The Problem: Ransomware Attacks in the Industry Prompt Tough Questions From the Board About ICS Security Posture

As a global manufacturer with a long history of innovation, this company recently embarked on a key business initiative to implement digital transformation across its 150 plants worldwide, with the goal of improving safety and efficiency while reducing costs. In fact, by digitizing its manufacturing processes, the company has now seen up to 30 percent productivity gains.

At the same time, the increased IT/OT connectivity and deployment of unmanaged IIoT devices has also introduced a larger attack surface, and therefore greater risk.

Within that context, the IT security team at this F500 manufacturer were seeing signs that the ICS threat landscape was changing, and fast. They knew that sensitive trade secrets had been stolen from competitors, and that destructive ransomware had shut down production in competitors' plants.

So, the Global Director of Manufacturing Technology gave the engineers a green light to begin testing an agentless, non-invasive IoT/ICS security solution.

The team heard through industry peers that CyberX offered a passive solution that could protect them from ICS threats.

So they began to put the product through its paces. The Director of Manufacturing Technology reports that “the asset and network map that CyberX generated in the first hour was even more valuable than the initial protection it provided.”

Why? Before CyberX, the IT team couldn’t see past the network switches. Once CyberX was installed, the Global Director saw what he called the “*#%* network mess that was going on down there.”

What kinds of problems were brought to light? “All kinds of nonsense started showing up. We saw connections from the ICS networks to Google, ESPN, Microsoft – everything that engineers were doing in their spare time. We even saw a connection to a neighbor’s open WiFi.”

In the meantime, someone on the Board of Directors sat on the board of another industrial company that had just been compromised. Suddenly, the ICS security project gained additional urgency. Budget was procured and CyberX was licensed for an initial deployment of 8 sites worldwide.

The Solution: Visibility in IoT & ICS Networks

CyberX was deployed in a few weeks, after which the manufacturer began to use CyberX to edit passive vulnerability assessments on different plants so they could focus on the ones that exhibited the most risk.

CyberX’s automated vulnerability assessment generates an objective security score that can be measured over time to track continuous improvement. The manufacturer quickly learned that plants with knowledgeable and conscientious controls engineers received excellent security scores — in the 90s (out of 100) — and those scores stayed at their high levels over time.

Other plants required more help. The mitigations that CyberX recommended required new levels of cooperation between IT and OT, and the OT teams were understandably reluctant to change until they understood why they were being asked to change. In most cases, a discussion of the relationship between vulnerabilities and the likelihood of an attack — resulting in plant downtime — was enough to convince the OT engineers that a change was needed.

CyberX also provides an automated IoT/ICS threat modeling capability that predicts and visualizes the most likely paths an attacker would take to compromise “crown jewel” assets, and the attack vector diagrams it produces were also very helpful in explaining the risk to non-security personnel.

Plants that didn’t already have DMZs quickly established them in their networks, providing an additional layer of isolation between IT and OT. Connections to external networks were systematically snipped. Engineers were told that it’s a violation of corporate policy to connect laptops to the Process Control Network. Any connections from home offices were mandated to require VPNs.

CyberX is now deployed in plants worldwide, as well as the CyberX Central Manager which is deployed in the company’s SOC. All alerts are forwarded to the company’s SOC where they are viewed, investigated, and tracked in Splunk.

The Benefits:

Proof of the benefits that CyberX provides came a few months after the initial CyberX deployment. At one of the plants in China, CyberX alerted that IP addresses were showing up that hadn’t been seen before. As the Director recalls, “Our IT security team could not identify the IPs, so we went into intrusion mode. We started closing things down.”

As it turned out, the IT security team in China was performing a red-team exercise and hadn’t informed the Global Team. CyberX discovered the intrusion and as a result of the “exercise” there now exists a greater level of coordination and cooperation not only between IT security and OT but also between international offices and plants.

CyberX brought some of the deficiencies in network architecture to light. For instance, prior to installing CyberX the control engineers believed that the process control system was air-gapped. CyberX revealed connections between plants and prompted the engineers to address the issue by laying dedicated fiber between the plants.

Summary of CyberX Benefits

The company now enjoys full visibility into their OT network just as they do for their IT network, enabling them to immediately spot suspicious or unauthorized activities that indicate an adversary may have compromised the network.

This enables the Company to reduce the risk of production outages that could cost this manufacturer tens of millions of dollars. It also reduces the risk of catastrophic safety failures and environmental incidents.

In particular, the Company now enjoys benefits in each of these areas:

Asset Discovery
They continuously see what devices they have, how they're connected, and how they're communicating with each other.

Risk & Vulnerability Management
They now have a complete, up-to-date list of all network and device vulnerabilities and a prioritized to-do list for mitigating those vulnerabilities — based on risk to their most important "crown jewel" assets.

Continuous Threat Detection & Response
CyberX continuously monitors the company's OT network and generates real-time alerts for anomalies such as new devices being plugged into the network, unauthorized programming changes to Programmable Logic Devices (PLCs), destructive malware such as EternalBlue, and cyber reconnaissance activities such as network scanning. CyberX is the only industrial cybersecurity company to have been awarded a patent for its innovative, ICS-aware threat detection analytics and machine learning technology.

Unified IT/OT Security Monitoring and Governance via SOC Integration
Real-time information from CyberX is integrated with the company's SOC via their SIEM, enabling the company to leverage their existing investments in people, training, runbooks, and workflows.

This unified approach to IT/OT security monitoring and governance enables the company to leverage scarce resources across both IT and OT, and more effectively combat advanced threats that often cross IT/OT boundaries.

The company has also held SOC Integration workshops to break down organizational silos between IT and OT, and to help the teams better understand and communicate with each other.

Streamlined Compliance
CyberX has also helped the company streamline its compliance and internal audit reporting. Activities that were previously performed manually, such as collecting and reporting on asset inventory information, are now automated and as a result happen more frequently and more quickly.

Centralized Command-and-Control

Perhaps most importantly, the engineers and analysts at the company now have centralized command-and-control over their OT networks. They not only see their current network topology and all activity, they can take action to make their network more efficient. They not only see anomalous traffic but hunt down anomalies and take corrective measures. And they not only spot intrusions and malware, they implement firewall and NAC policies to block or quarantine malicious hosts.

CyberX is providing defense-in-depth via continuous IoT/ICS asset management, risk and vulnerability management, and continuous threat monitoring — along with a unified approach to IT/OT security monitoring and governance.

In summary, CyberX is now an essential part of ensuring that this F500 chemical manufacturer is optimizing its security posture as well as its manufacturing operations.