A wake-up call for manufacturers: Cyberattackers are at your door
When global aluminum producer Norsk Hydro was struck by an extensive cyberattack in the early hours of March 19, 2019, the situation escalated quickly. Within hours, the company network had to be taken down: Production in most of its 170 plants was switched to manual operations and stopped in some of them. Although Norsk Hydro responded quickly and decisively, the financial impact — of what corporate information security officer Torstein Gimnes Are called “a company crisis” — ultimately amounted to US$71 million.

Norsk Hydro’s laudable transparency affords us rare insights into the aftermath of such a security breach. But it is only one example of many such attacks in recent years, serving as a wake-up call to manufacturers everywhere that this can happen to any organization inadequately equipped to defend against cyberattacks.

Adversaries come in many forms: state-sponsored attackers, hacktivist, and those bent on corporate espionage. They can disrupt manufacturing operations or steal sensitive product design information or proprietary and differentiating production techniques. On a small scale, a successful cyberattack can affect the manufacturing organization’s reputation and financial performance. On a larger scale, cyberattacks can have a negative impact on national security and the nation’s gross domestic product (GDP).

Connected manufacturing environments increase security risks

The backbone of most manufacturing organizations is their operational technology (OT), which includes industrial control systems connected via programmable logic controllers (PLCs). These OT solutions focus on the safety of human operators and the integrity of the manufacturing equipment. Most legacy manufacturing equipment uses proprietary control system network protocols and isn’t connected to the internet, and so the industry has not put much emphasis on cybersecurity.

Historically, this air-gapped network architecture, with separation between corporate business systems and the operational and control systems on the manufacturing shop floor, was sufficient. However, as manufacturers implement more automation to improve production throughput and quality and to reduce operating costs, they are increasingly connecting equipment with surrounding processes, business systems and remote operators.

Traditional IT and OT silos that used to operate almost entirely independently have started to converge, with equipment becoming IP-enabled and connected with other enterprise network environments.

This makes it possible, for example, to consolidate and centrally operate and control manufacturing processes from remote operations centers, and removes the need for human operators to be physically located on the shop floor. And while that helps increase productivity, it also amplifies the risk that production equipment can be remotely accessed and controlled by external parties.
A striking example of the risks that convergence can introduce is the discovery of issues related to Ripple20 in common OT devices. Ripple20 is a set of 19 security vulnerabilities discovered and published by Israeli security research group JSOF in June 2020. These defects stem from a widely used software library from U.S.-based company Treck. The code, which is embedded in a wide range of automation and internet of things (IoT) devices across all industries, potentially allows a malicious attacker to remotely gain control of vulnerable devices and obtain or manipulate sensitive data on these devices.

Treck is a known and reputable company, and its shared library was used extensively in millions of products over two decades. Analysts and national advisory agencies have given the Ripple20 vulnerabilities high criticality ratings. While many automation vendors have informed customers of which products are affected, this is not true for all suppliers; in fact, the full exposure may never be fully established. Updating or replacing such products will, therefore, be a lengthy activity and leave manufacturing operations at elevated risk.

From a security perspective, IT/OT convergence and challenges like Ripple20 are driving organizations to develop a holistic and harmonized approach to security in order to deliver an optimized technology solution and reduce business risk.

But even as manufacturers struggle with this development, they must contend with the fact that their enterprise’s traditional boundaries are expanding to support the increasing globalization of manufacturing supply chains. The shift to demand-driven supply models requires manufacturers to expand their reach across a growing network of supply chain partners, business partners and consumers; all this increases risk.

**Connected devices, sensors and smart things must be secured**

To support these changes, manufacturers need a way to securely exchange data and connectivity with manufacturers, partners, consumers and connected devices. It is critical that all business-to-business connections be protected — not just with firewalls and intrusion prevention devices, but also by monitoring all traffic traversing into and out of the organization, so that anomalous network activities can be identified.

Covert activities and insider attacks can be spotted through the use of behavioral learning. By knowing which users typically access what systems at a given time, a security solution can detect unusual behavior. A cyberattack can be detected early, before it starts to have an impact on the production process.

Of course, IoT adds another wrinkle to the manufacturing security scenario, with the addition of countless new components and network-connected devices that communicate internally or externally. These smart connected devices, sensors and controllers are changing the game in manufacturing plants. For example, real-time tracking solutions for manufacturing supply chains such as DXC OmniLocation™ can improve decision making by providing new visibility into inbound materials and track-and-trace solutions for outbound finished goods. When these IoT components and devices are connected to the network, they instantly fall under the purview of the cybersecurity management process.
Today, while a number of IoT standards have been put forth, no dominant standard exists. This complicates the IoT security challenge. It is important for manufacturers to address IoT security risks and mitigate these with an enterprise-wide solution. Manufacturers should use IoT gateways and edge devices to segregate and provide layers of protection between insecure devices such as those affected by Ripple20 and the internet to help manage the overall lack of security that exists with IoT.

**Protect intellectual property**

Protecting information in a manufacturing organization is very different from protecting information in other industries. Whereas the financial, retail and healthcare industries focus on securing personally identifiable information (PII) and credit card records, the manufacturing industry needs to reduce disruption in the supply chain and protect intellectual property.

IT controls for protecting information systems are mature, ensuring confidentiality, integrity and availability. The same cannot be said for the OT domain: This is an area where manufacturing organizations need to adapt and evolve their capabilities to protect production processes from cyberattacks.

The introduction of advanced digital manufacturing applications will require next-generation solutions for monitoring both IT and OT, including sensors, networks and connectivity, and edge-oriented computing. Operating models for security management will need to be modernized and strengthened to ensure end-to-end integration, with security mandated as a prerequisite across both IT and OT domains.

Many manufacturing practices in use for years should now be deemed vulnerable and unsuitable to ensure a secure modern environment. The same is true for many IoT and OT assets, such as those including Treck’s exploitable shared libraries (which will require additional layers of protection until the equipment can be updated or replaced).

DXC Technology Security services protect some of the largest manufacturing companies in the world. Our Advisory and Managed Security Services have helped customers defend against modern-day attacks and improve and strengthen their OT security, so cyberattacks can be mitigated through preventive, detective and proactive response measures.
About the authors

Bruce Sneddon is the lead consultant/practice partner on Manufacturing for DXC Consulting in the Australia and New Zealand region. He provides industry thought leadership and vision for manufacturing and other industrial customers so they can achieve process optimization and productivity improvements through enabling technology innovation and IT-led business transformation.

TM Ching is the Security chief technology officer with DXC Technology. TM is chiefly responsible for cybersecurity thought leadership as well as research and development activities for DXC Security worldwide. In his current role, he works closely with vendors and professional bodies to identify technological evolutions or disruptions on the horizon, and develops security roadmaps for both customers and DXC Security to achieve service readiness for meeting the threat landscape changes in the next 12 to 36 months.

Frank Stoermer is the DXC Security principal, regional focal contact and subject matter expert for Manufacturing across North and Central Europe. In his work, he covers Security business and key customers in the region, positioning DXC as a trusted partner for safeguarding the convergence of industrial IoT, OT and IT in digital transformation initiatives.