YOKOGAWA

Co-innovating tomorrow™

White paper : The First Step in Securing your OT Environment

Discovering your Baseline with OT Security Risk Assessment

Bulletin 43D07T31-01EN July 3, 2020

Contents

1. Executive Overview

Enterprises today rely on high levels of automation and Information Technology (IT) to meet the global demand for supplies in a modern competitive world. Managing Operational Technology (OT) security is one of the leading business challenges to achieving reliability and availability, ensuring health and safety, and meeting regulatory compliance. Furthermore, triggered by the outbreak of COVID-19, executives are actively looking into reconsidering and improving business operations. From the business continuity perspective, cyber security management plays a vital role.

Organizations face the following issues in managing OT security:

- Difficulty in assessing risk due to low visibility of OT assets
- Mitigating risk and prioritizing investment
- Keeping up with industry standards and incorporating safety systems in the scope
- Managing security risk throughout the entire plant lifecycle with limited OT expertise

This whitepaper describes how companies and organizations can address the above challenges by taking the risk-based approach to cybersecurity management. Readers will learn:

- Why the risk-based approach is essential for effective security risk management
- How technical security risks assessments determine the security baseline
- How the outcomes of the assessments will lead to efficient investment and risk management

2. The Current State of OT Security

In a modern competitive world, the efficiency of industrial systems needs to be optimized and increased to meet the global demand for supplies. As a result, this leads to systems becoming more complex with an increased reliance on high levels of automation and IT. Although using IT has principally benefitted the industry, it also brought new challenges to OT security.

Digital transformation accelerating IT/OT convergence and cyber threat

Many of the industrial plants that were once completely isolated are now connected with the outer world. Companies are striving to transform their operations and businesses digitally for competitiveness, by connecting not only vertically within their plant, but also horizontally within sites, companies, and across the supply chain. The vast connection creates not only business opportunities but also challenges in securing the network and data.

With more components and functions required to optimize the operation, industrial plants are becoming increasingly complex and automated, and the use of IT in industrial environments is now essential. However, these commercial off-the-shelf technologies like Windows, Ethernet, and TCP/IP have typically been developed for environments with less stringent requirements. This results in industrial plants having larger attack surfaces, which lead to considerably larger exposure and increased probability of facing cybersecurity issues.

Research shows that the top three cyber threats are devices and "things" added to the network, internal threats (accident), and external threats (supply chain or partnerships), which are all accelerated from IT/OT convergence (Figure 1) [*1].

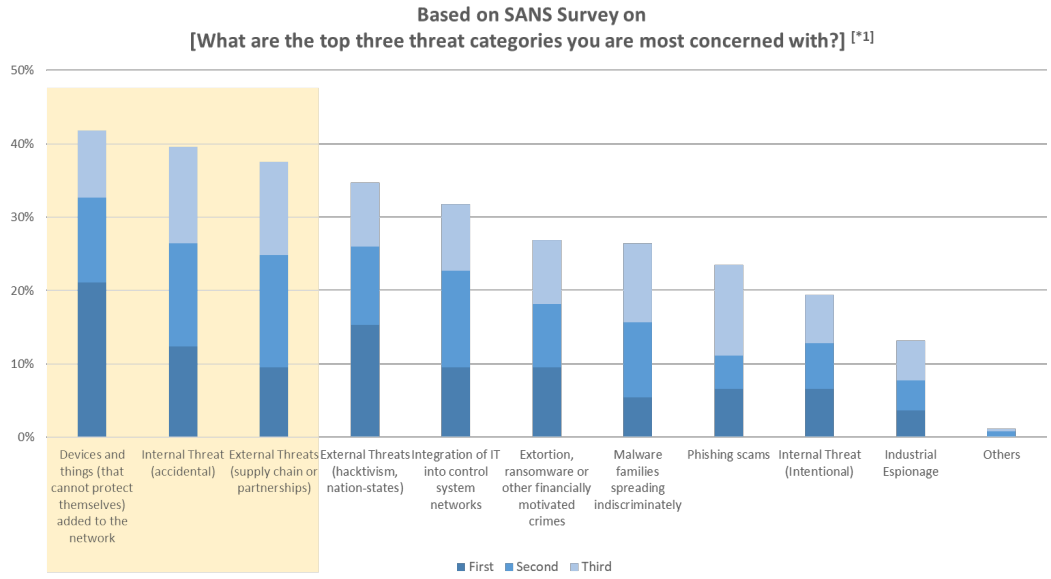

Figure 1: Leading Cyber Threats as per SANS 2019 State of OT/ICS Cybersecurity Survey

High reliability and availability requirements leading to difficulty in security management

Responsible for the critical infrastructure supporting our everyday life and business operation; reliability and availability requirements for industrial control systems are naturally very high. For asset owners, the high reliability and availability requirements make effective security management very difficult, as they wish to refrain from making unnecessary updates if the system is running without any current problems.

Industrial systems arising as potential targets

Criminals and state actors have become aware of the potential target of industrial systems. Targeting critical infrastructure has a significant impact on society, while the cyber security of industrial systems is generally less mature than those of other IT sectors.

The increasing number, variety and impact of cyber threats in the OT domain can no longer be ignored. Threats vary from unintentional infection through USB devices, to disgruntled employees trying to cause harm or blackmail, up to nation-state attacks with the intent to cause death and destruction. The last example refers to the Triton attack in 2017, where a nation-state actor was suspected of having modified the safety system of a plant to cause severe damage. The attack failed, however, due to an error made by the attackers that exposed their effort.

Not only can these security breaches have serious operational and safety consequences, but it can also affect your business in different ways. Think of economic damage or reputational damage, when a part of the plant becomes locked down due to malware. Most companies, including boards and executive leaders, now recognize cyber risk as one of their top business risks (Figure 2) [*1].

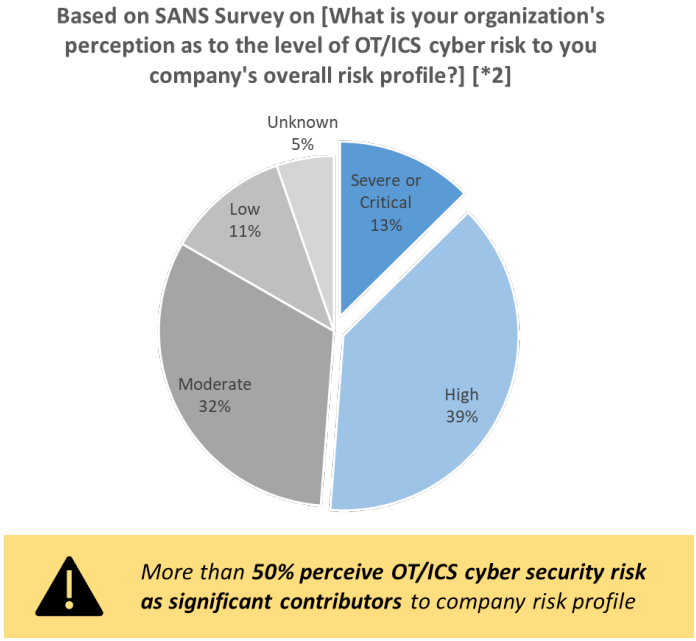

Figure 2 – OT/ICS cybersecurity risks as significant contributors to company risk profile as per SANS 2019 State of OT/ICS Cybersecurity Survey

3. Why OT Security is Harder than Ever

Industrial control systems serve as the brain of the plant. Its availability, resilience, and sustainability will significantly impact the availability of the entire plant, as well as safety, operational cost, and business performance. As seen in recent plant shutdowns triggered by ransomware attacks, security incidents can bring negative impact to top management and stakeholders.

Furthermore, as the entire world faced an extremely challenging economic and business situation in 2020 due to the outbreak of COVID-19, executives are looking into reconsidering and improving business operations from the business continuity perspective, preparing for operation under a state of emergency. Security risk management, which is creating a sustainable system to manage and mitigate security risk, is a top priority for organizations and responsible teams; however, it is harder than ever due to the following challenges:

Difficulty in assessing risk due to low visibility of OT assets

Since industrial plants expand and evolve during their long lifecycle, it is challenging to gain visibility of OT assets. The SANS 2019 State of OT/ICS Cybersecurity Survey shows that less than 36% of respondents claim to have a comprehensive overview of all the elements of control systems security for their enterprise or plant. As top 2019 initiatives for increasing OT/control system and network security, 45.5% of respondents raised "Increasing visibility into control system cyber assets and configurations," whilst 37.3% stated, "Perform security assessment or audit of control systems and control system networks."[*1].Organizations are not reaching down into the ICS infrastructure to monitor those assets considered to have the highest impact if exploited.

Mitigating risk and prioritizing investment

Teams responsible for OT security need to justify investment decisions and explain to the board members on the current risk they are facing, where to spend the initial investment, and the entire investment plan to mitigate security risk for their enterprise. Yet many companies lack visibility in their OT assets, therefore making it impossible to explain clearly how much they need to invest and where to start. If companies implement security measures on an ad hoc basis, this will lead to inefficient spending of budget and resources, with no one knowing whether the security risk was reduced.

Keeping up with industry standards and incorporating safety systems in the scope

Implementing countermeasures and continuing to be compliant with emerging standards alone is challenging. Research suggests NIST CSF (Cyber Security Frameworks), ISO 27000 series, NIST 800-53, NIST 800-82, ISA/IEC62443, and CIS Critical Security Controls are being referred to by many companies. There is no single regulation, standard, or best practice that cover all aspects and regions.[1] In the case of Europe, the European NIS (Network and Information Systems) directive has been rolled out and will result in laws per country. The GDPR compliance is another example showing that regulations must to be followed in a security program.
Additionally, from the risk management perspective, it is highly recommended to comply with the two standards, IEC62443 and IEC61511, which are currently separately defined. In the recently published edition of IEC61511, a technical standard-setting practice in the engineering of Safety Instrumented Systems, it is explicitly stated that conducting security risk assessments have now become a mandatory requirement.

Managing security risk throughout the entire plant lifecycle with limited OT security expertise

While the implementation and management of the security measures must be continued throughout the plant lifecycle, which lasts for more than 20 years, security teams face the lack of security personnel and expertise when it comes to security. According to research regarding security skill gaps, more than 85% of respondents claim that their security teams are understaffed and feel overworked compared to the previous year. Also, 94% responded that the skills required to be an excellent security professional have changed in the past few years, which shows that security experts face difficulty in keeping up with the latest technology trends and security threats [2].

4. Taking a Risk-based Approach to OT Security

Why take the risk-based approach?

Taking the risk-based approach will effectively reduce risk at significantly less cost. According to a case study from McKinsey & Company, the maturity-based approach, which is building the highest level of defense around everything, costs a total of 14 million Euros. However, the risk-based approach, which optimizes defensive layers for risk-reduction and cost, costs a total of 5 million Euros, which is almost one-third of the traditional method [3].

Key requirements for taking a risk-based approach

The following are the four key requirements in taking a risk-based approach to OT security.

Determine the security baseline

Before risks can be managed, they first must be identified and assessed by a risk assessment. A risk assessment enables OT security stakeholders to understand the baseline. Acknowledging the current status of the plant is fundamental and is the starting point of the security journey.

Define risk from a holistic view

Risks come from many different directions and categories. For example, a risk assessment that only focuses on high-level business processes might fail to identify risks due to flaws in technical implementations. Insufficiently defined leadership regarding security at the boardroom level is a risk, but a poorly configured firewall is also a security risk.

Therefore, it is essential to have a scope that is sufficiently broad and incorporates different parts of the organization. Furthermore, a combination of a paper review with an onsite, technical assessment is vital for a comprehensive risk assessment.

Comply with security standards for guidance

Compliance with a security standard is beneficial since it makes the implementation of a security program more effective and straight forward compared to the alternative of reinventing the wheel on your own.

In the OT security domain, there are many emerging security standards, like there are many standards for the IT domain. Currently, many OT security stakeholders follow the guidelines of the IEC 62443, which is becoming the key standard in the industry. IEC62443 is designed for industrial systems and is, therefore, more suited for the purpose than other security standards that are not explicitly focused on industrial systems. As an entire series of standards, IEC62443 covers every aspect of a security program, ranging from risk assessments to technical design specifications.

The IEC 62443 level approach is to define a target security level for your plant or zones of your plant (Table 1). Companies are required to establish the correct target security level upon assessing their plant.

Security Level based on the description in IEC62443-3-3

	Description
Security Level 0	No specific requirements or security protection necessary in the IACS
Security Level 1	The IACS has a cyber security protection against casual or coincidental violation
Security Level 2	The IACS has a cyber security protection against intentional violation using simple means with low resources, generic skills and low motivation
Security Level 3	The IACS has a cyber security protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
Security Level 4	The IACS has a cyber security protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

Table 1 - Security Level based on the description in IEC62443-3-3

Establish a systematic process

Organizations must follow a systematic process to establish a persistent operational risk management process for OT security. This risk management process is a strategic activity that involves short- and long-term considerations. Thus, planning for strategic risk management is necessary to ensure continuous risk assurance.

Adopting a risk-based approach will guide organizations to make complex decisions, on which action to take, and where to invest. Effective risk management starts with knowing and thoroughly understanding your risks. However, the complex operational environment, evolving cyber threats, and continuously updated laws and policies make this responsibility extremely challenging for organizations to handle on their own. Therefore, many companies are seeking for support from security partners when it comes to security assessments. According to a recent survey, 64% of the corporate security experts mentioned that their company would benefit from outside help [2].

5. Starting Point to Obtaining the Baseline: Technical Security Risk Assessment

To take a risk-based approach to cyber security management, Yokogawa recommends the Technical Security Risk Assessment as the starting point to obtaining the OT security baseline. By assessing the impact and likelihood associated with threats facing the OT environment, the Technical Security Risk Assessment determines the security risk to the organization.

Overview of the Technical Security Risk Assessment

Yokogawa's Technical Security Risk Assessment starts with a vulnerability assessment that aims to identify which vulnerabilities are present in the OT environment. When the vulnerabilities are identified, a scenario-based risk assessment is conducted to define the highest risks facing the OT environment, and which problems need to be solved most urgently. Vulnerabilities and risks are not the same, a vulnerability is a flaw or weakness while a risk is the probability of something bad to happen.

In the technical vulnerability assessment phase, multiple methods are used to gather vulnerabilities, verify and check findings, and create a complete and reliable picture of the vulnerabilities that exist in the environment.

This database of vulnerabilities will be the input of the risk assessment phase and will be conducted by the same team that was involved in the vulnerability assessment phase. This means that a large amount of knowledge and insight regarding the vulnerabilities facing the OT environment will be present at the start of the risk assessment.
A report will conclude the technical risk assessment. This report includes findings on any high-level risk and the immediate actions required, a list of risks and vulnerabilities, a gap analysis between the existing state of the plant and security requirements, and a roadmap on how to develop or improve the security program; this includes the planning of countermeasures and other concrete recommendations.

Vulnerability assessment phase

IEC62443 defines vulnerability as a "flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy."

A consultant and an engineer will perform the vulnerability assessment. During the assessment, several methods are used to collect a database of vulnerabilities. Typical methods include conducting interviews and technical inspections.

The Yokogawa consultant goes through an extensive questionnaire that contains questions based on both the IEC62443 and Yokogawa extensive security experience. The questions vary from detailed technical implementation to how security is managed by the local organization.

Upon cooperation with the customer's local OT security organization, the Yokogawa engineer investigates the state of security through hands-on technical inspections. Networks and components such as User and PC Management, Network Devices, Patch, and Antivirus Management Servers are accessed and manually investigated.

Risk assessment phase

Once the assessment reveals the vulnerabilities of the system, the next step is to define the risk to the system. The risk will be determined by assessing the impact and the likelihood of each scenario.

IEC62443 defines risk in the following formula.

The Yokogawa Security Consultant leads the risk assessment workshop. A multidisciplinary team of experts and stakeholders from the customer must be present to support the accurate quantification of risks. During this workshop, the findings of the assessment are presented, and the risk is calculated with input from customer specialists with a technical, safety, financial, and environmental background.

Based on industry experience and vulnerabilities identified in the previous phase, the consultant presents threats and determines the likelihood of a scenario being exploited (Table 2).

Likelihood Level Description

Likelihood Level	Description
Likely	The threat scenario is most likely to occur in the organization's IACS
Possible	The threat scenario is quite possible to occur in the organization's IACS
Unlikely	The threat scenario is unusual to happen in the organization's IACS but possible to occur
Rare	The threat scenario is very unlikely to occur in the organization's IACS
Improbable	The threat scenario is unrealistic to happen in the organization's IACS

Table 2 – Likelihood level definition

The consultant also explains the consequence of the system when this scenario is exploited.
An example threat scenario could be a disgruntled employee installing ransomware, which will hold the system hostage via an infected USB stick.

The consultant will evaluate the vulnerabilities in physical protection and finds that it is easy to insert a USB stick. Another vulnerability is that the software is only updated every three months, which makes it possible for known malware to spread over the network. The backups are not stored offline but on the backup server, which will be infected as well.
In the above example, the likelihood is: **Likely**

The impact of the threat scenario is determined by the customer, who is best in assessing the impact on the operational process. Based on the explanation, it is clear for the customer that all operator stations are lost in this scenario, including the backups, which means the plant will be down for a long time.

The impact is split into four subjects: safety, environment, financial, and reputation impact. For all topics, the 'likely' impact is determined, and the highest impact score is used for the risk calculation (Table 3).

Impact Level	Areas of Impact: SAFETY	ENVIRONMENT	FINANCIAL	REPUTATION
CRITICAL				
MAJOR				
MODERATE				
MINOR				
TRIVIAL				

Table 3 – Impact Level Definition

The combination of the two determines the risk (Table 4).

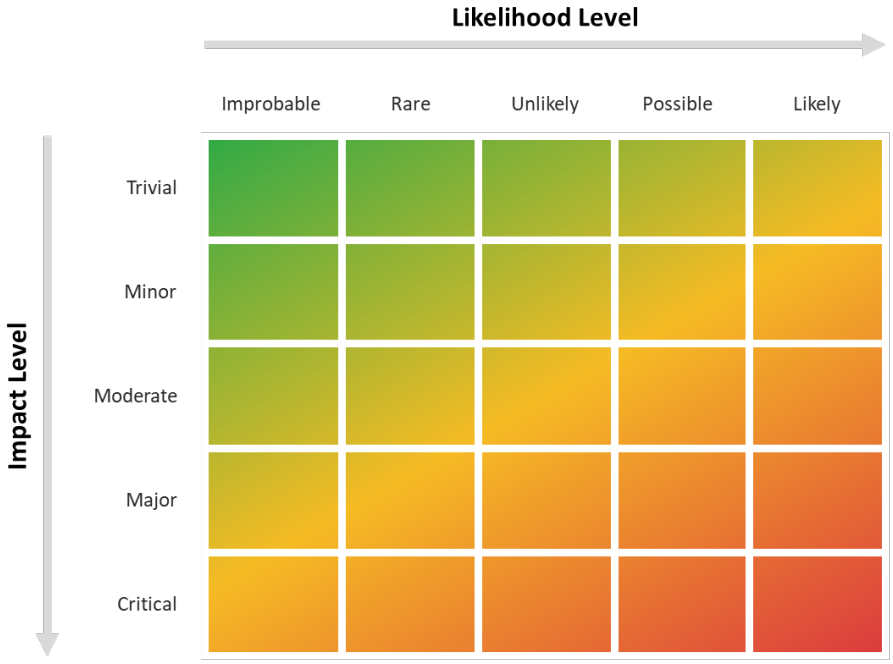

Table 4 – Risk Level Definition

In addition, the effectiveness measured in risk reduction of possible countermeasures will be assessed when the unmitigated risk is considered too high.

Technical Security Risk Assessment Report

The result of the risk assessment and the vulnerability assessment is documented in the Technical Security Risk Assessment Report that contains:

- An executive summary
- An overview of the used methodology
- An overview of the risks facing the OT environment
- An overview of the vulnerabilities that are present in the OT environment
- A gap analysis between the existing state of the plant and the security requirements
- A roadmap on how to develop or improve the security program

The outcome of the assessment will support constructive discussion with the management on what immediate measures need to be taken to address the high-level risk, and how to plan an effective security program to implement the countermeasures.

Yokogawa has extensive experience in OT security, ranging from developing policies and procedures for security governance, secure network design and implementation, and providing managed services. Yokogawa will help with addressing any of the issues revealed during the risk assessment and support customers in continuing with their security journey.

6. Business Benefits and Case Studies

Business benefits: Reduce enterprise risk with minimal investment

Based on the outcome of the Technical Security Risk Assessment, companies will be able to identify risks and create mitigation plans to address the highest risks and remove critical vulnerabilities. With more insight in risks, assessments help OT security stakeholders better prioritize the actions to be taken, effectively reducing security risk while optimizing investment.

The draft roadmap will support companies to create a mid to long term plan on how to carry on the security program for their plant and in which manner to implement the countermeasures. This roadmap also avoids inefficient investment and unmanageable security controls while complying with industry standards.

Case Study

The following case study introduces how Yokogawa addressed the customer's challenges through the Technical Security Risk Assessment.

Customer Challenges

The customer has multiple plants at a single location. All the plants are working standalone but have a local DMZ and a network connection to one central upper zone. The customer suspects that the security of their plants is not where it should be, but a clear overview of high priority issues is not present. Besides some small-scale ad hoc initiatives to improve security pushed by the head of the local IT department, not much has happened for the past ten years. During that same period, the OT infrastructure has been steadily growing, and various systems have been interconnected. Concerns about security have occasionally been raised to low-level management, but no decisive action was taken because the precise nature of the risks and the cost to mitigate always remained vague and unclear.

From the higher-level management, clear instructions were issued that actions must be taken. The customer started from the IEC62443 standard and has set Security level 2 requirements (SL 2) for each plant. However, the local organization struggle on how to implement security on delicate OT infrastructure. While the IT organization is willing to support, they lack knowledge of the OT domain. The team struggles where to start and how to change the organization.

Solution

Yokogawa proposed to perform a Technical Security Risk Assessment to map the current security status of the plants. By this assessment, Yokogawa measured the current state of security of the plant to determine which IEC 62443 security requirements are met and which are not. After this measurement, Yokogawa created a roadmap for each plant with a plan to add additional security countermeasures to reach the required security level.

Outcome and Customer Feedback

Based on the IEC62443 requirements list, the gaps and vulnerabilities were listed. Below is an example of a single IEC62443 requirement with a recommendation on how to comply based on the assessment.

Example of IEC62443 Requirement and Recommendation:

Security Requirement	**Security Level**	**Title**	**Compliancy**
SR 1.1.1	2	Unique identification and authentication	**Not Compliant**
The control system shall provide the capability to uniquely identify and authenticate all human users.			
Recommendation		**Explanation**	
Avoid shared user accounts		All users should have their unique user account. If multiple individuals use the same user account or login credentials, it is not possible to comply with this requirement.	
Active Directory integration		Active Directory allows individuals to use their unique user account to authenticate on multiple systems. Without Active Directory, it is very complicated to comply with this requirement in an environment that contains multiple users and computers.	

The roadmap provided to the customer listed all vulnerabilities that must be addressed to meet the security goal of the customer. The roadmap started by listing critical vulnerabilities that must be resolved immediately. It was followed by recommendations that require relatively little effort and have a significant contribution to reduce security risks, such as implementing a physical key switch on the safety controllers; and to increase the patch and antivirus update frequency. The roadmap ended with the more complex recommendations that will take considerable time and effort to realize, such as create security policies and procedures, upgrade all legacy systems, and implement centralized monitoring.

The customer was satisfied with the roadmap. It provided a clear overview of the necessary steps and where to start. After concluding the technical risk assessment, Yokogawa was asked to provide a quotation for the implementation.

Yokogawa worked with the customer to create a feasible investment plan to meet the customer's budget while addressing the highest risk vulnerabilities.

7. Conclusion

OT security is a high priority at the management level to ensure health and safety and meet the market demand with maximized plant availability. Executives are also actively looking into reconsidering and improving business operations, and cyber security management plays a key role in business continuity.

Security risk management is challenging for many organizations due to low visibility in OT assets leading to difficulty in prioritizing investment for effective risk management. Keeping up with the continuously updated industry standards and managing security risk throughout the entire plant lifecycle also makes it difficult for organizations to tackle the challenge by themselves with limited OT expertise.

Adopting a risk-based approach to cybersecurity will guide organizations to make complex decisions, on which action to take, and where to invest. Before risks can be managed, they first must be identified and assessed by a risk assessment. Acknowledging the security baseline of the plant is fundamental and is the starting point of the security journey.

Yokogawa's Technical Security Risk Assessment sets the foundation and direction for companies to plan and execute their security risk management program. By using multiple methods to gather vulnerabilities, verify and check findings and create a complete and reliable picture of the vulnerabilities that exist in the environment, Yokogawa assesses the impact and likelihood associated with threats facing the OT environment and determines the security risk to the organization.

The outcome of the assessment will support constructive discussion with the management on what immediate measures need to be taken to address the high-level risk, and how to plan an effective security program and implement the required countermeasures. With more insight into risks, assessments help OT security stakeholders to prioritize the actions to be taken, effectively reducing security risk while optimizing investment.

Risk management will guide in a complex operational environment with mazes of laws, policies, and directives, along with an evolving threat landscape. Since this can be challenging even for the most experienced professional, many companies are seeking for support from security partners when it comes to security assessments. With in-depth knowledge and vast experience in both plant operation and OT security, Yokogawa's consultants and engineers will guide you along the security journey.

For more information, please visit our website at:
https://www.yokogawa.com/solutions/services/oprex/oprex-lifecycle/oprex-safety-and-security/

References

[1] SANS 2019 State of OT/ICS Cybersecurity Survey (June 2019)

[2] Tripwire Cybersecurity Skills Gap Survey 2019 (February 2020)

[3] McKinsey & Company, The risk-based approach to cybersecurity (October 2019)

Authors

- Mark Hellinghuizer, Security Consultant at Yokogawa Europe B.V.
- Gijs van Erp, Security Engineer at Yokogawa Europe B.V.
- Ai Takano, Marketing Executive at Yokogawa Electric Corporation

---

YOKOGAWA ELECTRIC CORPORATION
World Headquarters
9-32, Nakacho 2-chome, Musashino-shi, Tokyo 180-8750, Japan
http://www.yokogawa.com/