Managed Security Services for Energy

Enabling the benefits of convergence while preventing threats

Benefits of convergence for energy

Improved Flexibility
Organizations react more quickly to market changes. They can change production timelines based on outside factors efficiently while still meeting business objectives.

Enable Best Practices
Organizations use IT/OT convergence projects to bring longstanding IT best practices to their operational systems.

Lower Operating Costs
Convergence drives lower costs by optimizing resource utilization.

Better Performance
Combining IT and OT data means organizations can generate more accurate and meaningful KPIs.

Challenges of convergence for energy

Insufficient funds, legacy equipment issues, and lack of expertise make it difficult for energy firms to justify investment.

Top three digital transformation challenges

"What are the top-three challenges holding back your organization from undertaking digital programs that support the transformation of services?"
Showing the top five answers ranked based on top, second, and third priority combined

Source: Omdia

The security team has lots of issues corresponding to rapidly changing sophisticated attacks like ransomware, while also supporting execution of business strategy.

"What are the issues that most affect security organizations?"

This is paired with cybersecurity concerns around digital transformation.

Note: n=601
Source: Omdia

How confident are you about your organization's resilience?

Most organizations describe their security visibility as "good," but the aim should be "excellent."

Responding quickly to high-priority security events is a must for businesses, yet only 1 in 4 can respond within hours.

Which best describes your organization's security visibility across on-premises, branch, cloud, and remote/home environments?

Note: n=181
Source: Omdia

How quickly can your organization respond to, and successfully resolve 'high' priority security events?

Note: n=181
Source: Omdia

Without action, risk could grow. Efficiently manage to mitigate risk.

Ineffective cybersecurity management can leave gaps that could potentially lead to shutting down operations as a precautionary measure – even if intrusion begins on the IT side of the business.

Security researchers have demonstrated lateral movement across levels of the Purdue model, through the OT network, as can happen in IT networks.

Recent major breaches, such as May 2021 Colonial Pipeline ransomware attack, showcase how an IT breach can impact OT. The attack began on the IT side, with breached credentials, but operations were shut down for six days as a precautionary measure.

An effective cybersecurity program builds systems to enhance safety & control

An effective cybersecurity program includes:

Assessment: Consideration of assets, devices, and users across sites, remote locations, and networks.

Implementing cybersecurity controls clarified by the assessment will allow organizations to apply security measures in a cost-efficient manner.

Visibility and monitoring of effective cybersecurity controls will allow organizations to gain a clear, accurate picture of their networks, as well as continuous monitoring.

Detection and response need to be timely, with clear response, remediation plans, and playbooks that consider both IT and OT implications.

Recovery and reporting policies will need to be in place for recovery and reporting, in order to aid best practices in cybersecurity resilience and knowledge sharing.

Continuous improvement: Organizations must provide for continuous improvement by verifying and improving the efficiency of each activity.

Regulatory compliance and standardization will help, but expert interpretation and support is necessary.

Critical industries, like energy, are heavily regulated, and increasingly cybersecurity requirements are being developed by governments globally. These are helpful in developing an effective cybersecurity program, but determining how to navigate and implement standardization, and meet regulatory compliance, needs expertise.

The NIS 2 Directive.

Focus is on infosec policy, incident prevention, detection and response, encryption, supply chain security, crisis management, and vulnerability disclosure – with a revamped approach to incident reporting.

The North American Electric Reliability Corporation.

Critical Infrastructure Protection (NERC CIP). Includes requirements spanning asset identification, management control, employee training, physical access control, incident response planning and reporting, and vulnerability assessment.

IEC62443 – The ISA/IEC 62443 series of standards.

These standards set best practices for security and provide a way to assess the level of security performance. Their approach to the cybersecurity challenge is a holistic one, bridging the gap between operations and information technology as well as between process, safety, and cybersecurity.

NIST Cybersecurity Framework (CSF).

The US NIST CSF specifies categories for firms to build a security posture, breaking threat protection into five categories: identify, protect, detect, respond, and recover.

Benefits of a Managed Security Service

Convergence issues	Managed security service
Budget constraints	Managed services help organizations justify the investment in by providing and implementing the right security controls that meet top requirements
Uncertainty about new IT/OT convergence threats	By providing reliable expertise, managed services help organizations gain more confidence in responding to attacks
Skills shortages in security – both technical and operational	By providing security service operations as well as consultative and technical expertise, managed services help to address the skill gaps
Lack of visibility across field or plant devices to determine vulnerabilities and implement security	By providing carefully chosen cybersecurity tools, managed services help organizations gain more visibility in their plant
Meeting executive management and regulatory requirements	Managed services help organizations to implement a holistic cybersecurity program, including the optimal measures for the security level for each plant

OMDIA

Brought to you by Informa Tech