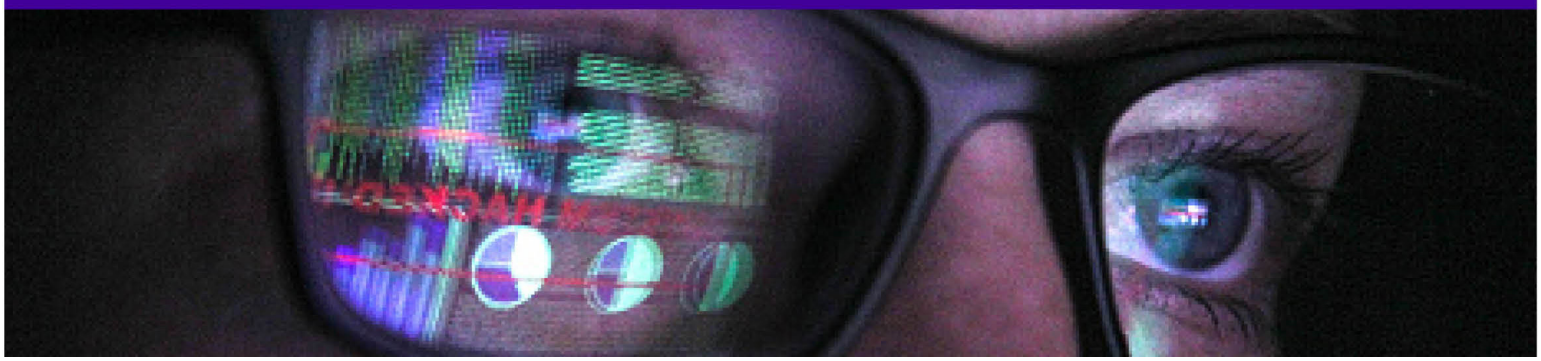
CYBER LOSS NEWSLETTER

Q2 2021 Issue



This document is intended to provide general observations with regards to cyber losses of FM Global clients and in the industry and identify notable cyber loss trends and/or representative samples of the types of losses occurring.

DISRUPTION DOES NOT ALWAYS MEAN INFECTION

On May 7, 2021, public reports emerged that a ransomware incident had struck Colonial Pipeline's Information Technology (IT) environment. Colonial Pipeline is a midstream oil and natural gas (ONG) pipeline and storage company based in Alpharetta, Georgia, USA that transfers refined petroleum products between downstream refining facilities to storage sites and refining facilities located on the East Coast. Out of an abundance of caution, Colonial operators temporarily halted OT (Operational Technology) systems, suspending delivery of oil through its pipelines to its many clients. This action caused gas prices to rise in many states due to anticipated supply shortages.

As IT and OT environments become more connected, the potential for operational or manufacturing disruption grows, whether a malware infection spreads into the OT environment or not.

THE INHERENT RISK OF OT ENVIRONMENTS

The OT environment is where Industrial Control Systems (ICS) reside. ICS are the digital systems and controls that manage physical machinery and processes. ICS environments focus primarily on production, so there is a limited set of IT security systems to monitor and protect the environment. Network connections and systems within the ICS environment are dedicated solely to the management of production systems rather than monitoring for threats. As a result, if a malware infection begins in an organization's *corporate* IT network, the organization may find it difficult to understand how the infection could affect the OT environment. Colonial Pipeline might have struggled with this determination.

KEY POINTS

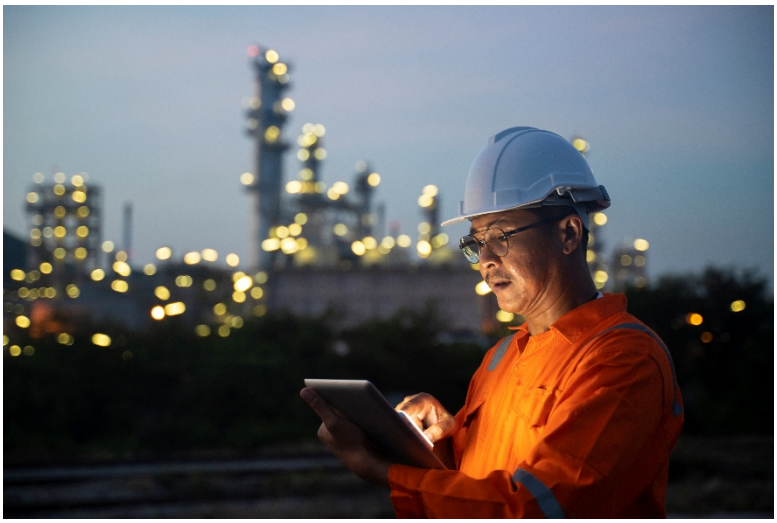
- Cyber attacks in 2021 **are increasingly affecting operational technology (OT) systems,** where Industrial Control Systems (ICS) reside
- Inherent limited visibility into OT systems means without proper preparation **the response can disrupt operations as much as the malware itself can**
- Holistic cyber risk assessment is key to mitigating loss

To determine if its OT/ICS environment had been infected, Colonial Pipeline halted most of its pipeline transportation of gasoline. However, taking this time to determine the impact of the ransomware infection created a business and supply interruption to clients. Initial indications show the ransomware did not spread into the ICS environment. Nonetheless, to be certain, Colonial Pipeline drastically scaled back production to conclude this initial assessment.

> "[Colonial Pipeline] said it had shut the pipeline itself, a precautionary act, apparently for fear that the hackers might have obtained information that would enable them to attack susceptible parts of the pipeline."

New York Times, "Cyberattack Forces a Shutdown of a Top U.S. Pipeline," May 8, 2021

KEY STARTING POINT: RISK ASSESSMENT OF ICS AND CORPORATE IT ENVIRONMENTS



The majority of cyber disruptions are preventable, and the path to prevention starts with a holistic understanding of an organization's cyber risk. A thorough assessment of corporate IT and ICS environments can help identify vulnerabilities proactively. Only when an adequate understanding of the risk is achieved can an organization develop action plans to help mitigate the risk where appropriate. Proactive risk mitigation can close gaps, reduce cyber threats and maintain cyber hygiene–just as regular operational maintenance activities keep plants continually running.

For Colonial Pipeline, better risk assessment of both its Corporate IT and OT/ICS environments might have revealed potential improvements in both environments. Gaps in their corporate environment could have been identified and closed, possibly preventing the initial ransomware infection. Moreover, further recommendations to enable logical separation between their Corporate IT and ICS environments could have provided them with confidence and assurance that the malware could not have spread into the ICS environment. The creation of a buffer zone, also known as a "demilitarized zone" (DMZ), could also mitigate the risk of infections spreading to ICS environments. These controls could reduce or eliminate production interruptions.

FM Global's Cyber Risk Assessment can identify potential risks across both IT and OT environments through our industrial control systems, physical security, and information security evaluations. Together, these components provide a unique and holistic view for managing cyber risk. Contact your FM Global client service team or AFM account team to learn more about how our Cyber Risk Assessment can help you protect your company from cyber threats in this rapidly evolving environment.

https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

