PAY NOW OR PAY LATER

Understanding the costly consequences of neglecting OT/ICS Cybersecurity

INSIGHTS

This paper underscores the critical necessity for implementing robust cybersecurity measures in the domains of Operational Technology (OT) and Industrial Control Systems (ICS).

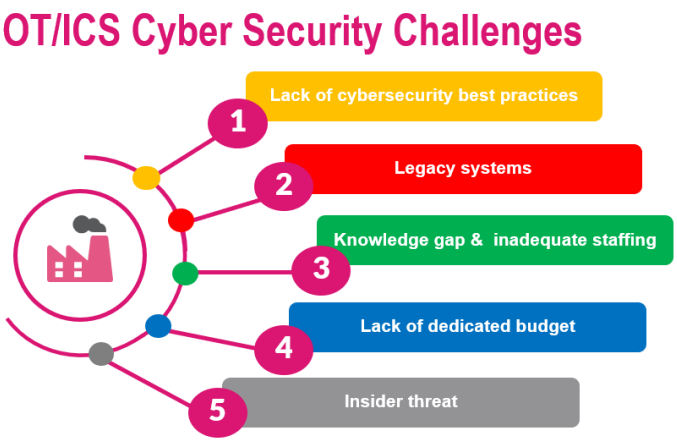

Figure 1: General OT/ICS Cyber Security Challenges

Considering the growing convergence of IT and OT, the advent of digital transformation, IIoT (Industrial IoT), Industry 4.0 and the migration to cloud-based infrastructure, the vulnerabilities of these systems to cyber threats have become a paramount concern.

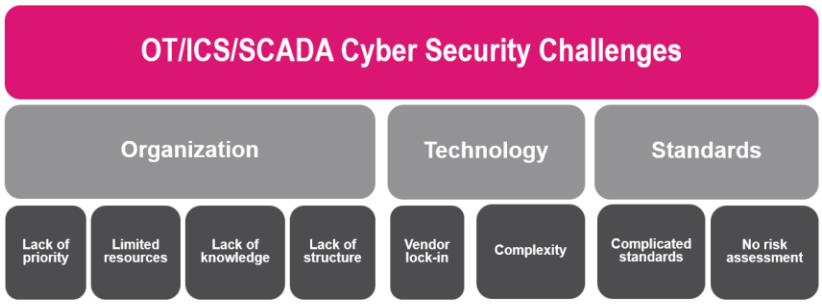

Figure 2: Organizational, technology and standards challenges

RISK AND CONSEQUENCES

Cyber threats targeting OT/ICS systems pose potential risks that cannot be ignored. Neglecting cybersecurity in these domains can have severe consequences. However, assessing risks in these complex environments is a challenging task. OT networks are typically static, and the life cycle of assets in this realm is long. Common assets found in OT networks include Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), Human Machine Interfaces (HMIs), and Intelligent Electronic Devices (IEDs). Hackers, aware of these challenges, make attempts to exploit outdated software and vulnerable ICS assets to infiltrate and compromise OT networks.

In the year 2022, the manufacturing industry emerged as one of the most targeted Operational Technology verticals. The risks associated with cyberattacks on OT systems, such as Critical Infrastructures and CNI (Critical National Infrastructures), are diverse. The risks range from physical damage and operational disruptions to potential loss of life. Additionally, there are other risks such as state sponsored attacks, hacktivism and cyber warfare, API security vulnerabilities, malware, Advanced Persistent Threats (APTs), propagation attacks and supply chain attacks. It is crucial to address these risks and ensure robust cybersecurity measures are in place to safeguard OT/ICS systems. The consequences are highly dependent on the maturity of the OT environment. Safeguarding OT/ICS systems from cyber threats is crucial to ensure public safety, economic stability and national security.

CHALLENGES

In today's shop floors/plants, outdated Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) with serial interfaces like RS-232 interfaces are still widely used. However, the adoption of IIoT (Industrial IoT), Industry 4.0 has become challenging for OT administrators and operators as many assets, particularly those equipped with serial interfaces, are not connected to the network due to their lack of IP capabilities. The digital transformation of OT environments brings along several other pain points that need to be addressed. One of the major challenges is the reliance on legacy hardware and software, which often also comes with limited connectivity options. This can pose difficulties when trying to integrate and connect different systems seamlessly. Additionally, there are concerns related to data management and security, as safeguarding sensitive information becomes crucial. Interoperability is another significant challenge in the digital transformation of OT environments. Ensuring the smooth operation and communication between various devices and systems can be complex and requires careful planning and implementation.

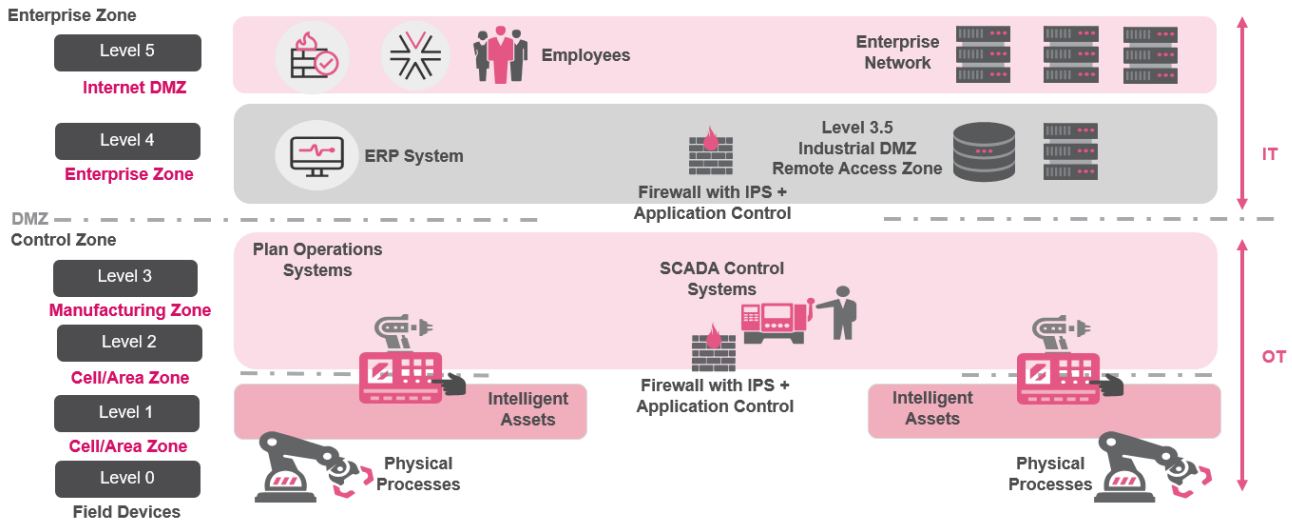

Figure 3: The Purdue Model

Moreover, compliance and certification needs must be met to adhere to industry regulations and standards, which can further complicate the transformation process. Vendor lock-in is a common issue that organizations face during digital transformation. It can be challenging to switch between different solutions due to dependencies on specific vendors, limiting flexibility and potentially hindering innovation. Furthermore, with the exponential growth of IoT (Internet of Things) and IIoT (Industrial Internet of Things) devices, the attack surface expands, making OT environments more vulnerable to cybersecurity threats. OT environments are becoming more complex and interconnected. Managing this increased complexity requires robust strategies and expertise to ensure smooth operations and minimize disruptions. Lastly, unmanaged and shadowed device fleets pose risks to the overall security and effectiveness of the digital transformation and outlines the need for proper device management and monitoring. The cloud journey opens a completely new realm. ICS environments often require real-time communication and low latency. The reliance on cloud services can introduce potential challenges related to connectivity and bandwidth. The availability and reliability of network connections between the ICS environment and the cloud infrastructure need to be carefully managed to ensure seamless operations. An example of this could be securing telemetry data. That brings us to the second cloud challenge, as ICS environments deal with sensitive data related to industrial processes, critical infrastructure, and operational control. Migrating this data to the cloud requires robust security measures to protect against unauthorized access, data breaches and insider threats. Encryption, access controls and secure data transmission protocols should be implemented to maintain data integrity and confidentiality. Thirdly, the regulatory compliance standards are essential too. Lastly, dependence on cloud services introduces the risk of service downtime or outages. ICS environments often require continuous operations and any disruption in cloud services can have significant impacts. Organizations need to consider redundancy, failover mechanisms and disaster recovery plans to minimize the impact of cloud service disruptions.

BEST PRACTICES

To ensure optimal performance in OT, it is crucial to direct attention towards various key areas of best practices.

1. **Risk Assessment and Management |** It is important to assess and manage risks associated with OT systems to ensure their security and reliability.

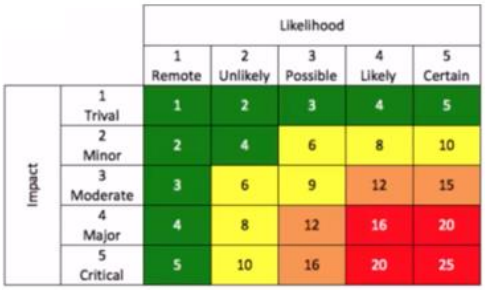

Figure 4: ISA 62443-3-2 formula for calculating the risk factor (R)

$$Risk\ (R) = Likelihood\ (P) * Impact\ (I)$$

$$Risk = P * I$$

2. **Defense-in-Depth |** Implementing multiple layers of security control, like access control and IPS to minimize risk of unauthorized access and potential disruptions.
3. **Network Segmentation |** Dividing the OT network into isolated segments helps to minimize the impact of a security breach and limit unauthorized access. Furthermore, it is reducing the risk of lateral movement and minimizing the potential damage to the entire operational technology infrastructure.
4. **User Authentication and Authorization** | Implementing robust authentication mechanisms ensures that only authorized users can access, make changes to the OT systems or other malicious activities.
5. **Patch Management |** Regularly updating and applying patches. Reducing security flaws, bugs and exploitation of vulnerabilities.
6. **Continuous Monitoring |** Monitoring OT systems in real-time allows for the detection of any suspicious activities or anomalies that could indicate a security breach.
7. **Awareness and Employee Training |** Educating employees about the importance of security and providing training on best security practices.
8. **Incident Response Planning |** Having a plan in place for responding to security incidents enables a quick and effective response to minimize damage and downtime.
9. **Collaboration and Information Sharing |** Sharing information and collaborating with industry peers and security experts helps to stay updated on the latest threats and best practices.
10. **Secure by Design |** Incorporating security measures from the initial design phase of OT systems ensures that security is built-in and not an afterthought.

THE IMPORTANCE OF DEDICATED OT SECURITY CONTROLS

I. Security Gateway (OT internal, OT DMZ and OT external firewall) Quantum IoT Protect, Quantum Gateways & Spark Gateways

Implementing a Security Gateway is OT best practices, also with usage asset discovery, usage of zones, IPS & Application Control and Deep Packet Inspection (DPI) the risk could be decreased from impact level 5, critical and level 25, certain likelihood to level 2 minor and unlikely. With an overall risk of 4. IPS will patch know vulnerabilities via signature for known vulnerability. Furthermore, with zones and segmentation possible lateral movement and propagation attacks are prevented. As well as misconfigurations. For unknown vulnerabilities, Zero Days threat emulation and threat extraction is available however this is not a best practice in OT environments as there is a possible downtime and safety risk. This solution is also a robust countermeasure for hacktivism and cyber warfare.

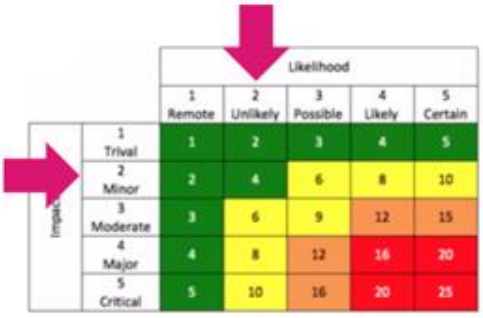

Figure 5: Example calculation dedicated OT gateways.

II. Security inside the device with on-device, run time protection Quantum IoT Embedded Nano Agent

By incorporating embedded OT and IoT security controls, the device is hardened from within. Providing a zero-day safety net and is offering 99.999999 preventative security controls for all network and device attacks. In addition, misconfigurations, weak passwords, APTs and unsecured keys are secured) The risk factor is will be decreased from impact level 5, critical and level 25, likelihood “certain” to level 1 remote and trivial. With an overall risk score of 1.

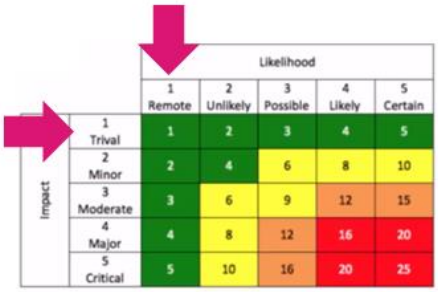

Figure 6: Example calculation on-device security.

III. Training
Check Point Mind Academy

To maintain a very strong security posture throughout the plant, training is highly recommended. Addressing concerns like malicious USB, Tactics, Techniques and Procedures (TTP), Malicious Insider and how to handle and act on system errors.

CONCLUSION

It is imperative to underscore the paramount importance of implementing strong cybersecurity measures in OT/ICS environments. The growing integration of IT and OT, the advent of digital transformation, cloud adoption and the rise of IIoT and Industry 4.0, all expose these systems to significant cyber risks, demanding proactive measures to protect critical infrastructure. By comprehending the dangers, embracing best practices, and tackling key obstacles, organizations can fortify their cybersecurity stance in OT/ICS environments and effectively mitigate potential threats.

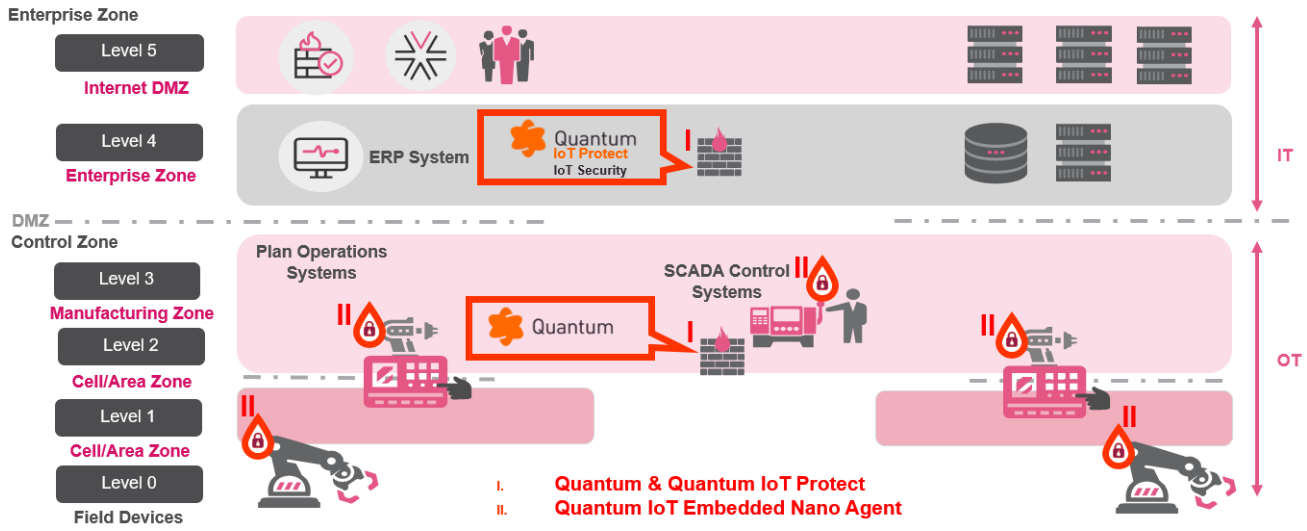

Figure 7: A secured and resilient OT environment.

Read more about how to use Check Point IoT Solutions, Quantum IoT Protect and Quantum IoT Embedded Nano Agent to addresses these challenges with the best **ROI** (Return on Investment) and a low **TCO** (Total Cost of Ownership). Want to learn more? Refer to Mind – Cyber Security Training Programs.

CONTACT US
Worldwide Headquarters | 5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599
U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel.: 800-429-4391 | www.checkpoint.com

December 2023