Protect Our Nation's Energy Backbone from Cyber Attacks

Data Breaches and Compliance Mandates Present Critical Challenges

Energy companies — bulk electricity providers and utilities — are incorporating enterprise applications and mobile technologies across their organizations. While those technologies help improve services, productivity and profitability, they also increase the risk of accidental and intentional data loss.

The Stuxnet worm in July 2010 validated long-held fears that sophisticated cyber attackers could not just steal sensitive data — they could use that data to hijack enterprise and mobile technologies' Internet connections to remotely sabotage critical mechanical processes in vital infrastructure in a time of war or national security crisis. While Stuxnet did no damage in the United States, it represents threats energy companies can expect — and must protect against.

Data breaches can hurt not just energy companies but thousands, or even millions, of their customers. Recent research found that U.S. data breaches averaged $7 million apiece and over $200 per compromised data record[1] — meaning energy sector data breaches can quickly reach astronomical costs.

Protecting the nation's energy infrastructure from data breaches and cyber attacks has thus become a critical priority for both energy companies and the U.S. government. Four key compliance areas for data breach mitigation are listed at the right:

[1] 2009 Annual Study: U.S. Cost of a Data Breach, The Ponemon Institute, January 2010

Key Data Breach Prevention Mandates

IT Security

The Federal Energy Regulatory Commission (FERC) has mandated IT security regulations that the North American Electrical Reliability Corporation (NERC) has written and enforces. NERC has issued nine Critical Infrastructure Protection (NERC CIP) standards designed to protect the electrical grid from cyber attacks launched by either outside or inside threats.

Critical Infrastructure Protection

In addition to protecting IT systems, NERC CIP requires energy companies to mitigate exploitable vulnerabilities between IT networks and Supervisory Control and Data (SCADA) systems that control the mechanical processes of critical infrastructure. Stuxnet illuminated how data breaches could open energy companies to cyber attacks on SCADA systems that could have potentially horrendous, or even lethal, physical consequences.

Business Compliance

Energy companies want the advantages of online payment and other e-commerce capabilities and therefore must comply with commercial and government regulations, such as Payment Card Industry (PCI) requirements and Sarbanes-Oxley (SOX). Failure to comply can forbid violators from performing online credit card transactions, which can severely damage both profitability and customer trust.

Notice of Breach

Energy companies must comply with federal data protection legislation, including the Health Information Portability and Accountability Act (HIPAA), as well as state data breach notification laws mandating public disclosure of breaches that may compromise customers' personal information. Forty-six states and the District of Columbia now have such laws and Congress is debating a national law. Disclosure often brings negative public reaction, government scrutiny and hefty fines.

Self-Encrypting Drives and Wave's EMBASSY® Software: Keeping Energy Companies' Data Safe

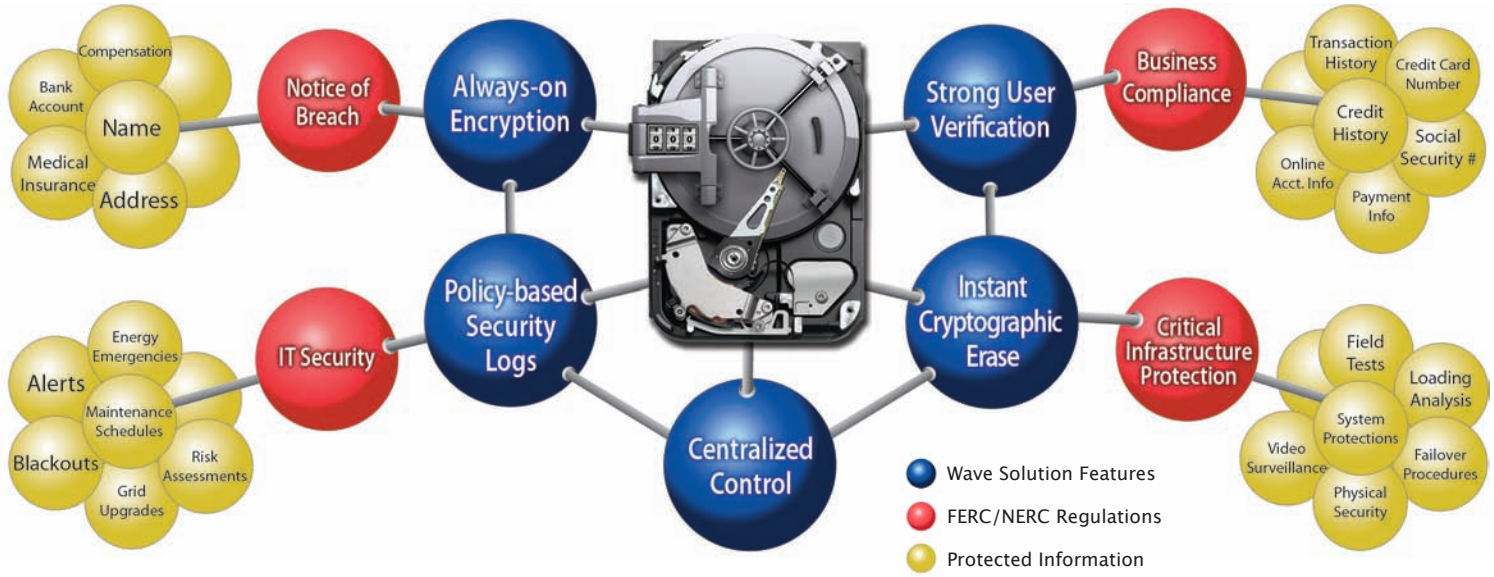
By embracing enterprise and mobile technologies and recognizing their vulnerability to cyber attacks, energy companies are more aware than ever of their need to protect sensitive data. Additionally, lost or stolen laptops accounted for more than one-third of data breaches in 2009, making securing information on these devices an essential element of energy companies' security and compliance strategies.

Options abound for protecting sensitive data but many experts consider full-disk encryption (FDE) the best because it encrypts everything on a hard drive, eliminating many vulnerabilities that attackers can exploit to gain unauthorized access to data. Unfortunately, software-based FDE, the most common form of FDE, has exploitable weaknesses — which means it can't guarantee that lost data is unreadable as required by IT security regulations and data breach notification laws. This fact leaves users — including energy companies — at continued risk of costly legal action.

To overcome these hurdles and thus achieve compliance with mandated regulations, more enterprises are turning to self-encrypting hard drives (SEDs). SEDs offer an alternative hardware-based FDE approach — making them more secure and less expensive to implement and maintain. SEDs house all encryption processes and keys in a protected hardware boundary impervious to traditional software attacks. Further, they cost only marginally more than non-encrypted hard drives, require minimal IT overhead and are transparent to end users.

Wave Systems, a pioneer in hardware-based laptop security, has partnered with leading hard drive manufacturers Hitachi, Samsung and Seagate to provide enterprise security management for their SEDs. Wave's EMBASSY software transforms these self-encrypting drives into a complete managed enterprise encryption solution: one that centrally provisions security policies, limits access to only authorized users and — perhaps most importantly — proves whether or not sensitive information stored on a laptop was encrypted at the time it went missing.

Because energy companies in particular often have IT infrastructure that mixes new and existing technology, Wave understands the need to protect information on PCs that do not have self-encrypting hard drives. Wave's EMBASSY software manages endpoint encryption equally well for all commercially available SEDs, integrated OS solutions, such as Microsoft BitLocker and legacy software-based solutions. Whatever your full-disk encryption needs, we've got you covered.



03-000284/ version 1.05

Copyright © 2011 Wave Systems Corp. All rights reserved.
Wave "Juggler" and EMBASSY® logos are registered trademarks of Wave Systems Corp. All other brands are the property of their respective owners. Distributed by Wave Systems Corp. Specifications are subject to change without notice.

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238
(877) 228-WAVE • fax (413) 243-0045
www.wave.com

wave®
Simplifying Encryption and Authentication