GoSecure

USE CASE BROCHURE

ENERGY

THE IMPERATIVE FOR ROBUST CYBERSECURITY IN THE ENERGY SECTOR

VULNERABILITIES IN NUMBERS:

20%

In North America, the energy sector accounts for 20% of cyberattacks

39%

Energy sector faces 39% of critical infrastructure attacks

$4.65 MILLION

Average breach cost in energy sector

Your ally to consolidate, evolve & thrive

SAFEGUARDING ENERGY INFRASTRUCTURE IN THE DIGITAL AGE

As the energy sector embraces digital transformation, it becomes increasingly vulnerable to cyber threats. From smart grids to automated systems, technological advancements bring efficiency and sustainability, but also expose critical infrastructure to potential cyberattacks.

These attacks can cause widespread blackouts, economic disruption, and threats to national security, highlighting the urgent need for strong cybersecurity measures.

Cybersecurity in the energy sector is not just about technology; it requires a comprehensive strategy involving threat detection, incident response, employee training, and stakeholder collaboration.

Proactive measures like regular security assessments and real-time monitoring are essential to protect against sophisticated cyber threats.

HAZARDS OF A WEAK CYBERSECURITY PLAN:

- OPERATIONAL DISRUPTION
- DATA BREACHES
- FINANCIAL LOSS
- SAFETY RISKS
- REGULATORY CONSEQUENCES
- LOSS OF PUBLIC TRUST
- INSIDER THREATS
- COMPETITIVE DISADVANTAGE

Worse yet, users with elevated privileges could inadvertently give attackers the “keys to the kingdom”.

INFO@GOSECURE.AI

www.GOSECURE.AI

GoSecure

SECURING OUR POWER WITH GOSECURE

GoSecure leads the way in securing our future against cyber threats by meeting the NERC's Compliance & Enforcement standards.

CHALLENGES

INCREASING ATTACK SURFACE

The shift to smart grids and the Internet of Things (IoT) expands the number of entry points for cyber threats. Each connected device or system component can be a potential vulnerability.

SUPPLY CHAIN VULNERABILITIES

The energy sector's reliance on third-party vendors and suppliers introduces additional risks. A cyber-attack on a less secure partner can compromise the entire supply chain.

INCIDENT RESPONSE AND RECOVERY

Developing and maintaining effective incident response and recovery plans is challenging. Rapidly identifying, containing, and mitigating cyber incidents requires well-coordinated efforts.

DATA PRIVACY CONCERNS

Protecting sensitive data, including consumer information and proprietary business data, is a growing concern. Data breaches can result in significant financial and reputational damage.

GOSECURE'S RESPONSE

We deploy comprehensive threat detection and monitoring systems to secure every connected device within your network. Our continuous monitoring and threat intelligence services protect against intrusions at all entry points, keeping your operations safe.

We conduct thorough risk assessments of your third-party vendors and supply chain partners. By implementing robust supply chain security protocols and continuous monitoring, we protect your operations from potential vulnerabilities.

GoSecure's incident response teams are specialized in energy & utilities' operations, providing swift action plans and recovery measures to restore services with minimal downtime.

We implement advanced encryption and data protection measures to safeguard your sensitive information. Our data privacy protocols meet **NERC's Compliance & Enforcement** standards, ensuring that your data remains secure.

INFO@GOSECURE.AI

www.GOSECURE.AI

Your ally to consolidate, evolve & thrive

GoSecure

Know Your Risk to Mitigate Your Risk

With the industry's top players across North America, including the leading energy supplier in Canada, placing their trust in GoSecure, our reputation for excellence speaks volumes.

YOUR SAFETY IS OUR TOP PRIORITY

GoSecure is the best ally for the energy sector, gas industry, utilities, and renewable energy, with over 20 years of expertise safeguarding major players from coast to coast. Our unmatched experience and global presence make us the ultimate partner in cybersecurity, trusted by the industry's leading companies.

Our deep understanding of the energy sector's challenges allows our Penetration Testing Services to offer electric utilities comprehensive solutions to identify, assess, and remediate vulnerabilities.

Our expert team conducts meticulous assessments to pinpoint potential weaknesses before they can be exploited by malicious actors, establishing GoSecure as a trusted leader in energy cybersecurity.

With tailored services, an experienced team, and a steadfast commitment to compliance, we not only meet the unique security needs of energy sector companies but also elevate their overall cybersecurity posture.

Partnering with GoSecure enables companies to confidently navigate the complexities of the evolving threat landscape, ensuring the reliability and safety of their operations, safeguarding sensitive data, and upholding the trust and safety of their users for years to come.

CONTACT US NOW

DESIGNED TO IDENTIFY VULNERABILITIES IN YOUR ECOSYSTEM

INTERNAL NETWORK

- Thorough assessments of internal networks, identifying vulnerabilities and crafting tailored solutions for optimal protection of critical infrastructure and data.

OT NETWORK

- Identifies and mitigates vulnerabilities, ensuring compliance with industry standards and minimizing disruptions to essential operations.

EXTERNAL NETWORK

- Identifies potential entry points, and provides ongoing monitoring and threat intelligence to enhance security and safeguard critical assets from external threats

PHYSICAL PENETRATION TESTING

- Assesses physical security measures, simulating real-world scenarios to identify weaknesses and offering actionable recommendations to mitigate risks, ensuring robust protection of facilities, assets, and personnel.