Ransomware Crisis: 11 Actions to Avoid a Ransomware Attack by Securing Critical Infrastructure

Why Securing our Critical Infrastructure Matters

Operational Technology (OT) remains a key, but vulnerable technology for organisations with critical infrastructure. The Australian Government has defined critical infrastructure as “those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia’s ability to conduct national defence and ensure national security”.

OT systems are crucial components in producing and delivering many of the resources that we rely on daily, such as clean water, fuel and electricity. Other Industrial Control Systems (ICS) provide necessary services such as traffic light systems, automotive plants and waste management facilities. Despite the societal importance and reliability of these systems, OT infrastructure remains insecure and vulnerable to cyberattacks that can cause physical harm to the public or interrupt the delivery of critical services.

Organisations operating critical infrastructure can mitigate the impact of security incidents and increase the resiliency of their OT infrastructure by following some key components of basic cybersecurity hygiene.

The Colonial Pipeline Ransomware Attack

Colonial Pipeline is a fuel pipeline company located just north of Atlanta, Georgia responsible for providing approximately 45 percent of the gasoline supply to the east coast of the United States.

On May 9, 2021, Colonial Pipeline released a statement acknowledging that they were a victim of data theft and ransomware attacks affecting their IT environment. Multiple news outlets reported that on May 7, the hacker group being called “Darkside” infiltrated the Colonial Pipeline network and stole over 100 Gigabytes of proprietary data.

Upon confirming the May 7 incident was a ransomware attack, Colonial Pipeline immediately shut down a portion of its systems and remained offline until May 12 to both contain the attack and to protect the safety and security of its pipelines and the safety of the general public. Colonial Pipeline has engaged law enforcement including the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). The Cybersecurity and Infrastructure Security Agency (CISA) and the FBI released a statement on May 11 indicating that at this point in time, there is no evidence showing any lateral movement to Colonial Pipeline OT network.

The impact of this incident and other recent attacks with elevated impact, has elicited action from the Biden administration to produce an executive order issued May 12 to improve the nation’s cybersecurity.

In addition to the operational cost associated with a pipeline shutdown, according to Bloomberg, Colonial also paid the hackers nearly $5 million in ransom within hours of the attack in order to restore its disabled computer network.

The question ICS / OT asset owners need to be asking today is what actions can be taken immediately in the short term, to mitigate cybersecurity risks to their critical infrastructure while long-term protective controls can be implemented (or assessed) for effectiveness. Here are some key short and long-term steps that critical infrastructure controls systems operators can take to mitigate the impact of a cyberattack:

Short-Term Steps Organisations Can Take

- Broadly assess the potential cybersecurity risks which jeopardise operational resiliency and affect ongoing business operations.

- Implement a robust network segmentation to minimise the impact of a cybersecurity attack on an organisation's critical infrastructure.
- Ensure a backup and recovery programme is implemented, evaluated, and isolated from the production network.
- Secure remote access gateways and publicly available services. Validate that critical infrastructure assets are not exposed to the public internet. Ensure that all remote access and external access requires multi-factor authentication.
- Update Incident Response Plans, Business Continuity Plans, and Disaster Recovery Plans for all environments and ensure playbooks address potential impacts to critical infrastructure.
- Validate full coverage of security monitoring via Endpoint Detection / Response (EDR) products on endpoints and passive monitoring on the network with Network Detection / Response (NDR).

Strategic, Long-Term Steps Organisations Can Take

- Identify and backup critical project files to offline storage.
- Test and simulate your incident response plan via tabletop exercises and determine your organisation's response to ransomware operators.
- Implement manual override controls and alarms which permit operators to detect and override any unsafe commands sent to sensors or actuators.
- Invest in asset management to identify and validate the existing IT and OT technology devices throughout the organisation.
- Develop threat hunting capabilities to proactively search for potential security incidents within the OT environment.

It is an unfortunate reality that ransomware attacks and cybersecurity incidents impacting critical infrastructure appear to be on the rise. Therefore, it is imperative that organisations start reviewing and testing their response capabilities and procedures before an incident occurs. We will continue to monitor the defenses listed above and continue to provide guidance to bolster the strategic approach organisations can take to improve their cybersecurity posture and ransomware detection and prevention capabilities.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®