Ransomware Readiness for OT & Control Systems Environments

Is your organization ready to defend against ransomware?

The FBI predicts that ransomware attacks will exploit insufficient security procedures, protocols, backups and other infrastructure security gaps costing the world $11.5 billion in 2019, and $20 billion in 2021.

Recent attacks on state and local governments and critical infrastructures have major corporations reevaluating their risk exposure—especially those with operational technology (OT) environments. Example attacks in 2019 include:

- The Baltimore City government was hit with a massive ransomware attack that left it crippled for over a month, with a loss value of over $18 million. (Source: Baltimore Sun)
- New York City's capital was hit with a ransomware attack that took several key services offline. (Source: CNET)
- Norsk Hydro aluminum producer suffered a cyber-attack, that included ransomware, and later posted an 82% drop in Q1 profits due to the loss of production. (Source: CNBC)

> "Every 40 seconds a business falls victim to a ransomware attack. Cybersecurity Ventures predicts that will rise to every 14 seconds by 2019 —and every 11 seconds by 2021."
>
> **2019 Official Annual Cybercrime Report**

OT and control systems environments, which tend to use older, legacy IT systems, are easier targets for these attackers. Organizations running critical systems with vintage software that can no longer be patched or monitored appropriately are most at risk of a breach.

Prepare to Protect

Considerations for ransomware readiness include:

Key Objectives	To-Do	Pro Tip
Identify Risks	**Understand the key risks of ransomware:** • Important data stored on workstation systems not normally backed-up by enterprise processes. • Recovery of encrypted data is unlikely with modern ransomware malware. • Control systems often operate in enclaves or disconnected from enterprise IT systems that provide backup & recovery capabilities. • Flat networks allow for infected corporate systems to harm control system endpoints and servers.	• Talk to your users if you don't know what your pain points are for specific OT environments. • Analyze your process workflow as a starting point to identify critical resources. • Don't overlook the human element. Educate your people via training and awareness programs and exercise your incident response plan with tabletop workshops that engage all stakeholders.
Architect & Engineer Protection	**Patches** Keep your infrastructure and patches up to date.	Up front investments to replace and retool legacy systems may seem cost prohibitive but consider that losses due to ransomware-induced downtime is estimated to average $8,500 per hour. (Source: Govtech)
	Segmentation & Isolation Segment your OT and IT networks and isolate the "crown jewels" and systems known to be vulnerable. This helps reduce the attack surface while enabling business-critical information flows.	Consider a "kill switch" mechanism to enable isolation of critical production operations. This can be particularly important for OT and manufacturing plant floor environments.
	Logging & Monitoring Ensure you have copies of logs to help determine the source of infection. At a minimum, have remote access, authentication server/domain controller, and key application and workstation logs available. Also set alerts for changes from accounts with high privileges.	For Windows event logging and forwarding, look at WEFFLES to quickly build out a hunting and response dashboard. If you don't already have log aggregation and correlation capability, set up Graylog (or another ELK stack) to aggregate and correlate logs from infrastructure devices.

(continue)

Prepare to Protect

Considerations for ransomware readiness include:

Key Objectives	To-Do	Pro Tip
Architect & Engineer Protection	**Portable Media Management** Control and restrict usage of thumb drives and connections from third-party devices.	Deploy dedicated scanning workstations with multiple anti-virus and anti-malware products to detect malicious software and develop procedures requiring all USB drives be scanned prior to use in the OT environment.
Plan Recovery	**Ensure regular backups.**	Consider: • How long can you operate without automation control or monitoring? • How often do you make changes to your setpoints and interfaces?
	Verify fidelity and test restoration regularly. Use representative samples of disaster recovery spares if you don't have a test environment to ensure backups can be restored effectively	System restore points may not be safe. Unless you can identify the specific date and time the attacker initially compromised the network, restoring from snapshots or restore points may put you at risk of re-infecting upon restoration, providing the attacker with sustained access. Rebuilding systems from known good media and restoring system configurations is the safest option to avoid re-infection.
	Take offline / disconnect to get offline snapshot. This is the most important step to protect against ransomware. Separate VLANs and firewalls (access control rules) often do not prevent the malware from spreading. Ensure you can isolate a copy of your backups to a disconnected network segment or physically remove them from the network after successful completion.	This can be a multi-stage backup procedure with offline storage capabilities, or it could be as simple as an external hard drive connected to your historians or engineering workstation for backups and disconnected when not in use.

Prepare to Protect

Considerations for ransomware readiness include:

Key Objectives	To-Do	Pro Tip
Plan Recovery	**Be prepared to restore and rebuild critical data and applications.** Make sure you engage your vendors to get copies of software and processes to issue license keys ahead of time.	Surplus or recently decommissioned systems could be used for redeployment if necessary. Leverage any BCDR plans or rapid development if not available.

Partner with Accenture Security

Safe, reliable, always-on access to critical production operations is paramount, which means OT environments cannot always be secured in the same way as traditional IT environments. With a combination of industry-specific expertise and cross-industry best practices, our team provides unique insights to identify security risks to your operations and prioritize strategic remediations. Our experienced leadership and project managers have successfully executed large multiyear projects building security programs to defend some of the most attacked networks in the world.