WHITEPAPER

3 Solid Security Strategies for the Energy Sector

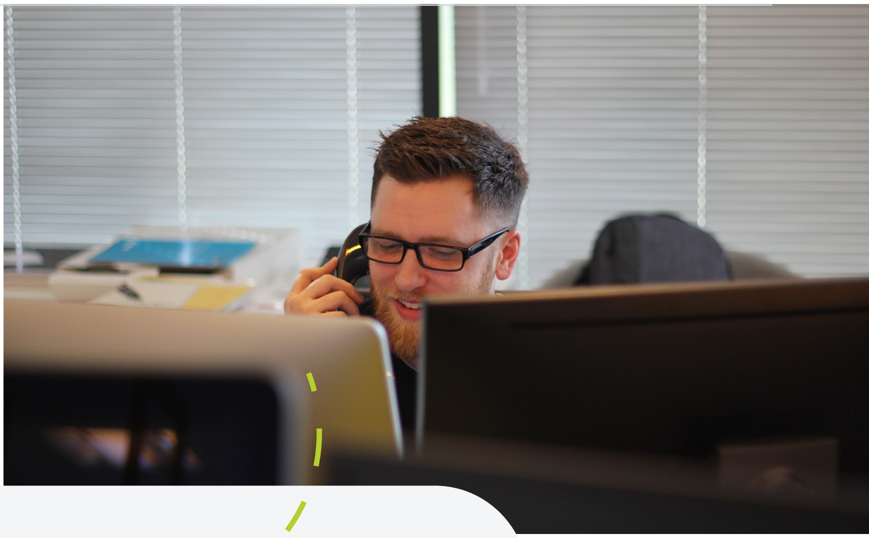
This article will recommend solid and verifiable security strategies for cloud project controls in the energy sector: communication, education, and integration—with the overarching goal of improving cloud security by attaining digital transformation.

Believe it or not, the **energy and utility** sectors need a more robust approach to ensuring that the human factor of IT and cloud security is improved upon. The failure to adequately communicate, train, and educate current and future employees – as well as to upgrade outdated IT networks and systems to real-time cloud technology and fully integrated cloud platforms hosting said technology – stands as a significant roadblock to energy companies being fully protected against bad actors and security threats again.

In other words, the human factor of digital transformation should not be overlooked regarding security.

McKinsey recommends that **the energy sector take a multi-level approach to tackle security threats.** Their recommendations include improving internal communication between departments and IT, facilitating clear information sharing channels between internal and outsourced IT support, and closing company-wide security and technology gaps.

We'll explore the implications of each of these recommendations for the energy industry, along with concrete steps you can take to improve your company's security infrastructure.



1 Security & Communication

Clear communication is difficult for everyone. For IT, however, industry standards are changing at a more rapid pace than in other industries.

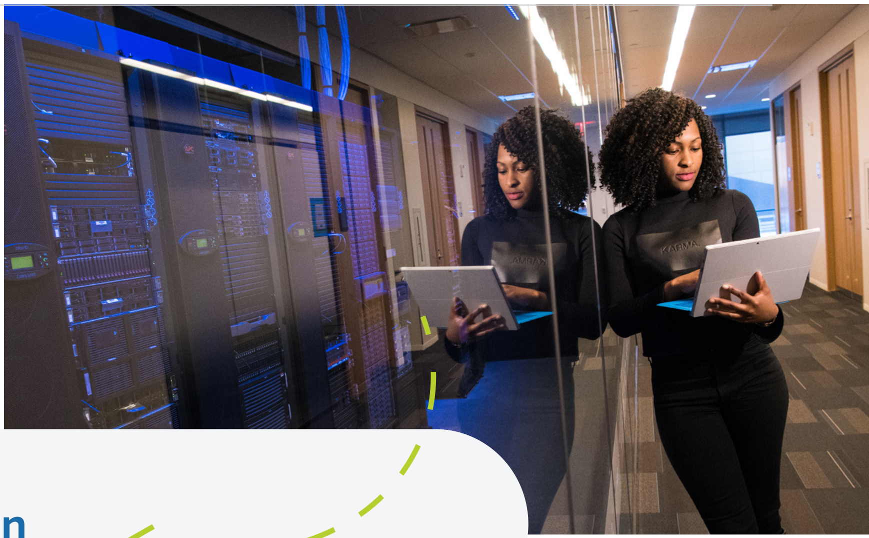
Because the energy sector is so vulnerable to attacks from outside sources, it is imperative that IT executives, department heads, and internal employees communicate well with each other and any outsourced parties like cloud security, cloud-managed services, and IT support teams. This means real-time communication and observation of local or trending security breach trends. Share current industry trends and security breach protocol with IT to minimize unexpected attacks.

For example, if phishing is a recent trend for local energy companies during or after power outages, notify both customer and internal (and outsourced) IT department heads to ensure your company acts proactively to prevent data breaches or billing fraud.

During recent power outages in Texas and Oregon, data theft came in unexpected forms such as door-to-door solicitation and phone calls—in addition to phishing schemes, ransomware, and hacking of IoT devices. Illustrating this last point, the **Department of Energy (DOE) and other federal security agencies** recently warned of potential attacks on programmable logic controllers and open platform servers.

For energy and utility companies that utilize cloud platforms to store their data, it is crucial to use a cloud with airtight security policies. In the event of a climate or data breach emergency, cloud disaster recovery is critical. **If the unthinkable happens,** it helps to have an entire team of security experts on the line to help you out. Specific protocols to restore lost data should include the following:

- Protected: Tier 4 cloud data recovery system protects data 24/7/365
- Recoverable: In the event of a full data center outage, all files are fully recoverable
- Aligned: Recovery Point Objectives (RPOs) are aligned with customer needs
- Flexible: Use our data centers, yours, or a combination of both



2 Security & Education

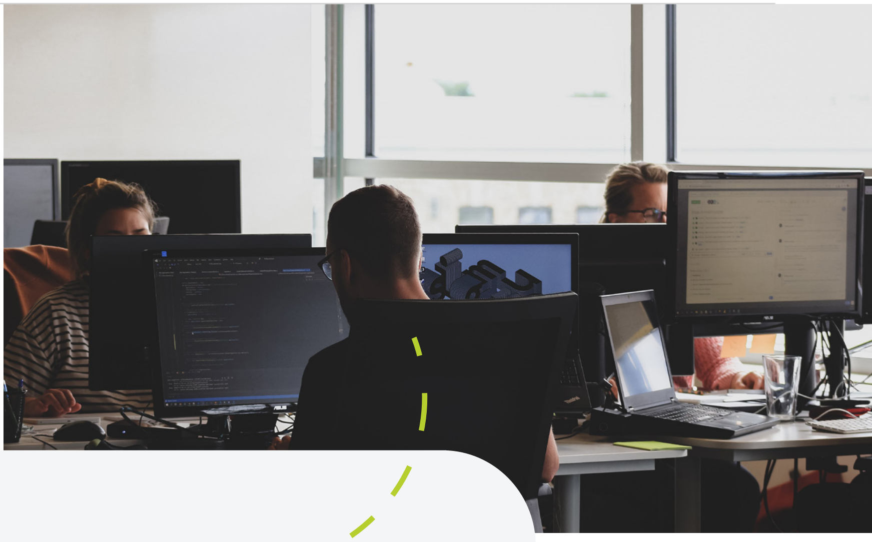
Continuing education is essential for IT departments and is connected to market competition. When hiring new talent or retaining existing information security professionals, there are budget constraints for energy and utility companies. As far as cloud security is concerned, many highly skilled security professionals are gobbled up by Silicon Valley – not energy or utility companies, who often can't compete with the salary range offered by up-and-coming tech companies.

According to the ISACA, at least sixty percent of respondents to their annual cybersecurity survey say they have unfilled positions, are understaffed, or have trouble retaining qualified cybersecurity professionals. Some of the reasons behind this retention difficulty include being recruited by other companies, poor financial incentives, or limited promotional opportunities.

Because of this, IT execs should offer incentives to make sure their IT support and security teams are happy and continuously train on the newest industry threats to keep them competitive with the current cybersecurity landscape. Ensure your security team is highly educated and knowledgeable about industry protocols like **Zero Trust security models,** where user provisioning is closely monitored.

Ensure all security teams are regularly uptrained and informed of current & potential industry-wide cloud security gaps (e.g., IOT work devices; outdated IT networks). A critical part of continuing education is making sure IT teams are up to date on all applicable technologies in their field. Being familiar with **industry-specific cloud security specializations** like system separation, firewall hardening, infrastructure redundancy, and data redundancy helps keep them relevant during future organizational changes—such as website migration or data center expansion.

Regarding future expansion, if your company is looking for the best next step, but you lack the resources to train new staff, hire cloud-managed services that are guaranteed to be up to date on training, security protocols, and customer support. Alternatively, **LoadSpring Academy**, our online training portal, allows you to add your own training videos and documentation for anyone using the platform.



3 Security & Integration

If your company utilizes the cloud, it's wise to automate security measures so your IT network thinks for you. But what types of security are industry-leading, specifically?

At LoadSpring, we implement rigorous technology procedures and standards:

- Application & Data Architecture
- Network & Infrastructure Security
- Security & Performance Monitoring
- User-Session & Password Security
- System Redundancy & Disaster Recovery

These areas of specialization all relate specifically to cloud security. To compete with newer startups and the rest of the IT sector, energy and utility companies need to adopt the latest technologies with guaranteed reliability, flexibility, and real-time updating capabilities.

Decrease the risk of security vulnerabilities by regularly maintaining software updates & compliance standards—or, better yet, utilize a Platform-as-a-Service that updates your software licenses for you. PaaS-based cloud security engineers can protect your data for you, eliminating the need to burden your internal IT team unnecessarily.

Implement comprehensive company-wide programs & protocols for diverse types of energy-related disaster recovery to ensure business continuity and minimize awareness gaps. Also, be sure to establish secure, clear user provisioning and integration guidelines to control access to data in a trackable way from anywhere.

How LoadSpring Protects Resources

Consider **LoadSpring's work with POWER Engineers,** who had been searching for a partner to help them with planning, design, implementation, and hosting of a program management solution. They needed a partner who valued collaboration and demonstrated program & project management experience—along with the ability to provide long-term infrastructure expertise, software knowledge, and customer support.

POWER Engineers chose LoadSpring as a partner because we were not only able to supply POWER Engineers with hosting for rapid software deployment; but we also enabled them to upgrade in several key ways:

- Rapidly expand program management capabilities
- Speed up implementation and training
- Increase software adoption
- Provide secure access to all stakeholders
- Integrate P6 and PCM with new software applications

According to Ross Pritchard, Director of Program Management at POWER Engineers, "LoadSpring's ability to listen and understand our strategic goals, and work with us to create the Program Management capability that fit our organization's unique environment, was critical. Other vendors seemed to want it done their way, which was inconsistent with our needs. In addition, LoadSpring's collaborative spirit and program management expertise ensured that POWER's Program Management Initiative was successfully executed in an extremely condensed timeline."

If you are a leader in the energy sector looking for a collaborative partner or secure cloud service provider, look no further than LoadSpring. We can take care of all your IT customer support as well as protect your static and in-transit data security needs. Whether you need to cloud-enable older, legacy systems or are simply looking for a safe way to integrate all your software applications into one platform dashboard location, LoadSpring's got you covered.

Want to learn more about protecting your company assets and resources in the cloud? Contact us today »