WHITE PAPER

PROTECTING OPERATIONS IN THE ENERGY SECTOR AGAINST CYBER ATTACKS

MOTOROLA SOLUTIONS

THE ENERGY SECTOR'S VULNERABILITY TO CYBERCRIME

The energy sector is one of the most susceptible industries to cyber attacks. In fact, according to the U.S. Department of Homeland Security, in 2014 a staggering 32% of all cyber attacks targeted energy companies. Cyber criminals are targeting the entire spectrum of potentially valuable data: data at rest, data in transit, and data in use.

It's not just data being lost, but potential profits, as well. Ponemon Institute reported that energy companies recorded average annual costs of $13.18 million due to cyber crimes in 2014.[2]

Combating this challenge has proven to be an uphill battle due to a wide profile of threat actors using an array of tactics. Malicious threats are coming from many places, including individuals who wish to make economic or political statements, or are simply disgruntled ex-employees. Others may seek financial gain or access to valuable, proprietary data on reserves and discoveries.

Whatever the motivation, the high attack frequency rates and corresponding downtime costs require strong cybersecurity safeguard controls.

32%
OF ALL CYBER ATTACKS IN 2014 WERE AGAINST ENERGY SECTOR COMPANIES[3]

$13.18
MILLION AVERAGE ANNUAL COST OF CYBERCRIME TO ENERGY COMPANIES[2]

37%
ENERGY COMPANIES VICTIMIZED BY CYBER CRIME[1]

SYSTEM CONVERGENCE LEADS TO HEIGHTENED RISK

The convergence of energy companies' operational technologies (OT) and information technology (IT) environments has perpetuated new security concerns across energy operations. Once isolated control systems are now integrated with corporate networks and the supply chain. The risk to these interconnected systems is magnified by the fact that threats can be introduced through their employees' private smartphones and devices.

Successful attacks in the form of malware have demonstrated that companies are often unprepared for the vulnerability these dynamic systems have introduced. SCADA and M2M devices that control drilling rigs, substations, and cloud-based services are primary targets, but the fact is that wherever there is digitally enabled technology or an intelligent device — even a simple device that controls a valve on the pipeline — there is a risk of it being used as a portal and taken over without authorization.

TOP 10 MOST CRITICAL SCADA VULNERABILITIES[4]

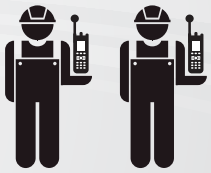
VULNERABILITY	SCADA IMPACT
Unpatched Published Vulnerabilities	Most Likely Access Vector
Web Human-machine Interface (HMI) Vulnerabilities	Supervisory Control Access
Use of Vulnerable Remote Display Protocols	Supervisory Control Access
Improper Access Control (Authorization)	Access to SCADA Functionality
Improper Authentication	Access to SCADA Applications
Buffer Overflows in SCADA Services	SCADA Host Access
SCADA Data and Command Message Manipulation and Injection	Supervisory Control Access
SQL Injection	Data Historian Access
Use of Standard IT Protocols with Clear-text Authentication	SCADA Credentials Gathering
Unprotected Transport of SCADA Application Credentials	SCADA Credentials Gathering

CYBER THREATS WITHIN THE CONTROL ROOM

Malware
2015: Symantec reported a malware attack on multiple energy sector companies throughout the Middle East, U.S. and U.K. The information reconnaissance threat called Trojan.Laziok allowed the attackers to gain access to employee computers and tailor their attacks by accessing system configuration data.[5]

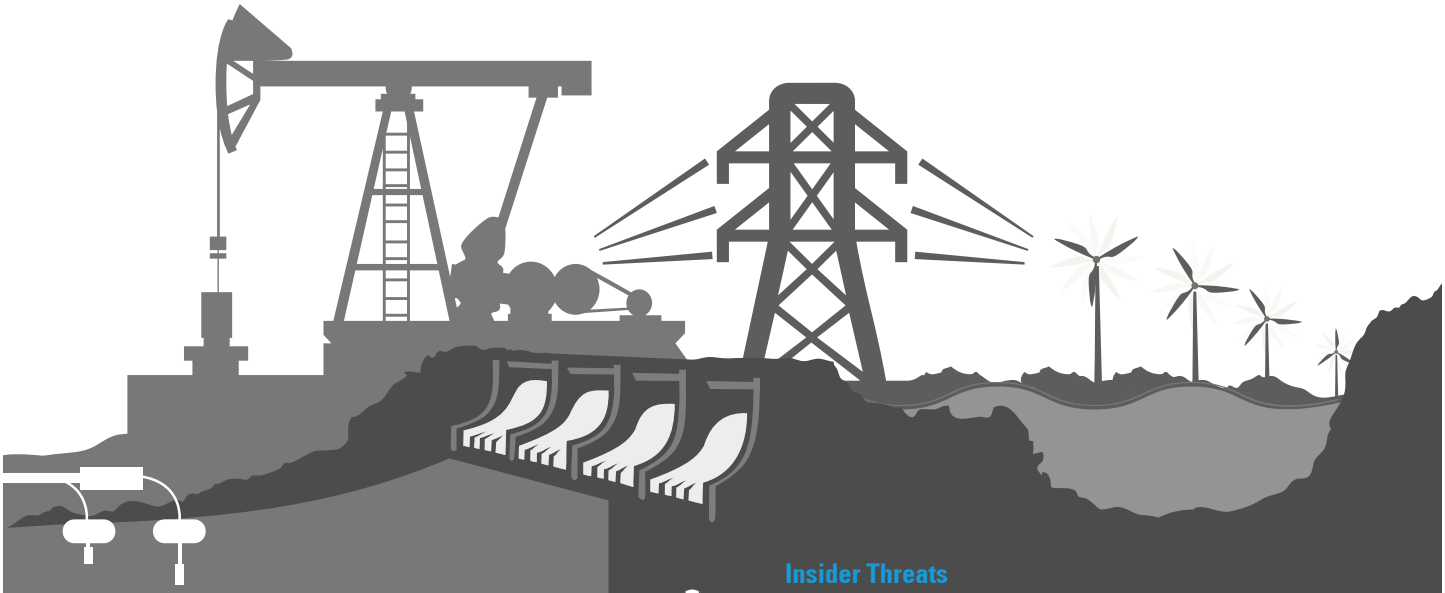
Malware and Phishing
2013: A spear phishing incident used publicly available information to customize an attack against an energy sector company employee. The attacker used public information to craft a malicious email disguised as a health insurance update from HR to an employee with access to the company's SCADA system.[7]

Advanced Persistent Threats
2014: Dragonfly (also known as Energetic Bear) launched attacks that compromised energy sector companies and energy control systems using a range of vectors including Phishing, Watering Hole exploitations, Remote Access Tools (RATs) and Trojanized Software. Its motive appeared to be cyber espionage, but it had the potential for sabotage as a secondary capability.[6]



Insider threats
2012: Shamoon was a malicious malware attack that resulted in the most destructive post-Stuxnet detection of advanced persistent threats. It targeted Saudi Aramco, removing and overwriting the information on the hard drives of 30,000 workstations. It was introduced into Saudi Aramco on a USB drive by a disgruntled insider that had full access to the system.[8]

CYBER THREATS IN THE FIELD



TODAY'S HARSH REALITIES

Attackers spend an estimated 243 days on a victim's network before being discovered.

In 2013, it took an average of 32 days to resolve a cyber attack.

63% of victims were made aware of their breaches by an external organization.

Source: Cybersecurity Roadshow, IBM, 2014

Insider Threats

2014: Harvard Business Review estimated that at least 80 million insider attacks occur in the United States each year. Their impact now totals in the tens of billions of dollars a year.[9]

Denial of Service

DDoS (Distributed Denial of Service) attacks cost energy companies $40,000 per hour (estimated average across all U.S. industries), with a duration of six to 24 hours, according to a recent Incapsula report. That makes the average cost of a single DDoS incident $500,000.[10]

Advanced Persistent Threats (APTs)

80% of Dragonfly (Energetic Bear) attacks occurred against energy sector or control system companies. 27 versions of the primary attack tool – the Havex Trojan – impacted 2,800 unique victims from 106 different organizations across 99 different countries.[6]

NIST CYBERSECURITY FRAMEWORK FOR CRITICAL INFRASTRUCTURE

In February 2013, Executive Order 13636 - Improving Critical Infrastructure Cybersecurity was enacted in response to the growing security, economic, public safety, and health risks caused by cybersecurity threats. The Order required the National Institute of Standards and Technology (NIST) to work with various stakeholders in the creation of a Cybersecurity Framework based on existing standards, guidelines, and practices.[11] The Framework comprises leading practices from various standards bodies that have proven to be successful when implemented. Motorola Solutions participated alongside government and industry partners to help develop this framework.

	NIST FRAMEWORK	CYBERSECURITY SOLUTION
IDENTIFY: 	• Business Environment • Risk Governance • Asset Management • Risk Assessment • Risk Management	• Robust maps of network assets (Physical assets, people, process capabilities)
PROTECT: 	• Policies • Processes • Data Security • Access Control • Protective Technology • Awareness and Training	• Edge and Core Firewalls • Authentication (End Device & Network) • Data and Voice Encryption • Escalation Procedures & Response Definition • Patching • Hardening • Anti-Malware • Gateway Access Controls
DETECT: 	• Anomalies and Events • Detection Processes • Continuous Monitoring	• Network Security Monitoring and Analysis • Intrusion Detection • Analysis Tools
RESPOND: 	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Firewall and Network Management Service • Remote Key and Certificate Management Process • Event Logging
RECOVER: 	• Recovery Planning • Improvements • Communications	• Redundancy • Backup & Recover • Process & Procedure Analysis • Lessons Learned

STEPS ENERGY COMPANIES CAN TAKE TO MANAGE THREATS

In today's interconnected business environment, a company's most sensitive information and operations are only as secure as its most vulnerable surface. Fortunately, that surface can be strengthened through a combination of planning and security solutions that can mitigate, contain, and remediate attacks with minimal disruption while reducing the chance of them happening again. This can only be accomplished by taking a holistic approach to understanding cyber risk across an organization's people, policies, processes, and technologies.

The first order of business when dealing with cyber threats is to implement a threat response plan. This plan will include the company-wide procedures and strategies necessary to manage the threats before they do irreparable damage and the technology that can help achieve this objective. This involves several steps:

Understand and Identify Vulnerabilities

As an initial step, energy companies must first understand and identify vulnerabilities across their organizations. The identification process accounts for risks associated with components such as control systems, communications networks, and back-end IT. Robust mapping of a company's network assets and process capabilities - physical, human and digital - can help to identify the infrastructure and operations that should be protected from different types of threats.

Implement Policies, Procedures, and Protection

Once cyber risks are identified, there are immediate controls that companies can implement to protect their system, but decisions regarding the right level of investment in protection vary based on a company's risk tolerance. At a minimum, instituting the appropriate workplace policies and procedures - along with relatively cost-effective physical and digital security measures to maintain updated firewalls, encryption, patching, and access controls - can mitigate approximately 75% of a company's risk.[12] Moreover, implementing a multi-layered combination of protective measures increases the complexity attackers must navigate to enter the company's networks, further mitigating the likelihood of intrusion.

Invest in Detection Capabilities

Identification and protection alone do not sufficiently secure an energy company from the most sophisticated and disruptive attacks; companies must also invest in detection capabilities to be alerted of a threat while it can still be contained. Network monitoring and threat detection tools help locate intrusions or abnormalities within an organization. These solutions can isolate threats early and improve security response time, increasing the likelihood of containment before an attack permeates other parts of the company.

Facilitate a Response and Recovery Strategy

An effective response plan in conjunction with additional tools can aid in resolving an attack and facilitating recovery. Procedures and communication within the organization can help to ensure critical systems are restored quickly, while key management and event logging solutions can be used to secure devices and analyze a threat.

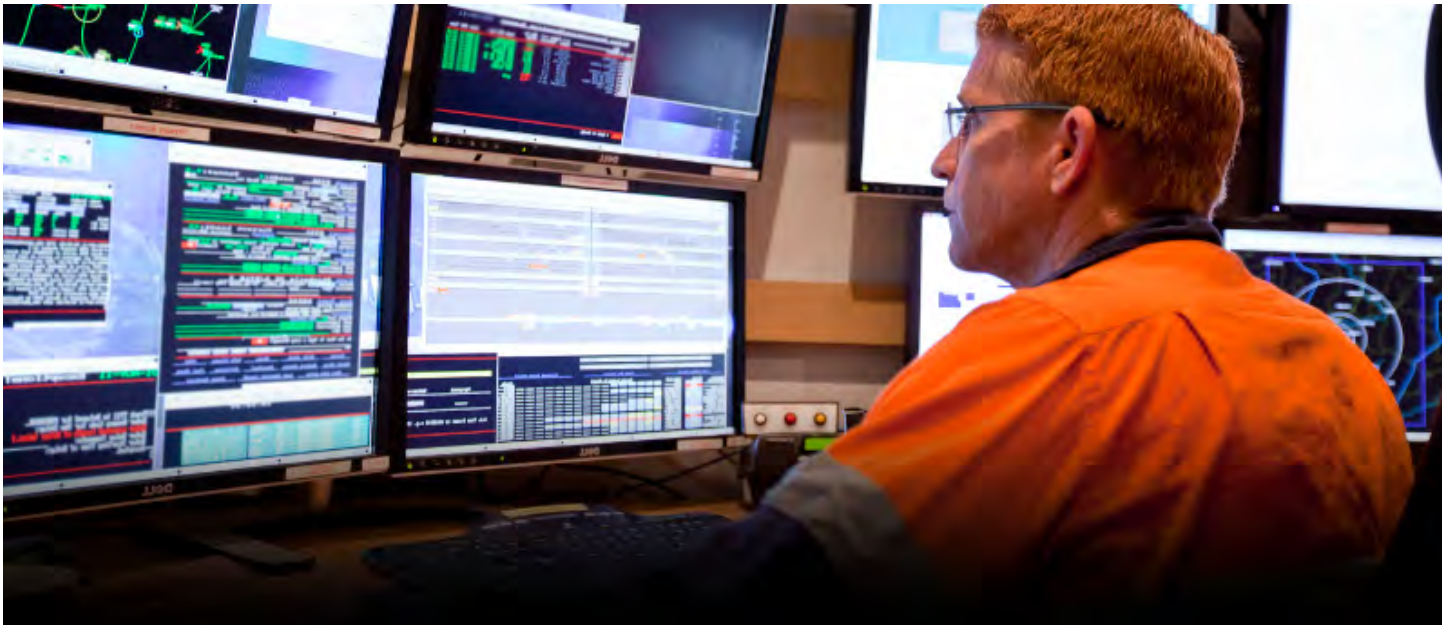
Response time is the most vital performance indicator of optimal cyber security, since in these situations, every second has significant financial impact to the organization. In very little time, critical data and processes could be erased or interrupted, resulting in a loss in productivity or physical damage.

A recovery strategy that includes redundancy or backup data logs allows operations to be restored quickly and safely. Additionally, proper procedural analysis after a breach will yield lessons learned which help to reduce the likelihood of future attacks.

STAY AHEAD OF CYBER THREATS

As energy companies are astutely trying to protect their control systems, communication networks, and other physical and digital assets, cybersecurity risk is heightened by a combination of increasingly complex systems, connected devices, open networks, and users with the potential to do harm. To truly combat today's cyber threats, energy companies must consider how their security measures across people, policies, processes, and technologies function in unison, and address any vulnerable interfaces between systems and users.

Motorola Solutions can evaluate your systems from end to end and deliver the security solutions energy companies need to identify, protect, detect, respond, and recover from cyber attacks.



SOURCES

1. http://www.threattracksecurity.com/resources/white-papers/data-breaching-malware-threatens-energy-and-finance-firms.aspx
2. http://www.ponemon.org/blog/2014-global-report-on-the-cost-of-cyber-crime
3. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf
4. http://energy.gov/sites/prod/files/Vulnerability%20Analysis%20of%20Energy%20Delivery%20Control%20Systems%202011.pdf
5. http://www.symantec.com/connect/blogs/new-reconnaissance-threat-trojanlaziok-targets-energy-sector
6. https://kasperskycontenthub.com/securelist/files/2014/07/EB-YetiJuly2014-Public.pdf
7. http://www.welivesecurity.com/2013/09/30/one-click-then-boom-spear-phishing-could-black-out-energy-companies-expert-warns/
8. https://www.tofinosecurity.com/blog/shamoon-malware-and-scada-security-%E2%80%93-what-are-impacts
9. https://hbr.org/2014/09/the-danger-from-within
10. http://www.elp.com/articles/powergrid_international/print/volume-20/issue-2/features/the-growing-threat-of-denial-of-service-attacks.html
11. http://www.nist.gov/cyberframework/
12. http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf

To learn more about protecting your energy operations, visit
www.motorolasolutions.com/cybersecurity