Guidehouse
Outwit *Complexity*

The Energy Sector's Critical Cybersecurity Challenges

Energy organizations seeking to effectively prevent, detect, and respond to cyber threats are often hindered by the complex mix of legacy and modern systems, compliance concerns, and emerging security risks in the energy sector.

The energy sector is especially vulnerable to cyberattacks and data breaches, which pose enterprise-level risks throughout operations and particular vulnerabilities in generation, transmission, SCADA, EMS, and field support. Compliance and statutory frameworks from the North American Electric Reliability Corporation (NERC) and the Federal Energy Regulatory Commission (FERC) exert added pressure on the sector to harden security, regulate access, and improve resilience.

Energy organizations are therefore tasked with integrating nuanced differences in security requirements and documentation while improving internal governance processes and prepping for incident response across the sector's distributed threat landscape. Incomplete integrations spanning legacy and modern systems, IT and OT environments, and technical debt from mergers or acquisitions add significantly to the complexity.

The Energy Sector's Cybersecurity Complexity

Effective risk management starts with a holistic understanding of the sector's threat environment. The following present unique cyber risks for energy organizations:

Ransomware Attacks and Incident Response

Challenge: As providers of critical services, energy organizations are at greater risk of ransomware attacks by criminals or nation-state threat actors. What's more, such attacks can lead to severe repercussions in this sector—and remediation afterward often costs more. Any disruption in the operations of an energy provider's systems or of the bulk-power system (BPS) could have catastrophic consequences for populations, not to mention significant reputational and regulatory risk.

Solution: Assessing your organization's ability to effectively prevent, detect, and respond to attacks is critical. This can be done by reviewing internal governance processes, implementing security controls, and creating an incident response plan with the help of experts in postbreach remediation.

Identity and Access Management Inefficiencies

Challenge: Managing credentials and access is particularly crucial for energy organizations since they risk facing significant fines if access governance mistakes or delays are found during audits. But complying with regulations can be difficult when disparate HR and IT systems and failures in integration cause inefficient communication. Rigorous identity and access management (IAM) processes help energy organizations build toward Zero Trust and are critical for security in both traditional networks and cloud-based architectures. Through the merger of technology, people, and process, IAM provides the right people the right access to the right resources for the right reasons.

Solution: The utility workforce needs hybrid IAM solutions that integrate best-in-class processes and technology in compliance with industry regulations to ensure the protection of critical energy/electric infrastructure information (CEII), bulk electric system cyber system information (BCSI), and personally identifiable information (PII) while also bridging aging and distributed OT and IT architectures.

Incomplete Integration of Systems

Challenge: An energy organization's typical threat landscape includes IT and OT architectures, legacy and modern technology, and disparate systems acquired via mergers or acquisitions that struggle with interoperability. Integrating the right tools into control, transmission, generation, distribution, and field networks while remaining compliant requires custom solutions with open standards and APIs to assist with streamlining. The mix of legacy and new equipment means that some infrastructure can't be patched or hardened and instead requires a risk management approach that includes network segmentation, intrusion detection, and endpoint detection and response.

Solution: Energy companies need holistic assessments and strategies that integrate cyber hygiene and compliance to better protect distributed, inefficient, and legacy systems and build organizational resilience.

Energy Sector Risk Management

Guidehouse combines comprehensive cyber risk management expertise with deep industry knowledge of utilities and the energy sector. We offer:

- Cybersecurity Strategy and Security Architecture
- Cyber Resilience
- Identity and Access Management
- Incident Prevention and Response
- Data Protection and Privacy
- Cyber Threat Intelligence
- Supply Chain Risk Management
- Continuous Supply Chain Monitoring

FERC, NERC, and State and Federal Compliance Requirements

Challenge: Ensuring compliance, especially with NERC CIP, requires robust stakeholder engagement, clarity in roles and responsibilities, and continuous training and awareness initiatives. The nuanced differences between security best practices and regulatory requirements mean that utilities often struggle to integrate cybersecurity with compliance documentation and evidence requirements.

Solution: To achieve greater ROI, the sector needs to approach compliance from a practical perspective focused on efficiency to ensure that security operations lead to compliant outcomes.

Supply Chain Risks

Challenge: Due to issues like COVID-19, rising costs, unstable availability, geopolitical trends, onshoring pressures, emerging legal regulations, increased cyber interconnectedness, and environmental and sociopolitical drivers around supplier choices, supply chain risk management is an emerging imperative for the sector. The replacement or construction of critical pieces of infrastructure isn't just costly—the risk of cyber tampering or the disruptive nature of a delay could have significant consequences.

Solution: Supply chain risk management should be a critical part of every energy organization's risk management strategy and must ensure compliance with NERC supply chain requirements while integrating CIP-013 standards into enterprise processes. Due diligence, supplier illumination, supply chain risk management program design, and supply chain risk assessments are increasingly becoming business critical.

The Guidehouse Advantage

Guidehouse's Cybersecurity team and our Energy, Sustainability, and Infrastructure team promote and foster the effective security practices integrated with operational and compliance goals. Our deep energy industry experience, combined with a comprehensive understanding of the technology, strategy, and security interventions needed across the energy sector's IT and OT assets, positions us to start fast and succeed immediately. Our experts help energy companies and utilities conduct cybersecurity assessments, harden security, streamline compliance, and increase resilience—so they are prepared for any threats the future has in store for them.

Guidehouse
Outwit *Complexity*

For more information,
please contact:

Marianne Bailey
Partner, Cybersecurity
mbailey@guidehousefederal.com

Chris Luras
Partner, Energy—Security &
Compliance
chris.luras@guidehouse.com

Guidehouse's Energy, Sustainability & Infrastructure Segment

With more than 700 consultants, Guidehouse's global Energy, Sustainability, and Infrastructure segment is the strongest in the industry. We are the go-to partner for leaders creating sustainable, resilient communities and infrastructure, serving as trusted advisors to utilities and energy companies, large corporations, investors, NGOs, and the public sector. We've solved big challenges with the world's 60 largest electric, water, and gas utilities; the 20 largest independent power generators; five of the 10 largest oil and gas majors; the 20 largest gas distribution and pipeline companies; European governments; and the US federal government's civilian agencies involved in the country's land, resources, and infrastructure. We combine our passion, expertise, and industry relationships to forge a resilient path toward sustainability for our clients. We turn vision into action by leading and derisking the execution of big ideas and driving outcomes for our clients that enable them to reach their ambitions through transformation. For more information, visit **www.guidehouse.com/esi**.

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures, focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 12,000 professionals in over 50 locations globally. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit **www.guidehouse.com**

Web: guidehouse.com/cybersecurity / @GHTechSolutions linkedin.com/company/guidehouse-technology-solutions