USAID
FROM THE AMERICAN PEOPLE

FUNDAMENTALS OF OPERATIONAL TECHNOLOGY, CRITICAL INFRASTRUCTURE AND IT INTEGRATION CYBERSECURITY

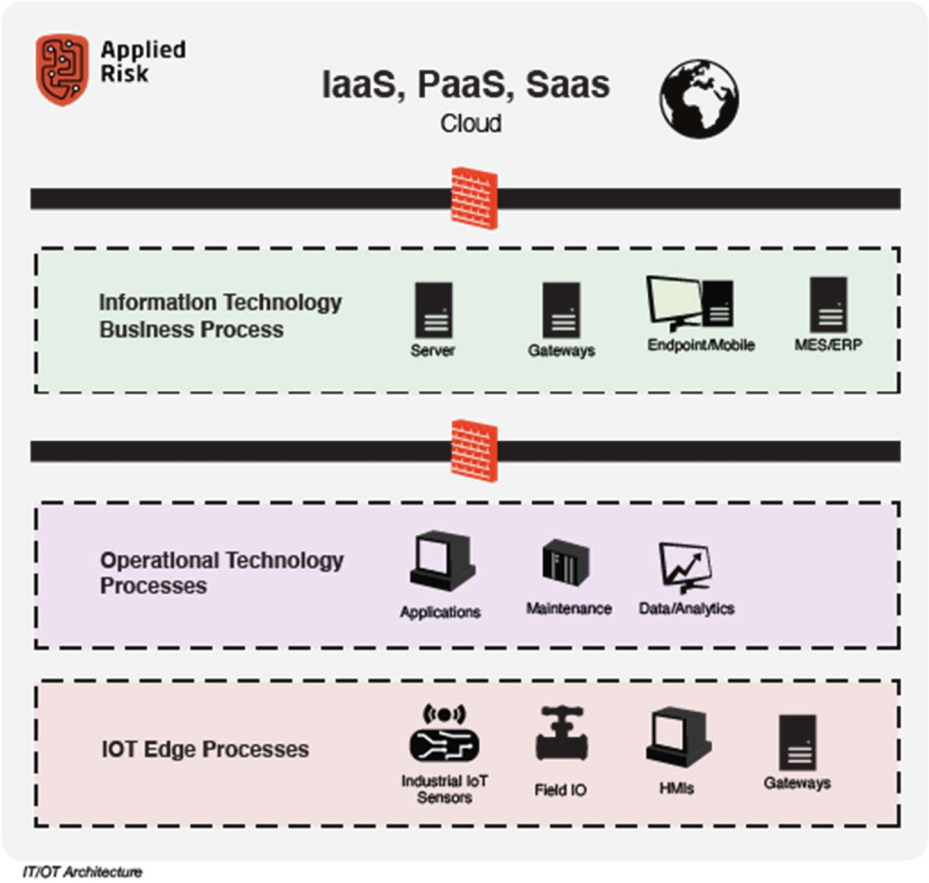
This publication was produced at the request of the United States Agency for International Development. It was prepared independently by implementing partner, Catalisto LLC for the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The authors' views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States government.

MODULE 5 - INTRODUCTION

IT and OT are increasingly becoming one and the same entity, and are approaching a common set of business goals and objectives for the future of many industries. Driven by the increase of Industrial Internet of Things (IIoT), Industry 4.0 and new business opportunities presented by digital transformation, many organisations are already entering the IT/OT integration journey and embracing the benefits as well as risks associated with such business models.

The benefits of economies of scale are shifting from owners and operators to manufacturers, and a number of research findings show that companies are more likely to integrate OT systems into their business models than in the past. One of the key benefits of managing IT OT convergence includes improved information for better decision making. This allows manufacturers to start transforming the data generated by machines and processes into valuable insights, such as predictive maintenance.

The convergence of IT and OT should be encouraged and promoted at technology, security and process levels (security as business enabler). While convergence and integration of OT brings improvements, current technology developments require managers responsible for the OT domain to start new discussions about how to keep critical infrastructures safe, resilient and up-to-date. However, for this to happen organisations need to consider both IT and OT environments and their readiness to converge, which is often not the case, as today many facilities lack the necessary infrastructure are certainly not future-proof.



IT/OT Architecture

OT CYBERSECURITY

The field of OT and cyber security is still evolving, and the number of well-documented incidents is still relatively low. Categorisation is an important step in identifying trends and ultimately identifying vulnerabilities and managing security risk.

A holistic approach is required to overcome the added challenges of IT and OT convergence and to secure critical infrastructure. Below are some important aspects to consider:

Governance: A new way of working requires a significant investment in company culture, to address in first instance the changing IT/OT governance (roles and responsibilities), risk management across both IT and OT domains, supply chain concerns and management of dependencies and services, such as Cloud.

IT/OT Reference Architecture: The need for comprehensive IT/OT reference architecture covering the full set of components and levels from edge devices to the cloud. Zones and conduits will need to be reconsidered.

Risk and Compliance: Assessment of the risks, threat models, and cyber kill chain unique to your critical assets (including safety) is a crucial first step to manage and thwart cyberattacks. Additionally, conformance to industry standards such the IEC 62443 to securely partition the infrastructure into zones and conduits hardens security. Compliance with regional and industry-specific regulations such as NIS EU Directive adds predictability to your essential services.

Situational Awareness & Threat Intelligence: Recent security incidents such the SolarWinds hack confirmed the need for adopting new strategies to improve cyber security situational awareness and resilience against threats. In this way, it enables you to be aware of and respond rapidly to threats.

Security Awareness & Training: The increased adoption of IT solutions in OT environments underscores the need to train operators and engineers, SOC analysts and management staff on best practices and security hygiene in a converged IT/OT environment. Third parties will similarly require training, since such service providers are often responsible for many tasks around IT and OT.

Understanding your IT/OT environment, navigating regulatory requirements, and crafting the right action plan for better security requires substantial technical expertise. Applied Risk provides tailored and client-centric solutions that assist asset owners, system integrators, and suppliers to develop, deploy, and maintain cyber-resilient operations and ultimately help you reach your business goals.

If you require assistance with any of the aspects mentioned in this article or would like to have a consultation about your OT security requirements, do not hesitate to reach out to us for more information or to receive non-binding advice from our experts.

SIX KEY GUIDELINES TO PROTECT CRITICAL INFRASTRUCTURE FROM CYBER THREATS

Critical infrastructure is defined as the assets, core systems and strategic networks — both physical and digital — that are so essential to a nation that their incapacitation or destruction could have a

debilitating impact on either physical security, continuity of the economy, interruption to the national public health system or any combination therein.

The U.S.'s Cybersecurity and Infrastructure Security Agency considers 16 sectors to be critical infrastructure, ranging from commercial facilities to nuclear reactors. For these sectors to rise to the level of critical infrastructure, they must be so vital that it is believed that their disruption would result in a noticeable socioeconomic crisis with the potential to undermine the underlying security of a society. If these sectors are compromised the political, strategic and security consequences are nearly incalculable.

For nations to mitigate and confront the threat to critical information infrastructures, they must tactfully balance the need for prevention, deterrence, identification and discovery of an attack with an effective strategy for a response, crisis management, damage control and, eventually, a protocol to return to regular operations. This is no small task. It demands a comprehensive understanding of the intersection of malicious players and the expanding attack surface.

UNIQUE CHALLENGES FOR CRITICAL INFRASTRUCTURE VERSUS OTHER SECTORS

What unifies these essential industries is often a combination of the necessary strategic planning to ensure basic cybersecurity and the specialized processes of operational network isolation, dedicated security protocols and a seemingly never-ending bottleneck of mission-critical files requiring sanitization.

According to a recent Deloitte report: "Most critical infrastructure protection programs only address physical threats, leaving states vulnerable to cyber threats ranging from service disruption to public safety concerns."

This segmented approach to security demands a reassessment of the risk mindset if it intends to manage increasing cyber risks. The reconsideration must integrate state-wide institutions with public-private collaboration to focus on raising awareness and crafting a unified response to cyber threats.

KEY GUIDELINES FOR CRITICAL INFRASTRUCTURE

In critical infrastructure, there are a number of key processes that can dramatically improve cybersecurity. These key guidelines clarify and streamline critical infrastructure defence.

Here are some of the most impactful guidelines:

Regulation and Industry Compliance

Industry-wide regulations (such as the North American Energy Reliability Corporation's Critical Infrastructure Protection (NERC CIP) standards) and their resulting fines dictate the pace of compliance. Money speaks, and this is even more true when it comes to the heightened financial consequences of noncompliance to industry and state-mandated regulations. For many critical infrastructure sectors, the balance of complicated legal mandates and new technological solutions can leave gaps, further emphasizing the importance of intervention to mandate a standardized approach to decreasing cyber risk.

Operational Network Isolation

Insulating vital systems (e.g., energy and wastewater management) from external networks decreases the attack surface, but you have to also consider that system-wide updates can become more tedious and difficult to apply.

Large-Scale Bottleneck of File Sanitization

With a plethora of important data points as well as external media and files requiring integration into isolated networks, critical infrastructure sectors must standardize a comprehensive sanitization process to prevent malware and malicious elements from compromising secure networks.

Security Tools

There is no lack of technical solutions to mitigate cyber risk — possibilities range from the inclusion of multiple layers of sandbox-based security solutions to isolation from broader networks to limiting user access to vital servers to various levels of encryption processes.

While each of the 16 sectors of critical infrastructure faces a unique risk environment, the integration of these common security processes — as well as SOAR (Security Orchestration, Automation and Response) or SIEM (Security Information and Event Management) systems — can provide the strongest technical foundation for cybersecurity in many of these essential industries.

Education

According to Kaspersky's State of Cybersecurity 2019 report, "Employee errors or unintentional actions were responsible for 52% of incidents affecting operational technology (OT) and industrial control system (ICS) networks in the past year, a study shows."

With such a large segment of cyber incidents stemming from a lack of employee awareness or understanding of common phishing and ransomware tactics, one of the first steps in protecting critical infrastructure must be to allocate more time to companywide prioritization of cybersecurity.

Update and Apply Patches Of All Software And Technology

Stopping the flow of malware to critical infrastructure cannot be done without the implementation of system updates and patches across the organization, including servers and endpoints.

According to CIO, "57% of cyberattack victims report that their breaches could have been prevented by installing an available patch, according to a new ServiceNow study conducted by the Ponemon Institute. And 34% of those respondents were already aware of the vulnerability before they were attacked." While hackers are creating new and ever more toxic malware to let loose on any number of sectors, many are utilizing existing malware kits with dramatic results.

Ensuring Critical Infrastructure Continuity

While some sectors have taken a proactive approach to cybersecurity, mitigating risks and creating a clear definition of the vulnerable elements, the overwhelming majority of critical infrastructure sectors are wilfully unprepared for the scale and scope of cyberterrorism that could impact their vital systems.

In short, for cybersecurity to become a true foundational element in the long-term defense of critical infrastructure, it requires active application of patches and system updates, education of employees and system users, the support of private-sector organizations, government legislation to impose harsh penalties for noncompliance, the implementation of diverse security tools and clear protocols to comprehensively mitigate cyber risk.

READING MATERIAL & LINKS

1. Module_5_Whitepaper1-integrating_cybersecurity_0
2. Module_5_Whitepaper2-deloitte-building-cyber-security-into-critical-infrastructure
3. Module_5_Whitepaper3-Comprehensive Guide to Operational Technology Cybersecurity
4. https://www.researchgate.net/publication/349969874_Understanding_the_Challenge_of_Cybersecurity_in_Critical_Infrastructure_Sectorshttps://www.cisecurity.org/white-papers/cis-controls-v8-mapping-to-nist-csf/