HSB

A Munich Re company

Cyberattacks

Are operational technology (OT) systems a hacker's next target?

HSB, a Munich Re company, is a technology-driven company built on a foundation of specialty insurance, engineering, and technology, all working together to drive innovation in a modern world.

Now that everyone understands the risks and impacts of cyberattacks on information technology (IT) systems, is there another risk associated with operational technology (OT) systems? To answer this question, we need to understand what OT systems do and what would be the reason for such an attack. On the IT side, there is financial, personal, business-related intellectual property (IP), and other critical business data that if compromised, could be leveraged to extract ransom payments, business concessions, or to incur damage to the compromised business.

What does the OT system do?

Instead of financial, personal, or business-related IP data, the OT side controls machines, processes, and formulas that are unique to that business, including the IT systems. OT systems can be divided into common systems and industry-specific systems.

Common systems support various functions like heating, ventilating, and air conditioning (HVAC), elevators/escalators, lighting, fire, security access, and other common functions such as mail.

Industry-specific systems support the machinery specific to the business that includes equipment such as turbines, ovens, conveyers, switches, pumps, transformers, and HVAC equipment specific to the business entity.

What is the impact of an OT system cyberattack?

The first identified reason for attacking the OT system is that such an attack could bring the business, or at least a major business function, to a halt. This type of attack could be the result of a ransomware attack, where the systems are encrypted, or a code attack, where code corruption will halt the operation.

Halting the business, or a major business function, would be a catastrophic event. Every business is susceptible to a major impact due to an OT attack, even if it is just changing the heating/air conditioning, stopping the elevators, or removing employee access to the building. Recovery would be similar to an IT attack where the OT systems would need to be recovered from the last backup.

The second reason for such an attack would be to damage the environment or the equipment being controlled. This type of attack would entail accessing the OT system and modifying the operating characteristics of the controlled equipment. Changing these settings could result in the machinery going out of specification, such as freezers functioning above 32 degrees F, or it could cause a machine to fail. If OT systems are like IT systems, why aren't OT system attacks more common? A review of OT systems history may shed some light on this question.

OT system development influences risk

Like IT systems, OT systems started as separate isolated systems, usually supporting a specific machine or vendor, like an elevator or air conditioning unit. Vendors included companies such as Siemens, Honeywell, Carrier, Otis, Dayton, etc., as compared to IT vendors such as IBM, HP, Dell, and Oracle. Initially, these OT vendors created application programming interfaces (APIs) to allow these systems to communicate from a control point of view and consolidate alerts. Over time, OT vendors created common interfaces supporting network interconnection and operator access.

Interconnected OT systems have trailed IT systems mainly because of the useful life of the equipment being controlled. IT systems have a useful life of five to seven years, whereas OT system have a useful life of 20 to 40 years, or longer. This means that for each new generation of OT systems, the IT side has already progressed four to six generations. Just like IT systems, although interconnected OT systems provide efficiency and ease of use, they also introduce significant risk.

OT systems are also being "opened up" to support analytical tools, such as digital twins, as well as linkage to sensor systems to identify maintenance requirements and predict failures. Since OT systems have not progressed as fast as IT systems, the underlying application code supporting Process Control Systems (PCS) is still very vendor specific, which is one of the reasons that OT system attacks are less common today.

Best practices for OT systems

Many best practices in the OT world are like those in the IT arena, such as identity management, firewalls, encryption, and access controls. The risks on the OT systems are different than those on the IT systems, and contrary to IT systems, where the main control point is the data, OT system vulnerabilities rest in controlling the supported machinery. Several industries are also controlled by regulations that dictate OT requirements such as:

- Strict "air gap" between OT and IT systems
- No remote access to Supervisory Control and Data Acquisition (SCADA) systems
- No Remote Terminal Support (RTS)

While these regulations are good for all companies, many companies cannot support the added cost of local operators. Companies utilizing these functions should be extra vigilant in how they design, control, and manage these interfaces.

Cyberattack risk rising for OT systems

While cyberattacks on OT systems are not as frequent as those impacting IT systems, we anticipate that they will become more frequent. As more companies refuse to pay ransom requests, we are already seeing acts of revenge against the IT systems, such as data destruction and data compromise. As hackers become more sophisticated, attacks against the OT systems could be more devastating and could become a new source of ransom.

HSB
One State Street
P.O. Box 5024
Hartford, CT 06102-5024
Tel: (800) 472-1866

HSB.com