Protect Your ICS Environment from Ransomware with Risk Assessments

Dr. Thomas G. Winston
Director of Intelligence Content
Dragos, Inc.

Webinar 17 November 2021, 1300 ET (US)

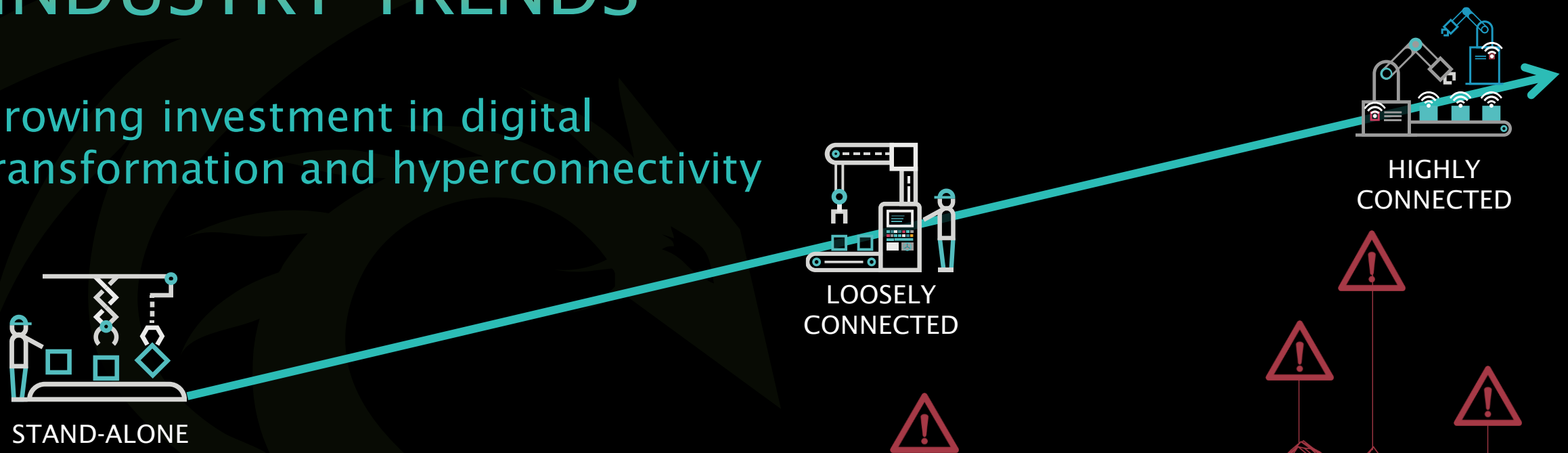
Agenda

- Ransomware trends and their impact on ICS
- The emergence and disappearance of ransomware adversaries
- A risk assessment metric to prevent ransomware
- The role of classic math and complex systems theory

Ransomware Trends and their impact on ICS

INDUSTRY TRENDS

Growing investment in digital transformation and hyperconnectivity

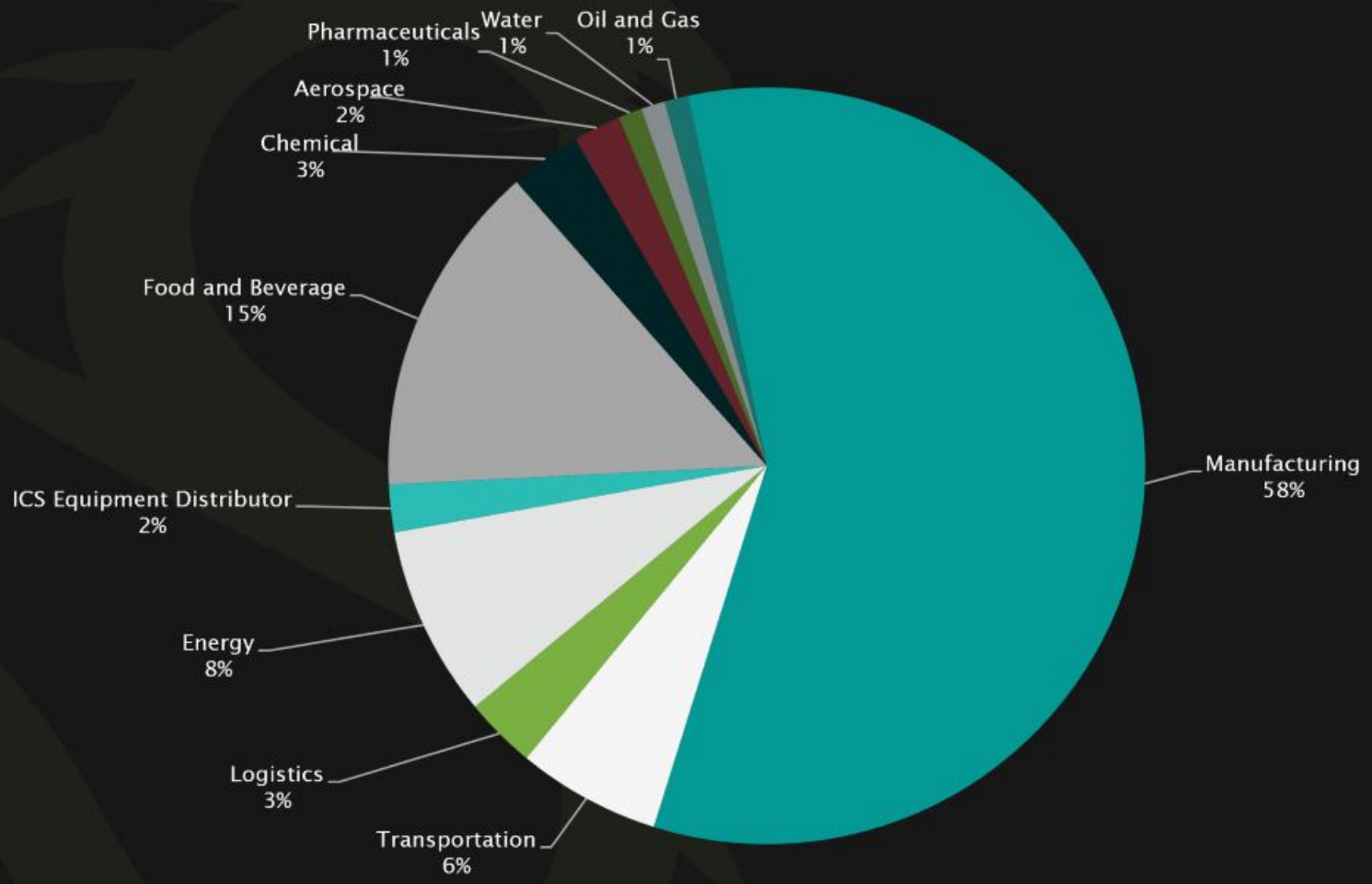


Greater exposure to malicious cyberthreats

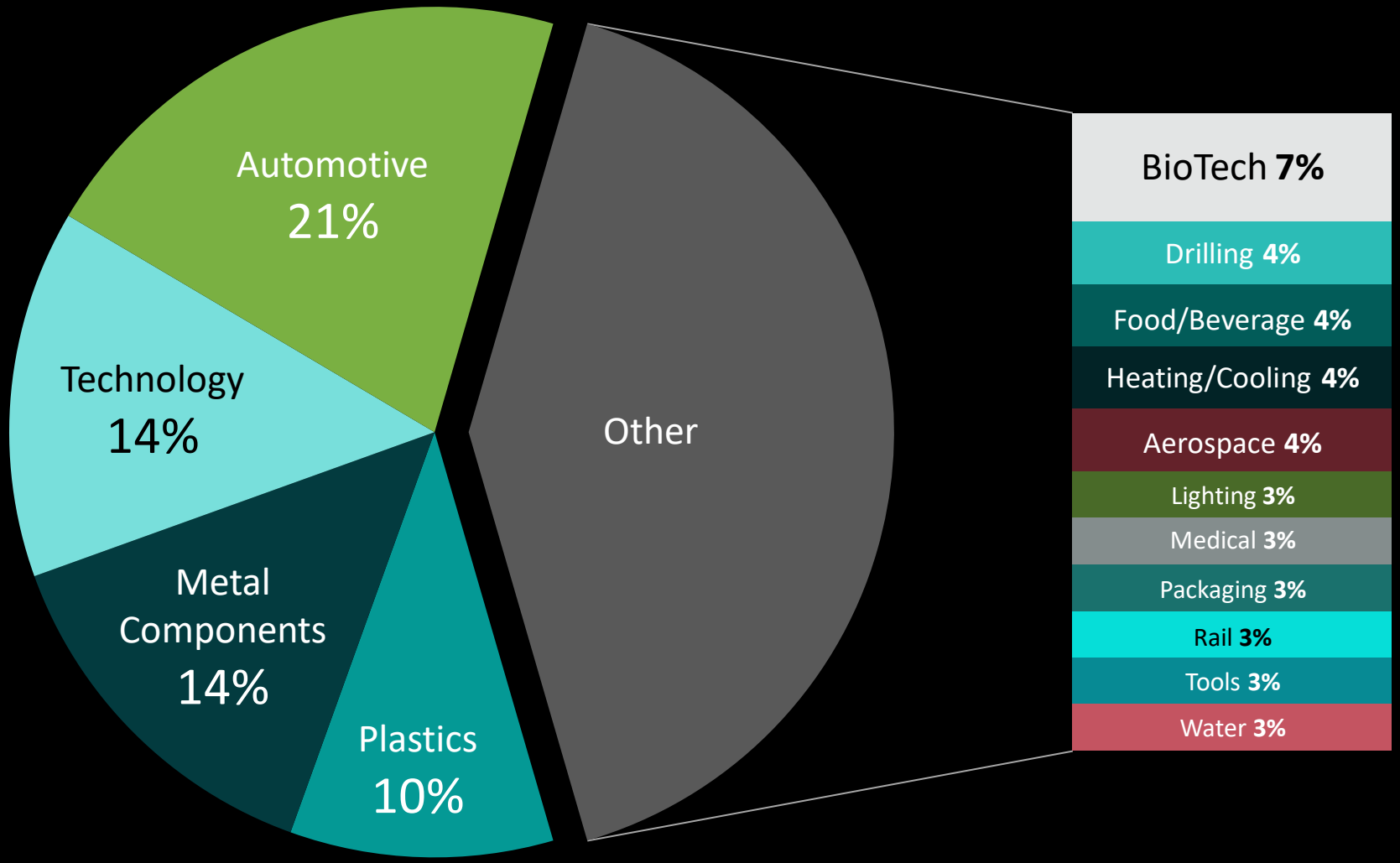
"Threat groups are rising 3X faster than they're declining…"
Source: Dragos 2020 YiR

ICS Ransomware by Country

ICS Ransomware by ICS Vertical



Ransomware Attacks Against Manufacturing Firms

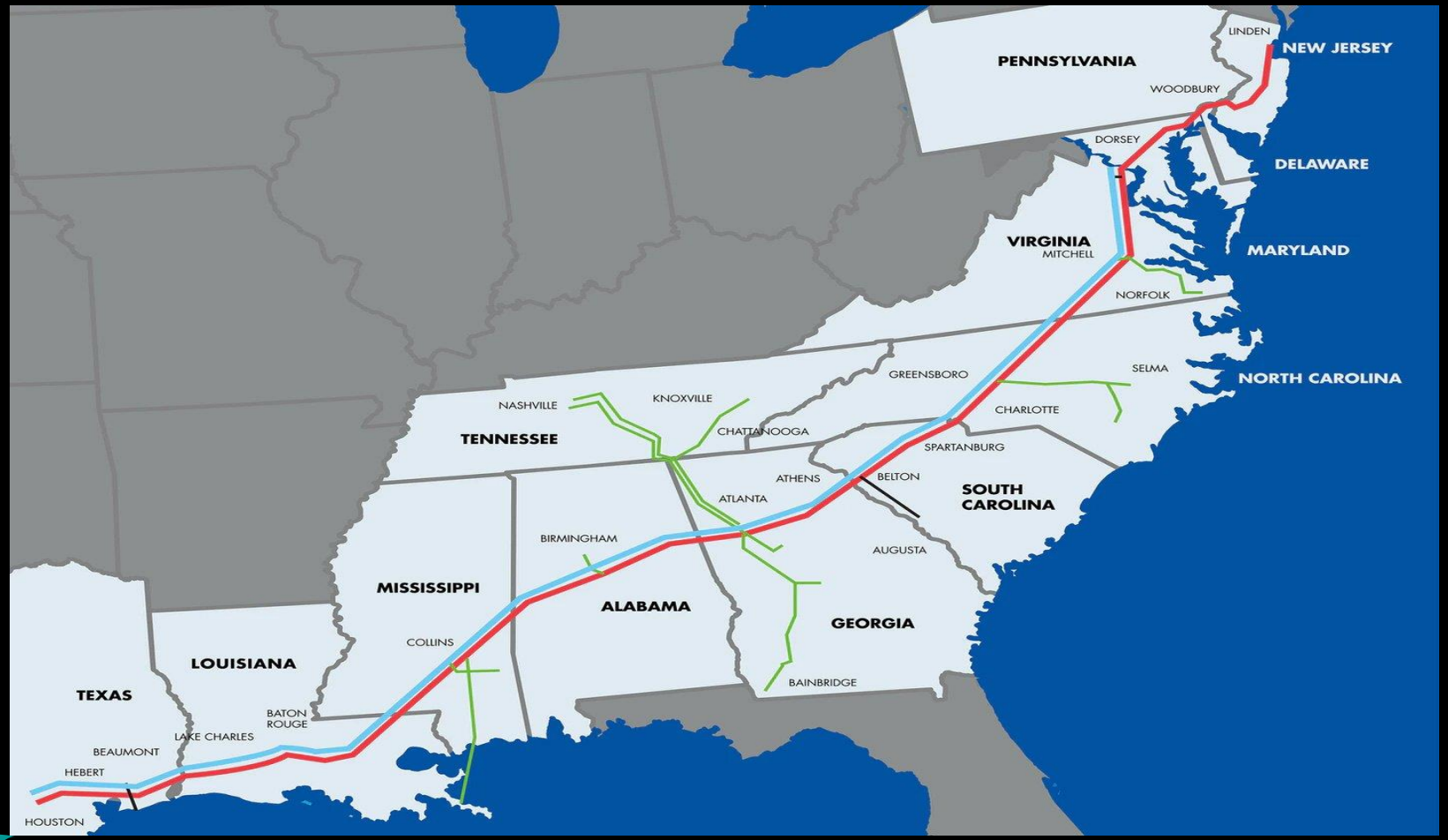


Ransomware – JBS Foods

- JBS Foods is the largest meat processing company in the world
- May 30 - the day of the ransomware attack.
- Discovered chunks of data uploaded to the 'Mega' file sharing service from JBS dating back to March 4th
  - Uploads continued sporadically, ~40-60GB of data uploaded
- While this may have been the work of a JBS employee, Dragos assesses with high confidence the activity can be attributed to these ransomware actors, as Mega has been used to store information by ransomware actors in at least three other exfiltration campaigns

Assessment: Dragos assesses with moderate confidence ransomware groups will continue slow exfiltration of data, possibly to avoid activating security controls, in the months and weeks leading up to a ransomware extortion event.

Colonial Pipeline Ransomware Example



The emergence and disappearance of ransomware adversaries

ICS OEM Nexus

- The infamous REvil ransomware group has reportedly been dealt a severe blow, courtesy of an operation conducted by officials in the US and other countries.
- Law enforcement and intelligence cyber specialists hacked into REvil's computer network infrastructure, thereby taking control of at least some of the group's servers, according to information from three private sector cyber experts working with the US, as well as one former official.

Ransomware Groups Return

- Ransomware groups are in some instances very well-funded by nation-states, and can therefore hide for a period of time, and then re-emerge with slightly modified TTPs.

Ransomware Risk Assessments

Ransomware Risk Assessments

- Prey upon WFH arrangements, and weak access controls through IT/OT integrated systems
- Proposal to assess risk using an algorithm
  - No Risk Assessment tool is perfect
  - Risk assessment cannot be blind to any system interaction
  - This risk assessment tool considers each of several organizational security functions, and using a qualitative approach calculates estimate of risk per function.
  - Each of the functional risks are then multiplied to get an overall “risk exposure” to malware

Malware Risk Assessments

- Rooted in complex systems analysis and differential calculus, but easy to use and implement.
  - Primary consideration here is using each system of systems as a multiplier to risk.
  - Security: F(S)=[(s(IT) s(OT) s(AC) s(AU))] – or the functions of the security of IT, OT, Access Control, and Auditing – comprise the F(S), or the function, of security.

Role of Mathematics in Risk Assessment

Math Plays a Role here

- According to Kirk (1970) in Optimal Control Theory, the Hamilton–Jacobi–Bellman (HJB) equation gives a necessary and sufficient condition for optimality of a control with respect to a loss function.
- It is, in general, a nonlinear partial differential equation in the value function, which means its solution *is* the value function itself.
  - Stated differently, the loss function recognized in ICS environments is not only affected by the IT environment, but by the product of the functions of the whole of all the systems both enterprise IT and Operational Technology - interconnected.
- 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 HJB equation fits, because in mathematics, the HJB equation is usually solved backward in time – starting from $t=T$ and ending at $t=0$.
  - Practically speaking, this refers to the time between the actual ransomware compromise and the time discovered. 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.
-

Formula

- **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.

Formula

- **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 have used blended approaches that effect simultaneously different parts of IT infrastructure. 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.

The Formula, Further Explained

- **Generalized Formula for Each Function**

- $s(X) = x_1+x_2+x_3...x_n / n$
- Each variable $x_1+x_2+x_3...x_n$ 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.

In Practice…Unprepared

"Remember closer to 1 means more prepared"

- *Example (not prepared for ransomware)*

- F(S) = .99*.50*.50 *.07 (s(IT, OT, AC)) are half prepared, and s(AU)is in really bad shape!!
- F(S) = .02 (the product of the composed functions is not good!!)
- 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 the 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)*

In Practice…Prepared

"Remember closer to 1 means more prepared"

- *Example (prepared for ransomware)*
-
- F(S) = .99*.99*.99*.99
  F(S) = .961
- with each function composition looking like this: (so all functions are well prepared!!)
-
  - 5.94 (.99+.99+.99+.99+.99+.99)/6 (6 is an arbitrary number of measured security implementations)
-
- 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).

Summary Recommendations

- ACCESS RESTRICTIONS and ACCOUNT MANAGEMENT
  - Restrict administrative access within a domain, limit the number of domain administrators, and separate networking, server, workstation, and database administrators into separate Organizational Units (OUs)
- RESPONSE PLANS
  - Develop, review, and practice cyberattack response plans and integrate cyber investigations into root-cause analysis for all events specific to OT
- THIRD-PARTIES
  - Ensure that third-party connections and OT interactions are monitored and logged, from a “trust, but verify” mindset
- VISIBILITY
  - Take a comprehensive approach for visibility and threat detection into OT environments to ensure that there is no gap in monitoring

Thank you!

Questions?