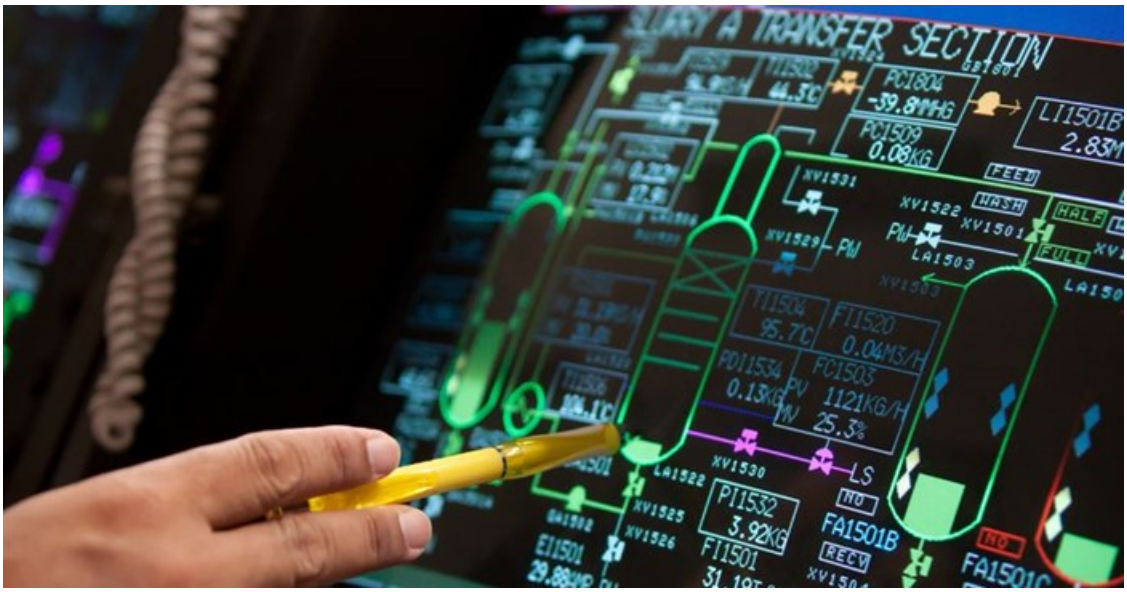
Your 10-step critical infrastructure operational security assessment

Almost 80% of industrial security incidents in critical infrastructure organisations are caused by unintentional internal issues such as software misconfigurations from human error and malfunctioning network protocols, according to cybersecurity solutions provider Fortinet.



©kiattisak chiphimai via 123RF

Critical infrastructure industries in particular, such as utilities, transportation and natural resource producers, together with the communities and economies they serve, face not only particularly damaging outcomes from cyber security attacks, but also need to deal with significant complexity due to the scale of their operations.

Evolving threatscape

“Organisations across multiple industries today face an evolving threatscape and growing pressure to rethink security strategies for long-term sustainability. A more holistic security approach is required to protect against intentional targeted attacks as well as human error from internal sources,” says Perry Hutton, regional vice president for Africa at Fortinet . “Solving ICS (industrial control systems) security issues requires a solution that unifies the best of current OT network security capabilities with an extensive understanding of ICS processes and protocols.”

The machines and technology used to manage and run hydropower dams, oil and gas companies and other infrastructures were never designed to be connected to remote or public networks. As these systems were isolated and physical access often restricted, information security has never been accorded the highest priority.

“But with emergence of Industry 4.0, these environments are now interconnected. Proliferation of open standard and off-the-shelf hardware and software also increases their vulnerability. This means that industrial control systems (ICS) now have a wider footprint for attack,” explained Hutton.

Top ten guidelines

As organisations cannot predict every threat, they must then focus on what they can control. Fortinet recently issued the top 10 guidelines to help local companies assess their operational technology (OT) vulnerabilities:

1. Identify critical elements that need immediate protection - This is a crucial first step.

2. Identify protocols for permission management or access to controls - Most systems were previously isolated. Now that IT and OT are interconnected, they need to keep pace with OT security best practices. In addition, determining the appropriate privileges for authorised users is just as important as blocking unauthorised access.

3. Update hardware and software operating systems regularly - Some hardware and software systems pre-date the very notion of cybersecurity. Organisations need to ensure compatibility with standard modern defences such as anti-virus software or threat scanning technologies.

4. Perform regular and routine organisation update and patch - While most operations cannot afford any down-time and cost associated with patching, deferring updates lead to wider security gaps.

5. Identify unsecured, and IP-enabled telemetry devices such as sensors and pressure gauges - Data on these devices can be manipulated, which then impacts the safety and reliability of the overall system.

6. Employ best practices in modern coding - Using embedded and often custom-built software written with little attention to recommended security techniques leaves OT systems open to attack.

7. Adhere to a standard procedure for logging events - Organisations that establish a process for noting and reporting system events can often use this data to detect irregularities and implement security measures.

8. Regulate component manufacturers and supply chain - Without proper monitoring and governance, equipment may be compromised before it is even installed.

9. Implement network segmentation - Many operations have not yet partitioned their networks into functional segments (while remaining fully interconnected). Without proper segmentation, infected data and applications can overlap from one segment to another, and attackers who manage to breach perimeter defences can easily move undetected across the network.

10. Prepare an operational recovery plan - In the unfortunate event of a disaster, every organisation needs a documented procedure to assess damage, repair systems and machines, and restore operations. Regular security drills also help operators implement recovery quickly and efficiently when it is needed most.