Case study

AcierTech is a manufacturing company based in Laval, Quebec, Canada. Founded in 1985, it specializes in the manufacture of steel parts for various industries, including automotive, aerospace and construction.

To meet the needs of modern industry, AcierTech has decided to implement cutting-edge technologies and adopt the principles of Industry 4.0. Industry 4.0 is a concept that aims to integrate digital technologies and cyber-physical systems into manufacturing processes to improve efficiency, productivity, and flexibility.

The implementation of Industry 4.0 will have a significant impact on AcierTech's cyber security. The convergence of information technology (IT) and operational technology (OT) creates new opportunities for cybercriminals to exploit potential vulnerabilities. Interconnected IT systems and smart devices used in Industry 4.0 can be attractive targets for malicious attacks.

Sylvestre Labouteille-Dacier, the company's CEO, is keen to understand the issues involved before embarking on this project. For example, what is the insurance impact for the company? Our partner Connectwise will be on hand to discuss Cyber insurance.

Cyber insurers are also issuing a number of prerequisites for accepting to insure companies.

These prerequisites often include IT environment hygiene, business continuity plans, incident response plans and advanced detection tools. NOVIPRO will discuss with you how to build these plans and assess your hygiene. Darktrace will explain how AI can help you to detect and respond to attacks with optimal visibility of your environment, while integrating the playbooks created in the incident response plan into their tools.

To find out how to understand the challenges of implementing technologies, meet our partner Nozomi Network, who will present frameworks for operational environments and how their solution helps to visualize and address vulnerabilities in these technologies.

Our partner Fortinet will also be on hand to talk about the importance of compliance with TO frameworks and its approach to securing these environments, as well as the benefits of the security fabric in the convergence of IT and TO networks.

The CEO appointed Cornelia Humanius, Director of Human Resources, as the person responsible for implementing C25 compliance. Cornelia is supported by NOVIPRO, their CISO and their lawyer, in complying with the law. However, she has just learned that the IT department has no capacity for data inventory. Data Sentinel will be there to talk you through this challenge.

Acera Technoplomus, the company's CTO, wants to transfer workloads to cloud computing to take advantage of SaaS services, but, like most companies, the environment will be in hybrid mode for some of the services in these local infrastructures. Our partner Zscaler will discuss with you the shared responsibility for securing cloud services.

The in-house IT team is at its minimum, and AcierTech is experiencing the same thing as all companies: it's hard to find employees, which forces the department to use a lot of external resources, just like the Operations Manager, Scadius Profibus, but for different reasons. Industrial equipment is supported and maintained by external suppliers.

Understand the risks associated with privileged access for these consultants and find out how to protect yourself with our partner Delinea.

In addition, AcierTech evaluated the possibility of setting up a dedicated cybersecurity team to constantly monitor suspicious network activity and take preventive action in the event of an imminent threat. Talk to our partner Arctic Wolf to get a true assessment of the associated costs and benefits of using Arctic Wolf's service.

The team also works closely with external cybersecurity experts to benefit from their expertise and keep abreast of the latest attack trends and techniques.

Thanks to these proactive measures, AcierTech will succeed in minimizing cybersecurity risks while reaping the benefits offered by Industry 4.0. The integration of digital technologies into manufacturing processes will enable the company to improve its operational efficiency, productivity, and competitiveness on the global market.

In conclusion, the implementation of Industry 4.0 will have a significant impact on AcierTech's cybersecurity. The company understands that it will need to take additional measures to protect its systems and sensitive data from potential threats.

However, thanks to a proactive approach and close collaboration with cybersecurity experts, AcierTech will succeed in taking advantage of the benefits offered by industry, 4.0 while maintaining a high level of IT security.

Please note that this story is fictional and does not refer to any real company. It is intended to illustrate the potential impact of Industry 4.0 and the convergence of IT and TO on cybersecurity in the manufacturing sector.