Cyber Immunity, a holistic view for Industrial Control Systems

Many enterprise environments see protection of critical data as their top priority, and to achieve that they employ multiple IT/IS personnel. However, the common practice of protection of critical data is often not translated over to establishing the security of Operational Technology (OT) environments. What is Operational Technology? It is software or hardware that controls processes, physical devices, and events in an enterprise, and ultimately is altering the state of a system; such system can include access control, process control, surveillance, voice technologies, etc. OT is categorically or used interchangeably as a part of or as an Industrial Control System (ICS).

In mission critical infrastructures ICS such as power grids, mass transit transportation systems (e.g. airports, bus terminals, roadways, or train stations), waste water facilities, nuclear power plants, the emphasis should not be only on security for the IT assets but also for the often-overlooked OT assets. Let's take for an example a power utility company which has implemented enterprise systems and has its IT department devoted to protecting these systems. On the flipside, the company has field assets—transmission and distribution stations which generate and distribute power to the consumers, and these assets are essentially the main driver of revenue stream and the life blood for that company.

Having spoken with many customers, some are surprisingly unaware of the threats faced by their OT systems, and such companies often believe that closed systems not connected to the public WAN are safe from threats. In reality, this is simply not the case; those systems are highly vulnerable, and being exposed to a cyber-attack after functioning long term without the capabilities of early detection or containment, they can suffer detrimental and crippling consequences in the aftermath of a cyber-attack. While it's safe to say that anyone or everyone is a hacker whether malicious or unintentional, let's focus on the internal threats to the OT systems. For example, all employees in the power utility company from the example have USB flash drives and smart phones, and they use their flash drives for data transfer or charge their phones within the corporate network. For simplification, let's classify such employee who has access to the OT environment as a "Trusted host". A Trusted host decides to plug in his/her USB drive or charge his/her smart phone. If the device has a virus ("Sick device"), a potential threat will be introduced to the company's otherwise classified closed system. Therefore, protection from the "good guys" is also critical. So how is your organization protected against these types of threats even though it's a closed system?

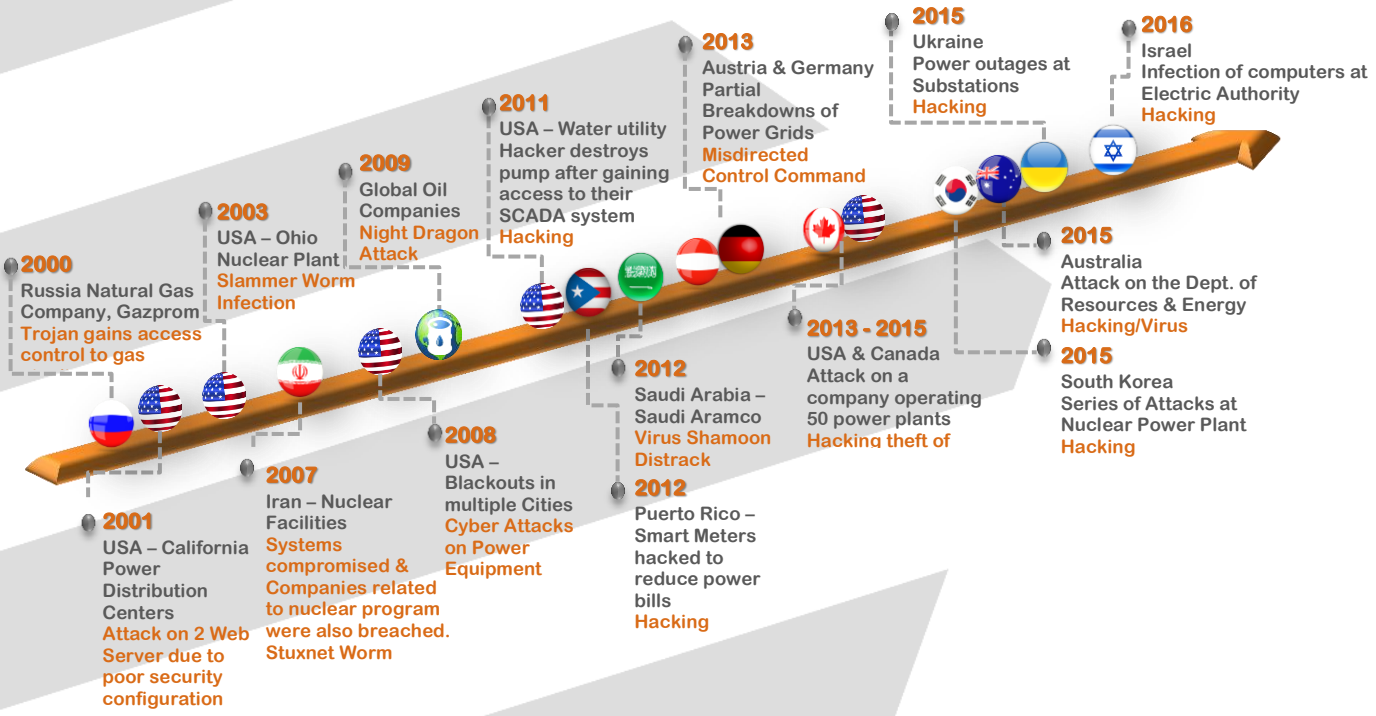
Historically and still in the present day, OT networks are legacy systems that were primarily isolated specialized systems using proprietary hardware and software. As such, they were not connected to the company's enterprise networks and run independently, thus resulting in "air gaps" between the IT network and the OT network. Air gaps occur when one network such as IT will have security measures that segment the IT environment from their unsecured OT counterpart. Good news is that with the advancements in

technology, OT networks are moving towards a more converged network environment and more efficient control of data transportation, storage, data analytics, and monitoring processes. However, now as a part of the converged network environment, OT networks users and administrators must put serious consideration to the cyber threat landscape. Even governments recognized the need for cyber protection and have legislated Critical Infrastructure Projects (CIP) to implement threat measures for protection of critical systems. For the purpose of this article, let's focus on the OT environments and how to adapt resilience from digital assaults.

When it comes to cyber resilience, the rise of cyber threats against ICS globally should always be on the top of the CEO's "To do" list. OT networks have a different set of protocols from an IT environment. Availability or access to assets of a nuclear plant or power substation are top priority for an OT network, versus an IT approach that prioritizes confidentiality as their number one concern. OT environments must have constant communications between devices monitoring or controlling critical functions. For example, critical assets in a nuclear plant that monitor thermal sensors could potentially avoid overheating and causing an explosion. Blocking of any virtual traffic due to security requirements to these critical assets may have severe consequences for the OT environment. Simply put, blocking traffic in the IT world (e.g. in a bank) may cause the bank to lose some transactions; as a result, the bank can shut down that part of the system for containment and quarantine, but this will be by no means life threatening. However, in the OT environment, blocking traffic can potentially lead to a death to of an employee or other people if the non-communicating device is responsible for process control and monitoring of a critical function such as cooling of a reactor at a nuclear plant. But even with accessibility as a top priority for OT networks, we can't conclude that OT networks should not be protected or can't be protected from cyber threats. Adversely, it is these types of systems that should be highly secure since they provide service with significant and immediate impacts to human lives that extend beyond the company's human resources.

Ongoing activities of hackers continue to threaten mission critical systems as they see vulnerabilities in industrial networks worldwide. Once hackers have infiltrated your corporate environment, they can traverse through other unsecured networks within the OT environments, target vulnerabilities, and propagate within the company. These types of threats have essentially become the new warfare in the present world whether by solitary hackers or state sponsored. The diagram below shows some case scenarios of cyber-attacks on ICS applications and its onward trend.

History of Cyber Attacks Globally in ICS (Industrial Control Systems) [1] [2]



When considering protecting your data you need to look at a "Defense in Depth" which is a multi-tiered or layered approach. There is no "out of the box security" that can provide a singular solution to stop Cyber threats in today's world, Security is not an isolated process but an ongoing process hence why a Layered approach is needed to constantly protect your critical data. Using best practices an Organization could limit future attacks, essentially creating an ecosystem to ensure Cyber Immunity with a holistic view. It is the sum of all parts working together to ensure optimum performance. Technology, while playing a vital part, alone will not prevent cyber threats in today's modern world. Rather, the principals surrounding Cyber Immunity should be developed and balanced around the fundamental pillars – People, Process & Technology. Security for your organization should

always be transformational to keep up with the latest threats and adjust to those threats within the pillars.

- **People**, within the organization, need to be made aware to the sensitivity of data, therefore Training staff about the potential threats and how to secure the data is essential, staff should always be updated whether in qualifications and skills to ensure competency to mitigate risks.
- **Process** will be important for effective execution of strategies. It will help to define how the organization will react and behave to ensure they follow documented protocol for data protection.
- **Technology** is crucial for putting in controls to stop and mitigate threats as well as logging and tracking user's activities.

When you consider drawing parallels to how the human body works, people also get viruses, and often relying solely on a body's defense mechanisms and healing power may not be enough. A proper nutrition plan along with adequate rest helps with the healing process, but at the end, a medication may be needed to start or bring to speed recovery. Generally, practicing good health, diet, exercising, and proper rest daily could mitigate potential sickness down the road, improve immunity, and make a person more resilient to sickness. In parallel, this holistic approach to wellness and health is not different from an organization's method of protection of their data and ensuring cyber resilience. So, to recap, if everyone in the organization implements and practices a cyber resilient lifestyle, then the organization would have a better chance of preventing future sickness of their data. However, having said this, it doesn't guarantee an absolute secure environment as the company operates into the digital landscape. Cyber threats have evolved in how to infiltrate or compromise systems, and as a result, organizations should continually strive to evolve and adapt their immunity to potential cyber threats as new strains of viruses, malware, or hacking techniques are introduced to this landscape. With this, adding layers of security is a much more effective approach than relying solely on a single mechanism for data protection. All the defense layers should work in unison to be effective and be validated throughout its lifecycle. So what would those layers encompass?

Let's start peeling the layers of the onion (aka the company's approach for cyber resiliency). As per the author of this article, the most important layers on which a company needs to focus are as follows:

- **Full visibility, understanding, and up-to-date recordkeeping** of current inventory or what's connecting or connected to the company's network, servers, databases, mobile devices, PLC's, Relays IED's, IIOT devices or simply discovery of all company's assets

- **Risk Assessment**—after taking inventory of all assets connected to the company's network, they must be evaluated, and those needed protection determined. Next, threats are to be analyzed, risks identified and assessed, and tolerances to those risks

determined. After that, current network architecture must be evaluated, and the need to make the network more secure when corresponding to the needs of the OT application determined.

- **Penetration test** on the company's current networks and establishing vulnerabilities and gaps. Conducting a penetration test is crucial for preventing data breaches and verifying effectiveness of the implemented security controls. For example, if a company performs a "brute force" attack as part of the penetration test, efficiency of passwords will be tested, and enforcing of a use of a combination of letters, numbers and symbols with a minimum 8 characters will be included into the organization's security compliancy procedures.

- **Incident Response**—have you ever tested how well does your organization respond to a cyber threat and manage its aftermath? The goal is to ultimately prevent data breaches of the organization's network but when the network has been breached, the organization needs to be able to contain the breach preventing it from further spreading into other areas of the network and ultimately taking down important process controls. An organizational emergency containment and recovery plan is a must for every organization and a crucial measure for mitigating outages and disruption in service to customers.

  As per the Escal Institute of Advanced Technologies (SANS Institute), a private U.S. for-profit company that specializes in information security and cybersecurity training, the six key phases of an incident response plan are:

  1. Preparation—preparing users and IT Staff to handle potential incidents should they arise
  2. Identification—determining whether and if, indeed, the breach is a security incident
  3. Containment—limiting the damage of the incident and isolating affected systems to prevent further damage
  4. Eradication—finding root causes for the incident and removing affected systems from the production environment
  5. Recovery—permitting affected systems back into the production environment while avoiding remaining threats
  6. Lessons learned—completing incident documentation, performing analysis to learn from the incident and potentially improve future response efforts

- **Disaster Recovery—**an organization should be well prepared when situations arise. Proper procedures must be in place to prepare, react, and recover from a disaster. Roles and responsibilities within the organization have to be clearly defined and

communicated. The company should always have backup of their data in case of failures, and as per the best industry practices, the backup should be kept at a remote site, often referred to as a disaster recovery (DR) site. Once in a while, fire drills have to be conducted to test the effectiveness of the DR plan and modify risk tolerances accordingly while ensuring business continuity.

- **Governance**—compliancy within the organization typically surrounds policies, procedures, and training for employees. There should be compliance controls in place so that employees are following the established organizational policies for data protection. Some compliance often is mandated by local or national authorities and regulations, and compliance with these authorities and regulations must be incorporated in the organizational compliance policies.

In retrospect, we speak of fundamental principles that encompass a holistic view to what organizations need to consider when looking at shaping for cyber resilience in their ICS application. The company's journey to cyber security should never stop at one singular aspect but employ an overall continuity of many moving parts. Of course, even while implementing a total security solution, nothing is absolute. Perpetual transformation, harmonizing, and understanding of the needs of a converged network from both IT and OT peers while securing the environmental needs to be top priority. Constant vigilance, review of new and potential threats, and ongoing transformation of the organization in adapting to the ongoing threat landscape is paramount to the success of any company.

References:

[1] Payal Bhattar "Power-up the security blanket. Internet: https://www.wartsila.com/twentyfour7/innovation/power-up-the-security-blanket, June 27, 2017 [Nov 21, 2017]

[2] Shawn Wasserman "Infographic: History of IIoT Cyber-Attacks and How to Avoid Them. Internet: https://www.engineering.com/IOT/ArticleID/13353/Infographic-History-of-IIoT-Cyber-Attacks-and-How-to-Avoid-Them.aspx, October 12, 2016 [Nov 21, 2017]

About the Author: Jonathan Azarcon is currently the EVP of Marketing for iS5 Communications and has over 22 years combined experience in Telecommunications Technology working in Business Enterprise and Industrial Control Applications. He has designed and implemented networks for customers worldwide as a Professional Services Consultant with Alcatel Networks and as a VP of Global Services & Support at RuggedCom Networks and Siemens AG was instrumental in helping customers implement & support Communications Technology for their ICS.