Overview

A multinational manufacturing company engaged Applied Risk with the goal of understanding the vulnerability of its Operational Technology (OT) assets to cyberattacks. The company took this step for two reasons. On a macro level, it was aware that organisations in the same industry had experienced security breaches, and its directors were keen to determine whether the company as a whole was vulnerable to similar attacks. On a more granular level, it sought to understand the level of risk it might face because of the maturity of the cyber security controls of its existing operational technology systems and components.

Applied Risk responded to the company’s needs by launching a risk assessment programme across various sites, which also enabled the company’s various stakeholders to understand the nature and scope of the challenges facing the manufacturing sector.

Business Case

The business case for the company to undertake a risk assessment programme was supported by the leaders of the company’s engineering and Information technology (IT) divisions, the latter of which had recently been tasked with overseeing OT systems. It was also favoured by the head of the company’s cybersecurity team, which was responsible for integrating security solutions into systems overseen by the IT division. Additionally, it was strongly endorsed by the company’s head of automation, who proved to be an influential advocate once the programme was underway. The company cited three reasons for choosing Applied Risk’s programme over its competitors:

- Focus on OT security and engineering practices;
- Thorough understanding of the differences between IT and OT systems and how cyber security controls need to be adapted for the differing environments;
- A wide range of skills and solutions and agnostic approach.

“I think we all have a better picture now of what steps we can take to ensure business continuity while also sharpening our technological edge.”

Managing Director

“The team helped bridge the gap between the shop floor and the C-suite by teaching everyone involved what the stakes were.”

Senior OT Administrator

“I feel like management finally understands why we don’t always want to go with the lowest bidder.”

Member of IT/OT security team
Challenges

In initial discussions, Applied Risk determined that the manufacturing company faced five key challenges:

The company’s primary focus was production, so security considerations were typically outweighed by concerns about downtime.

The company’s managers and executives had only recently become aware of the risks facing OT systems, so they were not accustomed to thinking of their systems as targets.

The company faced budgetary constraints because profit margins were falling in the manufacturing sector. The push for cost-cutting led many departments to cut back on security as they reduced the scope of ongoing and future projects, as well as planned upgrades.

The company’s OT landscape included multiple sets of control systems. Some of these were legacy technologies that could not easily be updated to meet current security standards and/or were not compatible with the security solutions used in the company’s other facilities.

The company’s OT systems received support and upgrade services from third parties, so on-site technical knowledge was often limited. Since these third parties did not always provide security management for OT systems, on-site familiarity with cybersecurity was also limited.

Our Approach

A high-level risk assessment was used to determine the business, reputational and Health, Safety and Environment (HSE) impact in the event of system compromise or failure, as well as the likelihood that this will happen. The purpose of the risk assessment is to identify the worst-case unmitigated risk to the System under Consideration (SuC), as well as the residual risk after implementing barriers. The target group for completing the risk assessment requires stakeholders from engineering, functional safety, IT and the business disciplines.

The output of the risk assessment was used as input to the grouping of assets into zones and conduits and the detailed risk assessments which will cover the as-is situation and recommended zoning and conduits based on the leading industry standard for securing industrial control systems, IEC 62443.

Furthermore, the risk assessment used a holistic approach to cover all risk areas including people, process and technology.
Steps involved in the cyber security risk assessment

- Identification of the SuC
- High-Level Risk Assessment
  - Define IACS system/packages in scope
  - Define worst case threat scenarios
  - Independent layers of protection
  - Likelihood of worst case
  - Business criticality (consequence)
  - High-level risk assessment
- Partitioning into zones and conduits

Interested in assessing your OT systems’ vulnerability to security incidents? Contact sales@applied-risk.com about this case study for more information.
Initiatives Undertaken

This approach enabled Applied Risk to:

- Define, on a holistic level, the worst-case cyber threat scenario based on inputs such as the corporate risk matrix and business impact assessments.
- Define the business criticality/consequence of the worst-case scenarios (safety, environmental, financial, reputation) complemented by using relevant inputs from the safety discipline work related to HAZID and HAZOP activities.
- Describe which of the OT systems and packages that have critical functionality required to implement the safety systems and barriers and define the generic independent layers of protection for these systems.
- Define the likelihood of the worst-case scenarios (e.g. high, medium, low). The likelihood can, for example, be based on the threat agent’s capability, motivation and opportunity to exploit a threat vector. The opportunity is based on the vulnerabilities in the respective systems/packages.
- Based on previous steps, conduct a relative risk ranking of unmitigated risks relating to the SuC’s systems/packages.

Successful Impact

The risk assessment approach succeeded because it gave the company the information and the tools needed to understand and respond to the cyber risks facing the manufacturing sector using a repeatable process that the company could continue to follow. The results identified the vulnerabilities within the company’s OT systems.

The process also proved valuable because it heightened awareness of OT cybersecurity issues among those involved in the risk assessment and brought together various groups of stakeholders to develop a common understanding of the risks and challenges associated with OT cybersecurity.

Additionally, the programme brought stakeholders together to formulate a cybersecurity policy for the whole company leaving the company better off than it had been before.

Ready to align your maturity level to your business resilience requirements?

Is your organisation adjusting to the idea of being a target for cyberattacks? Are you working to identify and understand all the potential weaknesses in your OT and industrial control systems?

Talk to Applied Risk today to learn how our risk assessment programmes can help manufacturers determine what level of risk they face – and how they can reconcile the objectives of avoiding downtime and safeguarding their equipment and systems. Contact us today!