Published January/February 2021 on spglobal.com/platts

FEATURE: Manufacturing faces distinct challenges in cyber risk mitigation (Part 1 of 3)

Cyberattacks on steel producers can have serious repercussions, impeding production and causing significant financial losses for targeted companies. While steel mills face unique challenges in defending their systems, successful strategies can be implemented using the right set of tools, according to cybersecurity experts.

Several steel producers were subject to cyberattacks in 2020, among them Evraz, BlueScope and Stelco, disrupting global operations.

Evraz suffered an attack in March, causing the steel producer to lose approximately 3.5 weeks of production at its North American mills, according to CFO Alexander Vasiliev, who addressed the issue in the company's second quarter earnings call.

"Our production of steel products went down by 4.7% and the main driver there was the cyberattack that we faced in March," Vasiliev said.

Since the attack, the company has instituted new cybersecurity measures including more advanced tools and increased cybersecurity training, said a company spokesman.

Australia-based BlueScope was subject to an attack in May leading to global disruptions in its business. The company said its North Star, Asian and New Zealand businesses continued operating with minor disruptions. In Australia, manufacturing and sales operations were impacted; some processes were paused while others, including steel dispatches, continued with some manual processes and workarounds, the company said following the attack.

It was the first such disruption detected in the company's US businesses and left it scrambling for remedies.

In October, Canada's Stelco fell victim to an attack that left operations temporarily suspended while countermeasures were taken to limit the scope of the incident.

A customer of the mill said he was "dumbfounded by how much the attack shut them down," crippling operations to the point the steelmaker could not melt or finish steel and were losing track of where products were. "I think they lost a month [of production]," added the source.

Another customer said he was still waiting for some of his fourth quarter shipments.

"Cyberattacks are extremely prevalent," said a chief information security officer (CISO) in the steel industry. "You can see them in the news every day on small and large scales and these are just the ones that are being shared publicly."

One major North American steel buyer said he was surprised by how many attacks have occurred on smaller customers. "More and more customers we talk to so many people have gone through the same thing. But they just pay the ransom and get it over with," said the buyer.

Published January/February 2021 on spglobal.com/platts

FEATURE: Steel mills have unique challenges, vulnerabilities to cyberattacks (Part 2 of 3)

Historically, critical infrastructure systems like steel mills have had distinct vulnerabilities due to being purpose-built systems, designed to run with very little variation, according to Mark Fabro, president and chief security scientist at Lofty Perch, a consulting firm focused specifically on operational technology and industrial controls systems for cybersecurity.

In the past, cybersecurity was not a component of the build specifications or the procurement process. The risk of an attack was limited to anyone with physical access to the plant, creating opportunity for physical damage, malicious operation of the system or the introduction of malware via removable media, according to Fabro.

"Fast forward to where we are now, and those systems that were traditionally protected through isolation are now connected to back office, to the supply chain, to the vendors," Fabro said. "Those systems are now networked to a wide range of external systems, making it hard to delineate the extent of the interconnected systems. The challenge becomes accurately defining and securing the extent of the business-critical information infrastructure, and this is where new attack vectors can originate."

While cybersecurity measures can be implemented by steel mills, the older systems can pose additional problems. The last new blast furnace in the US was built more than half century ago.

A steel industry chief information security officer (CISO) said threat actors will look for "vulnerabilities in the software and work to exploit them. The manufacturing industry is often dealing with extremely expensive control systems that were either not designed with security in mind or are difficult to keep updated due to operating schedules."

The end goal will always be mitigating all vulnerability but that can be untenable, so asset owners need to think about consequence-based analysis, according to Fabro.

"Understanding the realistic cyber risk of manufacturing infrastructure needs to be done from the perspective of cyber-informed engineering, in order to understand how the uniqueness of manufacturing environments change the attacker's landscape of opportunity," he added.

The manufacturing industry has been slow to adopt appropriate cybersecurity measures, according to the steel industry CISO: "Financial organizations, for example, have had regulations for years requiring a focus on securing their data and systems, whereas in manufacturing it has been a choice to secure their systems."

Published January/February 2021 on spglobal.com/platts

FEATURE: Cyber-informed engineering perspective needed for cyber-defense (Part 3 of 3)

In order to effectively and efficiently protect assets from a cyberattack, companies need to go beyond IT security and evaluate cyber risk from a cyber-informed engineering perspective, according to a security specialist with a focus on manufacturing.

Mark Fabro, president and chief security scientist at cybersecurity consulting firm Lofty Perch, said that despite the disadvantages inherent to purpose-built systems like steel mills, the expected and deterministic behavior of the system can also be an advantage when developing cybersecurity measures.

"Interestingly, critical infrastructure and manufacturing have an advantage in doing consequence-driven cyber-informed engineering to narrow down the specific cases that are important to them. Cyber-informed engineering has significant value in defending these types of systems," Fabro said.

For organizations with a network of mills, Fabro recommended implementing a defense-in-depth strategy in and among company assets. A plant existing on its own separate network may reduce the opportunity an attacker has to move laterally within a particular network, but security must be implemented to account for an adversary with local access at a facility and the risk associated with removable media and transient devices.

Separate networks are a good idea, but the separation must be enforced with effective access control, anomaly detection and up-to-date security policies and procedures that enforce security at a corporate and programmatic level, according to Fabro.

A steel industry chief information security officer (CISO) also highlighted the need to implement defense-in-depth strategies in the steel industry.

"Recent events, including the growing prevalence of ransomware, have made this a priority for manufacturing and steel companies," the source said. "For any industry, including steel, there is no silver bullet. You have to apply defense-in-depth strategies to protect your network. The steel industry needs to know that this risk is not going away and is only going to grow, so we need to make cybersecurity a priority where it isn't already."