Brown & Brown

PROPERTY & CASUALTY

Securing the Heart of Industry: Protecting OT

Authored by Salman Ansari and Christopher Keegan

Despite a lull in 2022, the recent increases in ransomware attacks have prompted organizations to commit additional resources to protect IT networks. The interruption of Information Technology (IT) computer systems often receives significant focus across all industries, however, attacks targeting manufacturers and their underlying Operational Technology (OT) systems are steadily increasing.

Attacks upon process manufacturing, discrete manufacturing and critical industrial infrastructures have physical consequences that transitioned a theoretical problem during the last decade to a real threat today. In 2022, these attacks increased 140% over the previous year and impacted over 150 industrial operations, calling for additional security and coverage.[1]

Convergence of IT & OT

This year, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued advisories regarding 49 vulnerabilities in eight industrial control systems (ICS) used by organizations in multiple critical infrastructure sectors in one month. The CISA advisories coincided with a report from the European Union on threats to the transportation sector that warned of the potential for ransomware attacks on OT systems used by aviation, maritime, railway and road transport agencies.

Many OT networks are outside of the purview of the traditional IT Security umbrella and are often the responsibility of plant engineers who apply security controls outside of standardization. These systems are typically older and inherently vulnerable due to outdated code that did not initially employ security-by-design principles.

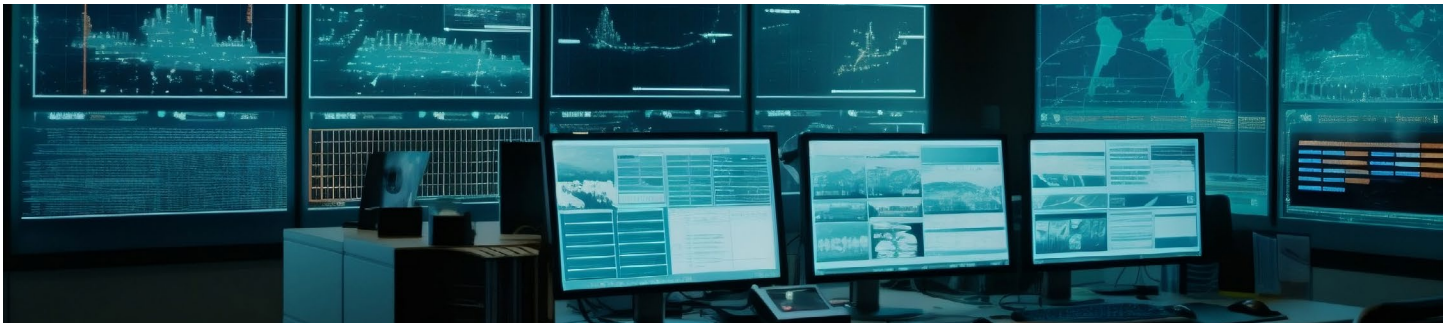
Possible Impacts of an OT Cyberattack

Business Interruption & Reputational Harm

In August 2023, Clorox disclosed in an SEC 8-K filing that it detected unauthorized activity on its systems. Clorox described the cyberattack as “material” and stated that the impact would be reflected in Q1 financial results. The cyberattack caused disruption to the company’s production capacity, triggered product outages at retailers, and disrupted order processing and supply chain operations. It took more than one month for Clorox to normalize operations. The decrease in Clorox’s net sales due to the cyber-attack is estimated to be around $500M, which the company estimated to be a decrease of 23 – 28% from the same quarter in the previous year.

Some businesses have not been able to recover from cyberattack losses. In late 2022, Prophete, a German bicycle manufacturing business, was compromised for over

[1] *Waterfall, 2023 Threat Report*



three weeks, during which no production could occur. The company inevitably had to declare bankruptcy after a $50M loss in sales.

Insurance. Insurance buyers can look for coverage under cyber and property policies, which have incorporated coverage for cyber-caused business interruption. Cyber insurance targets this exposure broadly with significant limits available in addition to cover for reputational harm.

Impacts of an OT Attack

- Lost revenue
- Liability for third-party damage
- Liability for injury to persons
- Direct injury to property
- Pollution
- Machinery replacement
- System upgrades
- Forensics costs

Physical Asset Replacement

Recent malware can infect the core hardware infrastructure and result in "bricking," which requires the replacement of hardware, software, reconfigurations, integrations to OT systems and expedited shipping costs for replacement systems. In 2012, a malware called Shamoon wiped out more than 50,000 hard drives at Saudi Aramco, costing millions to expedite replacements.

Insurance. Physical asset replacement is likely to only come from a cyber insurance policy. Replacement of "computer equipment" is now common in these programs, but it is important to review the "betterment" provisions for full reimbursement of equivalent systems.

Property Damage / Human Injury

Targeted attacks can mirror the normal operations of ICS and SCADA systems while manipulating physical assets to dangerous levels. In simple terms, hackers hide activities so that machinery controls and monitoring systems do not alert companies to an attack in progress.

Insurance. Direct property damage can be covered under property and cyber policies. Care should be taken when negotiating property exclusions and coverages, as some do not allow cover after a cyber-attack. Liability from third-party property and bodily damage claims can be covered under GL policy, provided special cyber-specific exclusions are not added. Cyber policies will cover direct property damage under specific programs or policy extensions by a limited number of markets.

Contamination / Pollution

Manufacturing, utility, pharmaceutical and energy companies often use chemicals and materials for a specific purpose and require remanufacturing if the process is

interrupted. Attacks on municipal water treatment plants have brought attention to the risk of cyber incidents to public utilities leading entities who store harmful chemical's to the conclusion that attacks on facilities could result on large pollution claims

Insurance. Cyber and environmental policies can cover both direct contamination and pollution costs. Environmental policies may be a more comprehensive vehicle for cyber-caused environmental damage but are viewed as discretionary purchases. Cyber policies can provide coverage only with specially requested endorsements and a lengthy underwriting process.

Specific terms in insurance programs can be critical to whether recovery can be made when faced with an OT cyberattack. Property policies can limit recovery to only specifically targeted attacks and have been contentious where the attack appeared to have come from a foreign adversary by applying war exclusions. To help effectively prepare against OT exposures, cyber insurance policies might require specific endorsements for certain terms, such as replacing OT hardware or voluntary takedown of systems to avoid further damage.

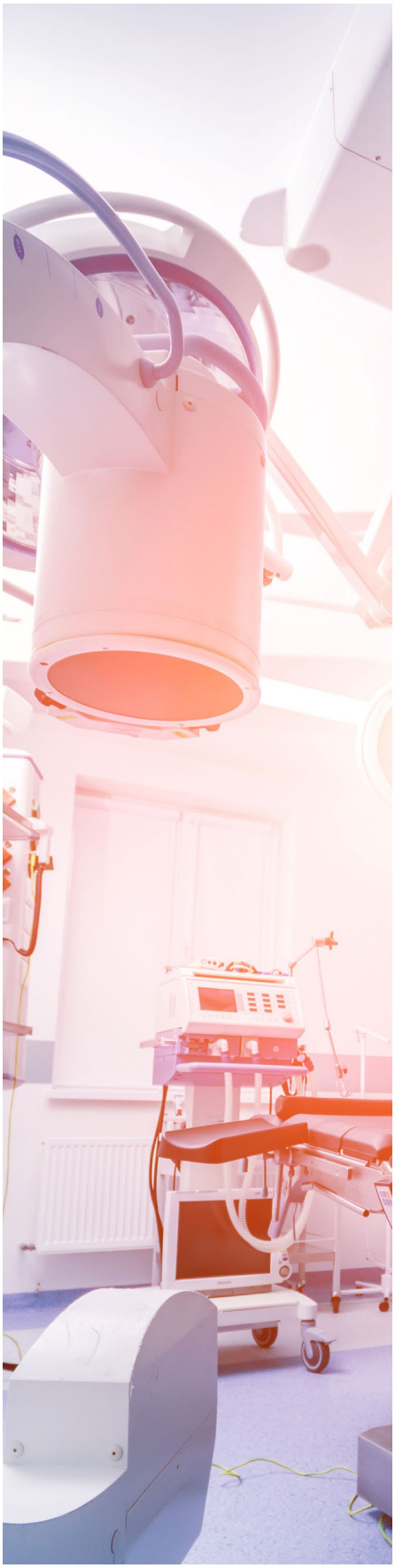
Cyber Insurance Coverage for OT

Cyber insurers' appetite for OT exposures is cautiously expanding. To assess companies' OT risk and relative cyber insurance coverage Brown & Brown recommends an analysis of the exposure, including an in-depth understanding of the OT environment and its vulnerabilities. Threat and financial loss modeling can help companies understand the nature of the risk and the potential business interruption impact. Analyzing potential costs from specific scenarios can round out the assessment, providing an estimate aligned with each company's risk appetite.

How Brown & Brown Can Help

Brown & Brown's modeling and assessment services take an integrated approach – combining a deep dive evaluation of your cyber and operational controls and resilience with business interruption risk quantification that leverages our insurance industry and actuarial experience. We align our actuarial, analytical, and technical IT security services and resources within our brokerage teams to develop tailored critical risk assessments and solutions for the individual needs of our customers. We have advanced experience and insight in cyber risk quantification to enable our customers to translate cyber risk into projected financial loss scenarios and make informed cyber risk management decisions. Our Cyber In-Site technology platform can provide a cyber risk view for risk management, CIOs, CISOs and board members.

Please contact your Brown & Brown representative or a member of our Cyber leadership team if you are interested in better understanding the risk exposure of an OT attack on your company.



How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

Find Your Solution at BBrown.com