Brown & Brown

CYBER WHITE PAPER

Operational Technology: The New IT Risk

AUTHORED BY:

Chris Keegan
Sr. Managing Director, Cyber & Technology
National Practice at Brown & Brown

Oren Wortman
Managing Director, Cyber & Technology
National Practice at Brown & Brown

Operational Technology: The New IT Risk

Colonial Pipeline is just one recent example. The rise of ransomware has organizations rapidly committing resources to protect IT networks in the event of a cyberattack.

While much of the focus has been on the interruption of computer systems, which affects all industries, there has been an increasing number of attacks targeting manufacturers and their underlying Operational Technology (OT) systems. The attack on Colonial Pipeline resulting in the pipeline being taken offline is just one recent example. While the Colonial ransomware incident did not directly affect its OT systems, they were forced to be taken offline out of an abundance of caution, disrupting gas supply all along the East coast. A cyber insurance policy with certain key amendments may be effective at responding to these types of attacks.

Operational Technology (OT)

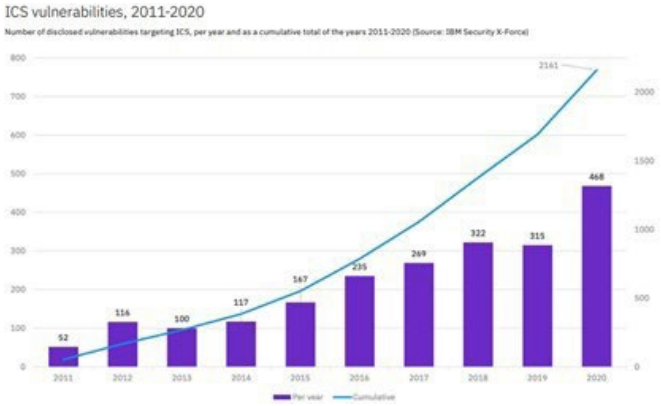
Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes and events. Examples include industrial control systems, building management systems, fire control systems and physical access control mechanisms.

https://csrc.nist.gov/glossary/term/operational_technology

Convergence of IT & OT

The injection of computer technology into the operational process has provided opportunities for organizations that manufacture goods, operate machinery and manage infrastructure to centralize and streamline the control and monitoring of manufacturing systems at a wide scale.

Colonial uses pressure sensors, thermostats, valves and pumps to monitor and control the flow of diesel, petrol and jet fuel across hundreds of miles of piping, all connected to a centralized management network. Historically, OT systems have been disconnected from corporate networks and the public internet, and instead, run on a dedicated network segregated from corporate IT environments. With the historical segmentation of environments, compromises of OT environments required a person's physical presence to infect and damage an organization's OT equipment.



Today's OT environments have evolved, allowing connectivity through corporate IT and internet-facing networks, providing organizations with the ability to control, operate and oversee multiple facilities remotely. However, the modernization of manufacturing and control systems may come with a security cost. As organizations become more aware of the risks of internet-facing networks, it is important to fully identify all the OT "Crown Jewels" that now need to be protected. This expanded attack surface and the exposing of legacy OT systems challenge even the best business continuity plans and place the very systems that increase productivity at risk. According to IBM X-Force, ICS vulnerabilities increased by 49% from 2019 to 2020.[1]

IT security has historically focused on the protection of data and computer software and hardware. Many users (employees) with varying levels of access to the data and hardware can share information and operate, protected under a company's IT security controls. Most OT networks are outside of the purview of the traditional IT Security umbrella and are often the responsibility of plant engineers who may apply security controls in a non-standardized manner. These systems are typically older and inherently vulnerable because they incorporate outdated code that did not initially employ security-by-design principles. Cyber Insurance can provide organizations with additional protections when developing an OT cyber risk mitigation plan.

1 https://www.ibm.com/security/data-breach/threat-intelligence

Possible Impacts of an OT Cyber Attack

Business Interruption & Reputational Harm

In January 2021, a paper and packaging company, WestRock Company, was infected by malware crippling their IT network and infecting the OT environment, shutting its operations for more than four weeks. The incident caused production loss leading to delays in shipping goods and distrust in the organization's ability to meet goals. Westrock's incident caused a stock drop, which at one point fell 11%.[1]

Insurance. Check for coverage under cyber, property and K&R policies, all of which have incorporated cover for cyber Business Interruption.Cyber coverage is most likely to cover this risk broadly with significant limits and may add cover for reputational harm.

Physical Asset Replacement

Recent malware is known to infect the core infrastructure of hardware and can result in "bricking." The result can require replacing hardware, restoring software, updating configurations, integrating OT systems and expediting shipping costs. In 2012, malware called Shamoon wiped out more than 50,000 hard drives at Saudi Aramco, costing millions to expedite the replacement.[2]

Insurance. When the impact is from a "non-physical" cyberattack, physical asset replacement is only likely to come from a cyber policy. Replacement of "computer equipment" is now common, though care needs to be taken over costs of replacement or "betterment" provisions to ensure full reimbursement. Replacement of OT hardware is not standard and should be specially added to the policy.

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 a business to an attack in progress.

Insurance. Direct property damage can be covered under property and cyber policies. Care should be taken when negotiating recently issued "silent cyber" instigated property exclusions as some do not allow cover after a cyberattack. 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 provided specific endorsements are added and coverage is coordinated between coverages.

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

1 https://www.ibm.com/security/data-breach/threat- intelligence

2 https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html

Contamination / Pollution

Manufacturing, utility and energy companies often operate using chemicals and materials meant for a specific purpose. Recent attacks on municipal water treatment plants have brought attention to the risk of cyber incidents to public utilities.[1]

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

Broadly, specific terms in cyber programs and traditional programs can be critical to whether recovery can be made when faced with an OT cyberattack. Property policies can limit recovery only to specifically targeted attacks and have been contentious where the attack appeared to have come from a foreign adversary by applying the war exclusion. To be effective against OT exposures, cyber insurance policies might require a specific endorsement for terms such as replacement of OT hardware and voluntary takedown of systems to avoid further damage. These are just two of many applicable nuances.

Industries at Risk

- Manufacturing
- Health Care
- Industrial Utilities
- Energy
- Logistics
- Construction
- Mining
- Real Estate

1 https://news.bloomberglaw.com/us-law-week/water-plant-cyberattack-raises-critical-infrastructure-concerns

Cyber Insurance Coverage for OT

With regulators focusing on confirming that coverage should either be affirmative or affirmatively excluded, property and GL policies have been limiting their coverage (or entirely excluding it) at the same time as cyber insurance markets have been expanding coverage. With the cyber market currently battling significant claims from ransomware, the time for expansion may be limited.

To best assess companies' OT risk and relative cyber insurance coverage, we recommend a complete analysis of the exposure, which requires an in-depth understanding of your specific technology environment and its vulnerabilities. We also suggest threat modeling to understand the nature of the risk, an insurance business interruption and expense analysis, and predictive analysis of potential liabilities from company-specific scenarios, all tightly aligned with IT security controls.

Brown & Brown's modeling and assessment services are delivered with an integrated approach – combining a deep dive evaluation of your cyber and operational controls and resilience with business interruption risk quantification leveraging our insurance industry and actuarial knowledge. Our objective is to provide customers with an economic basis for efficient risk treatment to help protect company assets and profitability.

Please reach out to 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.

About the Authors

Chris Keegan

Sr. Managing Director, Cyber & Technology National Practice at Brown & Brown

Chris Keegan leads the Brown & Brown Cyber and Technology Practice and places network, privacy, technology and media E&O insurance for companies in a variety of industries, including financial institutions, authentication providers, manufacturers, health care, retail and telecommunications companies. He has also executed cyber information risk assessment projects and worked with regulators on evaluation of E-Business risks.
He can be reached via email at ckeegan@beechercarlson.com.

Oren Wortman

Managing Director, Cyber & Technology National Practice at Brown & Brown

Oren Wortman leads the Brown & Brown Cyber Advisory team, helping customers better understand their maturity and risk exposures and helping enable them to make quantifiable and fact-based decisions relative to cyber risk treatment. His specialty is in information security, technology and cyber risk management, conducting cyber maturity and regulatory assessments, governance, and overall security program development.
He can be reached via email at owortman@beechercarlson.com.

Brown & Brown

Find Your Solution at BBrown.com