedent conditions may or may not relate well to current or future ones, and small changes, configurations, or upgrades can cause perturbations across the whole system that are generally not well tracked. This leads to the next issue regarding the effects of small changes leading to large events.

SMALL CHANGES CAN DISRUPT COMPLEX SYSTEMS

Arguably, this topic alone could provide the foundation for a sanguine discussion about how ransomware capitalizes on a lack of understanding of how IT and OT form a complex system. If a small, upstream perturbation causes an imbalance in the equilibrium of one system connected to another, it can cause catastrophic consequences for downstream entities. For example, the global pandemic forced more work-from-home arrangements and increased remote access paradigms for organizations. While functionally this solved the

problem of isolating employees and encouraged them to do their jobs, the sum effect of this has been seen in situations like the Oldsmar, Florida water plant breach¹⁴. The City of Oldsmar employees used a remote access software package, TeamViewer, that led to manipulation of control set points for the dosing rate of Sodium Hydroxide (NaOH) into the water^{15,16}.

EVOLUTIONARY DYNAMICS

Complex adaptive systems are often shaped by evolutionary dynamics. The mechanism of evolution starts with variation. Then there is selection of elements that are fit for the changed conditions. These elements flourish and multiply in the system. They may also change the external environment of the system, causing new variation. New variation may also come from outside the system. A new cycle of variation-selection-multiplication-variation starts. The system is never at rest. There is no movement to a knowable “end point” or equilibrium. There is constant change and innovation¹⁷. This relates almost directly to the variability of security over time and space of each of the components in the systems. A device may possess x number of vulnerabilities on day zero of its installation, but then when connected to other devices exhibits $x+n$ (n meaning new vulnerabilities discovered in the context of the system(s) where employees will use the device.

SELF-ORGANIZATION

Complex systems operate through distributed controls that affect different parts of different systems that interact. This classical idea suggests that systems organize themselves from the smallest parts to the largest parts. This characteristic of complex systems is a reach when considering the IT/OT ransomware

conundrum. However, it provides an idea that resonates with many IT and OT professionals – asset identification and understanding is key.

FUNDAMENTAL UNCERTAINTY

It is easy to understand and agree that cybersecurity is fundamentally uncertain. The future in cybersecurity is dim and there is no literature at the time of this publication that provides a good predictive tool for the health and security of the internet. Machine Learning (ML) applications in Artificial Intelligence (AI) are discussed regularly as part of this solution, but this science is relatively new. At the time of this publication, ransomware is prevalent and costing organizations millions of dollars. Therefore, it is safe to assume that this trend will continue.

MORE CONTEXT

As discussed in the previous section – IT and OT systems are complex in that there are many parts to each system, and that the systems interact in predictable or unpredictable ways, depending on the initial state of each system, and how they interact. To follow up on a comment earlier in this paper regarding the ubiquity of complex systems in daily life, this list from Randall (2011) suggests complex systems have the following features: cascading failures, complex systems may exhibit critical transitions, and relationships are non-linear¹⁸:

CASCADING FAILURES

Due to the strong coupling between components in complex systems, a failure in one or more components can lead to cascading failures that may have catastrophic consequences on the functioning of the system¹⁹. Localized attacks may lead to cascading failures and abrupt collapse in spatial networks²⁰.

COMPLEX SYSTEMS MAY EXHIBIT CRITICAL TRANSITIONS

Critical transitions are abrupt shifts in the state of ecosystems, the climate, financial systems or other complex systems that may occur when changing conditions pass a critical or bifurcation point^{21, 22, 23, 24}. The “direction of critical slowing down” in a system’s state space may be indicative of a system’s future state after such transitions when delayed negative feedbacks leading to oscillatory or other complex dynamics are weak²⁵.

RELATIONSHIPS ARE NON-LINEAR

In practical terms, this means a small perturbation may cause a large effect (see butterfly effect²⁶), a proportional effect, or even no effect at all. In linear systems, the effect is always directly proportional to cause.

Randall’s work illustrates a small sample of the variety of solutions available for what comprises complex systems. As noted earlier, this research proposes that ransomware is successful due to a non-systems approach to solving the cybersecurity issues in IT, and subsequently OT. This is not a slight against any IT or OT practitioner, but instead is a new idea for stopping the catastrophically disruptive effects of ransomware in organizations.

A COMPLEX SYSTEMS SOLUTION FOR A COMPLEX PROBLEM IN SIMPLE TERMS

At its core, complex systems analysis considers how systems with many components (abstract or real) interact with other systems and their components. These systems are difficult to model due to dependencies, competitions, relationships, or other types of interactions between the parts of the whole or the whole itself, or with their environments.

The complexity for this research breaks down into four categories: IT, OT, Access Control, and Auditing. Currents in social media and commentary point continuously to “best practices” with little or no explanation provided that covers the greater issues of how the systems interact. This should be the starting point for any conversation regarding, “how protected are we against ransomware?” The complexity of these systems and how they interact is at the core of solving the ransomware problem. According to Ross (2015), Optimal Control Theory is a branch of mathematical optimization that deals with finding a control for a dynamical system over a period of time such that an objective function is optimized²⁷.

Optimization problems consider the best operating state for many different systems of problems. According to Ferguson (1998) and Leonard & Long (1992), the goal of Optimal Control Theory is to find some sequence of controls (within an admissible set) to achieve an optimal path for the state variables²⁸. Arguably, this includes the interactions between IT, OT, and the various components that comprise those systems. The various

states of security on any of those devices taken wholly or separately make securing them a dynamical system. The objective function is a mathematical equation that describes the production output target that corresponds to the maximization of profits with respect to production. It uses the correlation of variables to determine the value of the final outcome. Taking a step back and putting this into practical terms, it is necessary to define some functions.

METHODOLOGY FOR THE RISK ASSESSMENT TOOL

Security: $F(S)=[(s(IT) s(OT) s(AC) s(AU))]$

The functions of the security of IT, OT, Access Control, and Auditing comprise the $F(S)$, the function, of security. It is very unlikely that any $[s(X)]$ will be a zero value, as most organizations have addressed in some way the myriad of security issues that comprise these functions. Now consider that time and initial states affect these values.

To simplify this, $F(S)$ changes over time for better or for worse, depending on the outcomes of the comprising functions. The function of overall security, $F(S)$, relies upon the state conditions of all the other sub-functions: $s(IT)$, $s(OT)$, $s(AC)$, and $s(A)$. In a perfectly optimized system, all functions would keep a steady state (secured) creating an overall secured infrastructure. A steady state is a continuous value between zero and one, closer to one, based on the design of this formula. States closer to zero represent less secure environments. As with other complex systems, even small changes to any of the defined functions will perturb (negatively or positively) on the overall security of the system²⁹.

$s(IT)$:

The sum of actions taken in this category. Up-to-date patch and vulnerability management for all connected components. Each component in the IT infrastructure will have its own set of security controls that comprise the $s(IT)$. Some of these may include database security controls, web server security controls, host-based operating system security controls, network security controls, storage system security controls, etc.

$s(OT)$:

The sum of actions taken in this category. Up-to-date patch and vulnerability management with all devices comprising the OT infrastructure; secured protocols, segmentation between functional or protocol-based boundaries in the OT environment; secured connections between facilities and/or IT infrastructures. Usage of security enclave establishment where possible. Secured connections between OT infrastructure and IT infrastructure.

$s(AC)$:

The sum of implementations in this category. While access control may seem a part of IT, writ large, it poses a special problem in securing systems against ransomware. Secure remote access paradigms to include multi-factor authentication between users and their remote access environments. Behavioral metrics collection against insider threats (this is part of a larger issue, addressed in another research project).

$s(AU)$:

The sum of actions taken in this category. Auditing IT logs can prevent ransomware. With the obvious exception of the case where ransomware adversaries use new Zero Days, anomalies caused by most initial access vectors can be detected early in the ransomware attack cycle. While many organizations invest time, effort, and training into intrusion detection or prevention systems, ransomware adversaries often use blended approaches that effect simultaneously different parts of IT infrastruc-

ture. For this function, it is not just IT logs, but database logs, firewall logs, continuous netflow monitoring, and proactive hunting for anomalies across these systems that will serve organizations well at optimizing ransomware protection strategies.

GENERALIZED FORMULA FOR EACH FUNCTION

$$s(X) = x1+x2+x3...xn / n$$

Each variable $x1+x2+x3...xn$ represents a measure taken to improve the organization's cyber defense posture. There can be any number of such measures, and a measure can mean a patch, a configuration, a detection or any method taken to secure an infrastructure.

This way the product of the functions will be a value between zero and one, with one being a completely optimized environment. This optimization will be nearly impossible to achieve but is a quantifiable goal. Identifying the security changes will be the most time intensive aspect of this process.

OPTIMIZATION IN THE SYSTEM

Using some simplified differential calculus, and complex systems analysis it is possible to prove mathematically that any loss of security in an IT environment that is in any way connected to an OT environment will cause an overall loss of security for both systems of systems. Furthermore, depending on the type of exposures created by one system, the risk can dramatically increase, thus lowering the value function of the system of systems. The value function here can be the cost-benefit analysis of the decision calculus behind making decisions, drafting policies, etc. that frame the overall security function of the organization $[F(S)]$. The analogy to the mathematical equation underpinning this risk assessment tool, because in mathematics is solved backward in time – starting from $t=T$ (present time, or the time the operator discovers the ransomware) and ending at $t=0$ (time when the ransomware actually silently attacked the systems). Practically speaking, this refers to the time between the actual ransomware compromise and the time at which the owner/operator discovers the compromise. There is anecdotal evidence that shows ransomware adversaries take careful steps and time to gain a foothold in, and move laterally across, systems. Time is differentiable in terms of degree of infection or success of the ransom.

FURTHER THOUGHTS ON THIS APPROACH

Best practices, intrusion detection systems, Security Information and Event Management (SIEM) tools, and spending money on cybersecurity are enough to prevent ransomware adversaries from succeeding. A new approach is therefore necessary. This is not a holistic approach either, but mostly because holistic is not well-defined (more or less as best practices are not well-defined). The difference in using math is in the formality of the approach. This approach assumes that the four composed functions for the $F(S)$ are going to have different variables, and that those variables will change over time. Such systems are deemed “stochastic,” and solving stochastic systems (like the weather for example) is not easy. This mathematical approach to solving the ransomware problem does not presume to be complete or the “silver bullet,” but aims to describe a security system using complex systems analysis

as the foundation. It endeavors to create a more comprehensive understanding of the variables, their interconnectedness, and a potential approach for multiplicatively solving the problem. It is necessary to multiply the functions because the role of zero plays an important part in understanding how systems can fail. Zero in this instance means a function value that has no value and thus no components, or practically speaking, implementation. The sum of the various parts of each function are multiplied to make a comprehensive risk assessment, which is dynamic and adaptive.

To keep the functions simple, each function will have n implementations and each implementation will have a value of zero, meaning not implemented or one meaning implemented. Gradations of the scale (.25, .5, .75) are owner operator determined.

SIMULATED EXAMPLES

At some level, some of these math machinations will be arbitrary, and thus subject to human designed error. Here are a few examples.

Given: $F(S)=[(s(IT) s(OT) s(AC) s(AU))]$

$F(S)$ = Some arbitrary evaluation of the various aspects of the Security of IT, the Security of OT, the Security of Access Control and the depth of Auditing. Assume that an overconfident assessment of these values would yield the following:

EXAMPLE 1 – *prepared for ransomware*

$F(S) = .99*.99*.99*.99$

$F(S) = .961$

with each function composition looking like this:

- $5.94 (.99+.99+.99+.99+.99+.99)/6$
(6 is an arbitrary number of measured security implementations, or in this example that which the owner/operators have stated are 99% completed/ implemented / installed, etc.
- The owner operator used 6 measures for each of the values of $s(IT)$, $s(OT)$, $s(AC)$ and $s(AU)$, and ranked each 6 items as being 99% completed / implemented / installed, etc.

$F(S)$ here would be .961, so the steady state as noted above would be a straight continuous line at .961. Any perturbation (breach, p0wnage, etc. would make this drop significantly, thus affecting the overall quality of the security implementation). It would appear as a horizontal line with a notable drop.

EXAMPLE 2 – *not prepared for ransomware*

$F(S) = .99*.50*.50 *.07$

$F(S) = .02$

This is more difficult. Assume there are still six security measures used. It is easy to derive .99, and even .50. However, deriving .09 yields a more complicated assessment of security measures and would look like: $(.10+.10+.10+.10+.005+.005)/6$. The important thing to note about this “unprepared security administrator” model is that it is likely more representative of what would be found in an organization. Keep in mind that the composition of the four main functions can vary over time, so this will be a continuum of values and measures.

SIMULATED “ORDINARY” ENVIRONMENT – *not prepared for ransomware*

This example provides a more detailed approach to the function composition.

Remember:

$F(S)=[(s(IT) s(OT) s(AC) s(AU))]$ (and for the sake of consistency, we will use six measured values)

$(s(IT)) = (.80+.50+.30+.50+.50+.10)/6 = .45$

$(s(OT)) = (.75+.50+.50+1.0+.25+.25)/6 = .54$

$(s(AC)) = (1.0+.10+.10+.50+.75+.80)/6 = .54$

$(s(AU)) = (.8+.8+.1+.5+.5+.5)/6 = .53$

Thus, the value of $F(S)=[(s(IT) s(OT) s(AC) s(AU))]$ will be:

$F(S) = .45*.54*.54*.53$
= .07

HOW TO ASSESS RISK ASSESSMENT VALUES OF SECURITY IMPLEMENTATIONS

It is necessary to ask the simple question: How to assess “a security implementation” at .99, or .5? So, here are some thoughts on that:

1. Consider that if nothing is done, the value is zero.
2. If a SIEM solution is part of $(s(AC))$, and it catches 75 percent of the attacks, a variable can be assessed as one of the n values for $(s(AC))$, with the value of .75. Perhaps there is a firewall, a network appliance (e.g.: Dragos Neighborhood Keeper Endpoint), an Access Control List (ACL) on the internal router, and an IPS running as part of the $(s(AC))$, and it is assessed that everything except the firewall is 80 percent effective at detecting ransomware entry tools. The firewall will be deemed zero percent effective in this ransomware paradigm. The ACL will also be deemed zero percent effective. That is a total of five things.
3. In this instance the $(s(AC))$ would be composed this way: $.75+.80+.80+0+0/5 = .47$ as the value of this function.

Back to the last simulation. In reality, most security administrators may not consider these values to be “quantifiable” per se, and may just assess them as zero or one. This is fine too as the outcome will be a steady state somewhere near .5.

CONCLUSION

The results of the simulated environments may be startling to owner-operators. Even in relatively well-secured environments, the complex systems analysis of the environments yields very low numbers. This research has not yet assessed what is an “acceptable value” for ransomware exposure. This research provides a generalized, quantifiable formula based on pre-existing mathematical theories, and attempts to provide users with a way forward to better secure and quantify the security, and ultimately (hopefully) prevent ransomware attacks.

This is by no means a fail-safe measurement tool for “absolute security,” and generally speaking, absolute security is unattainable in the majority of contexts. This mathematical approach puts a heavy weight on the value and necessity of measuring the usefulness (or even existence) of assets that perform security functions in a given environment. Understanding asset management and the security posture of each asset taken separately or as a whole is the strength of this approach.

FURTHER RESEARCH

It is very clear that more work is likely needed in the measuring of security implementation artifacts, and also perhaps tweaking of the formula used to determine “overall security.” Further research will have to explore these issues. Furthermore, this research can be applied to different malware or attack domains beyond ransomware. Owner-operators will have to trial and error some of the approaches with measuring the variables described herein, and may benefit from establishing thresholds of “critical low values” or critical F(S) values. This may be industry and or organization specific.

REFERENCES

- 1 [The State of Ransomware 2021](#) – Sophos
- 2 [Ransomware on the Rise in Critical Infrastructure Sector](#) – King & Spalding
- 3 [TR-2021-10: Manufacturing Sector Ransomware Insights June-July](#) – Dragos
- 4 [Ransomware on the Rise in Critical Infrastructure Sector](#) – King & Spalding
- 5 Op. cit. - Sophos
- 6 Rogers, R. W. (1975). [A protection motivation theory of fear appeals and attitude Change](#), Journal of Psychology, 91(1), 93–114. 3
- 7 [Dang-Pham & Pittayachawan, 2015; Hanus & Wu, 2016; Herath & Rao, 2009; Jansen, Veenstra, Zuurveen, & Stol, 2016; Meso, Ding, & Xu, 2013; Safa et al., 2015; Shillair et al., 2015; Sommestad T, Karlz H, Hallberg J. A meta-analysis of studies on protection motivation theory and information security behaviour. Int J Inf Sec Priv. 2015; 9\(1\):26–46.doi:10.4018/IJISP.2015010102, Vance, Siponen, & Pahlila, 2012\)](#)
- 8 Marijn Martens, Ralf De Wolf, Lieven De Marez [Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general](#), Computers in Human Behavior, Volume 92, 2019, Pages 139-150
- 9 [Assessing Ransomware and Extortion Activities Impacting Industrial Organizations](#) – Dragos
- 10 Ibid.
- 11 [The Basics of Game Theory](#) – Investopedia p
- 12 Bar-Yam, Yaneer (2002). [“General Features of Complex Systems”](#) (PDF). Encyclopedia of Life Support Systems. Retrieved 16 September 2014.
- 13 [A review of common characteristics of complex systems](#) – Future Learn 6
- 14 [Recommendations Following the Oldsmar Water Treatment Facility Cyber Attack](#) – Dragos
- 15 Ibid.
- 16 [When Intrusions Don’t Align: A New Water Watering Hole and Oldsmar](#) - Dragos
- 17 Op. cit. - Future Lean
- 18 [Alan Randall \(2011\). Risk and Precaution.](#) Cambridge University Press. ISBN 9781139494793.
- 19 S. V. Buldyrev; R. Parshani; G. Paul; H. E. Stanley; S. Havlin (2010). [“Catastrophic cascade of failures in interdependent networks”](#). Nature. 464 (7291): 1025–8. arXiv: 0907.1182. Bibcode:2010 Natur. 464.1025B. doi:10.1038/nature08932. PMID 20393559. S2CID 1836955.
- 20 Berezin, Yehiel; Bashan, Amir; Danziger, Michael M.; Li, Daqing; Havlin, Shlomo (2015). [“Localized attacks on spatially embedded networks with dependencies”](#). Scientific Reports. 5(1): 8934. Bibcode:2015NatSR...5E8934B. doi:10.1038/srep08934. ISSN 2045-2322. PMC 4355725. PMID 25757572.
- 21 Scheffer, Marten; Carpenter, Steve; Foley, Jonathan A.; Folke, Carl; Walker, Brian (October 2001). [“Catastrophic shifts in ecosystems”](#). Nature. 413 (6856): 591–596. Bibcode:2001Natur. 413..591S. doi:10.1038/35098000.
- 22 Scheffer, Marten (26 July 2009). [Critical transitions in nature and society](#). Princeton University Press. ISBN 978-0691122045.
- 23 Scheffer, Marten; Bascompte, Jordi; Brock, William

REFERENCES

- A.; Brovkin, Victor; Carpenter, Stephen R.; Dakos, Vasilis; Held, Hermann; van Nes, Egbert H.; Rietkerk, Max; Sugihara, George (September 2009). “**Early-warning signals for critical transitions**”. *Nature*. 461 (7260): 53–59. **Bibcode:2009Natur.461...53S**. **doi:10.1038/nature08227**.
- 24 Scheffer, Marten; Carpenter, Stephen R.; Lenton, Timothy M.; Bascompte, Jordi; Brock, William; Dakos, Vasilis; Koppel, Johan van de; Leemput, Ingrid A. van de; Levin, Simon A.; Nes, Egbert H. van; Pascual, Mercedes; Vandermeer, John (19 October 2012). “**Anticipating Critical Transitions**”. *Science*. 338 (6105): 344–348. **Bibcode:2012Sci...338..344S**. **doi:10.1126/science.1225244**. **hdl:11370/92048055-b183-4f26-9aea-e98caa7473ce**. **ISSN 0036-8075**. **PMID 23087241**. **S2CID 4005516**. Archived from the original on 24 June 2020. Retrieved 10 June 2020.
- 25 Lever, J. Jelle; Leemput, Ingrid A.; Weinans, Els; Quax, Rick; Dakos, Vasilis; Nes, Egbert H.; Bascompte, Jordi; Scheffer, Marten (2020). “**Foreseeing the future of mutualistic communities beyond collapse**”. *Ecology Letters*. 23 (1): 2–15. **doi:10.1111/ele.13401**. **PMC 6916369**. **PMID 31707763**.
- 26 <https://www.merriam-webster.com/dictionary/butterfly%20effect>
- 27 Ross, Isaac (2015). *A primer on Pontryagin's principle in optimal control*. San Francisco: Collegiate Publishers. ISBN-13: 978-0984357116, ISBN-10: 0984357114
- 28 Ferguson, Brian S.; Lim, G. C. (1998). *Introduction to Dynamic Economic Problems*. Manchester: Manchester University Press. p. 162. **ISBN 0-7190-4996-2**. Léonard, Daniel; Long, Ngo Van (1992). **Optimal Control Theory and Static Optimization in Economics**. New York: Cambridge University Press. p. 181. **ISBN 0-521-33158-7**
- 29 Léonard, Daniel; Long, Ngo Van (1992). **Optimal Control Theory and Static Optimization in Economics**. New York: Cambridge University Press. p. 181. **ISBN 0-521-33158-7**

ABOUT DRAGOS, INC.

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats and vulnerabilities are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries, including power and water utilities, energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIoT).

TO LEARN MORE ABOUT DRAGOS AND OUR TECHNOLOGY, SERVICES, AND THREAT INTELLIGENCE FOR THE INDUSTRIAL COMMUNITY, PLEASE VISIT www.dragos.com.

THANK YOU