ESCALATING RISK SPARKS NEED FOR MULTILAYERED SECURITY DEFENSE

CDW PEOPLE WHO GET IT

THE CHALLENGE

Security experts continue to hammer home a frightening message: Cyberthreats are becoming more frequent and more sophisticated — and energy cooperatives, a prime target for determined cyberattackers, are sometimes woefully underprepared to protect their data and infrastructures.

Why are energy cooperatives coming up short on cybersecurity?

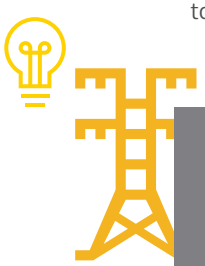
1. **Most cooperatives and utility companies have traditionally focused on security of physical assets rather than IT systems.**
2. **Unlike many other industries, the energy industry is vulnerable to all four types of cyberassault: hacktivism, cyberwarfare, cyberespionage and cybercrime.**
3. **Converging IT and SCADA systems to improve operational efficiencies exponentially increases the risk of data theft, operations disruption and equipment damage.**
4. **The widespread adoption of mobile devices creates substantial network vulnerability.**

Energy industry wake-up calls:

- Arkansas Electric Cooperative Corp. (AECC), a generation and transmission cooperative (G&T) based in Little Rock, is an example of co-ops taking a proactive approach to grid security. Arkansas Electric, which serves the state's 17 distribution co-ops, is already implementing changes in operations to meet new NERC security regulations that went into effect until April 2016.[1]
- The hard drives of more than 30,000 computers at Aramco were infected with the Shamoon "wiper" virus, destroying data and requiring 10 days to get the network back online.[2]
- Cyberattackers stole SCADA project files by breaching the internal firewall and security systems of Telvent, which supplies remote administration and monitoring tools to energy companies.[2]

Are you protected against these scenarios?

- Cybercriminals could create outages and malicious damage to electric cooperatives smart electric grid through connected devices or unmanned substations.
- Unauthorized access to a smart meter could allow access to the billing data of the surrounding areas, and potentially to the cooperatives' entire IT system.
- Cyberattackers could cause production stoppages, decrease product quality or destroy infrastructure by tampering with processes.
- Sprawling communication networks are the backbone of the interconnected smart devices. These networks create vulnerabilities that can be exploited by individuals seeking to disrupt power supply, steal profitable information and create chaos.



Only a quarter of energy companies agree or strongly agree that their organization effectively manages security risks to information assets, enterprise systems, SCADA networks and critical infrastructure.[3]

[1]http://www.nreca.coop/cyber-security-co-ops-work-to-confront-new-threats-and-reduce-grid-vulnerabilities/
[2]erpscan.com, "Oil and Gas Cyber Security — Questions and Answers," December 2015
[3]scottmadden.com, "Energy Industry Cybersecurity Report," July 2015

SOME SOLUTIONS FOR ELECTRIC COOPERATIVES

To combat pernicious cyberthreats, you need a comprehensive, robust strategy. CDW has the expertise, experience and full range of infrastructure, data, mobile and cloud security solutions required to safeguard your cooperatives' valuable assets.

A multilayered approach includes:

MOBILE SECURITY

Smartphones, tablets and other mobile devices increase the risk of data theft, loss or breach. Reduce risk with an enterprise mobility management (EMM) solution encompassing:

- Mobile device management (MDM)
- Mobile application management (MAM)
- Mobile content management (MCM)

AUTHENTICATION

Balance the need for workers to quickly access equipment in emergencies with measures that prevent unauthorized access to sensitive systems and data. Highly effective multifactor authentication combines:

- Passwords
- Key cards
- Biometrics

DEVICE AND ENDPOINT SECURITY

Safeguarding data in motion and at rest is becoming increasingly important with the rise of BYOD and the Internet of Things (IoT):

- Deploy devices with built-in security
- Use encryption, anti-virus and anti-malware software
- Implement data loss prevention (DLP) solutions to:
  - Classify sensitive data
  - Block or report transmission of sensitive data
  - Focus on specific weak spots
  - Ensure sensors are security layered

NETWORK SECURITY

Ward off attack and alert IT managers when the network has been breached:

- Unified threat management (UTM)
- Next-generation firewalls (NGFW)
- Intrusion prevention systems (IPS)
- Security information and event management systems (SIEM)

MONITORING

Detect anomalous activity that could indicate intrusion by using:

- Data logging
- Packet inspection
- Network traffic monitoring

THE BENEFITS

By bolstering your defenses with multilayered protection against cyberattacks, you can:

- **Ensure** the uninterrupted operation so critical to optimizing performance in today's challenging marketplace.
- **Avoid** the tremendous cost — both financial and reputational — resulting from data breach.
- **Support** the secure communication and flexibility that empowers your mobile workforce, improving productivity and customer satisfaction.
- **Achieve** regulatory compliance.

Don't become a cybercrime statistic. Protect your infrastructure and data with multilayered security solutions.

To learn more, contact your CDW Nonprofit account representative or call 888.294.4239