Electricity Advisory Committee

Implementing Effective Enterprise Security Governance

Outline for Energy Sector Executives and Boards

Introduction

As recent attacks, Presidential Executive Order for Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive 21 for Critical Infrastructure Security and Resilience have illustrated, managing security risks to our most important organizations and systems, including the electric grid, has become a national security priority. Enterprise security program effectiveness for both physical and cyber is now a CEO and Board-level concern and is called out as essential in the Department Of Energy's Electric Sector-Cybersecurity Capability Maturity Model (ES-C2M2).

Responsibility for physical and cyber security belongs not solely to technical, risk, or compliance specialists, but rather to the entire organization. It begins with senior leadership and extends throughout the enterprise to foster a more security-aware culture.

Organization-wide business processes must be adjusted to take into account the riskscape introduced by today's dynamic and evolving security threats.

Substantial changes to business-as-usual are required to adequately safeguard critical energy infrastructure, satisfy regulatory requirements, and protect customer data and corporate reputations. Changes of this magnitude can only be accomplished with the full support and leadership of senior executives and a new approach to Enterprise Security Governance.

A good place to start is with Carnegie Mellon CERT's definition of governance:

> *A process of providing strategic direction for the organization while ensuring that it meets its obligations, appropriately manages risk, and efficiently uses financial and human resources. Governance also typically includes the concepts of:*

EAC
Electricity Advisory Committee
U.S. Department of Energy

***1.1.1 Sponsorship:** setting the managerial tone*

***1.1.2 Compliance:** ensuring that the organization is meeting its compliance obligations, and*

***1.1.3 Alignment:** ensuring that processes such as those for cybersecurity program management align with strategic objectives*

In organizations large and small, effective enterprise security program governance should seek to drive a single, holistic, apples-to-apples view of the security and regulatory posture. Implementation of effective program governance will take time. For large companies, it may take several years. Not every company will have the internal resources to accomplish this, but even partial movement in this direction will better enable senior business leaders to understand enterprise risks, make business decisions that spare them unnecessary security expense and risk, and derive business value from their security investments.

This document provides a high level outline, suitable for senior business executives. The EAC recommends that DOE promote the establishment of enterprise security governance as a corporate norm in the Energy Sector in the near term.

I. Why Security Governance and Why Now

- Recognition of need for improved security understanding and awareness throughout Energy Sector organizations, particularly in senior management ranks
- The idea that implementation of effective enterprise security governance creates a safer business community for the company and for those that interact with them is not currently well-understood.
- Precedents in other strategic domains: audit, risk, compliance
- Why Now: Utilities face increased technological complexity and escalating security threats to strategic investments, as well as a highly dynamic regulatory environments

II. Characteristics of Effective Security Governance

- Clearly defined responsibilities from the board of directors to senior leadership to employees
- Presence of an active Security Governance Board comprised of senior stakeholders from across the company
- An executive owner of Enterprise Security: with purview over IT, OT and Physical security policy, designated CSO or similar
- Striving for 100% alignment with of security with business/mission
- Using measurement of key indicators to increase awareness and drive improvement (with maturity tools like the C2M2)

III. Security Governance Enablers

- Senior business leadership: striving to increase their own understanding and their entire organization’s Security awareness

- Senior Security leadership: seeking to communicate security conditions and requests in purely business terms
- Culture change: top down leadership by example can accelerate what might otherwise be a slow process of transformation
- Security factored into all business decisions: giving security a seat at the table when considering M&A, partnering, sourcing, hiring, etc. can save money and reduce security risk

IV. Outcomes and Benefits

- Better cost management: optimized capital and operational costs
- Risk managed: performance metrics with clear accountabilities and strategic business alignment
- More confidence via checks and balances: No party can make unilateral security decisions without influence, input or approval from other Security Governance Board members
- More secure: centralized point of authority provides common operating picture (COP) across the enterprise, enabling better understanding of current risk posture and ultimately appropriately resourced security efforts
- More aware: leaders and employees know their organization's security and privacy risks, know how to identify threats and constantly monitor for security/privacy risks

V. Recommendations

- Champion Enterprise Security Governance with the Electricity and the Oil and Natural Gas Subsector Coordinating Councils
- Establish Chief Executive Officer security awareness opportunities in coordination with the Department of Homeland Security, Trade Associations, Nuclear Energy Institute, North American Electric Reliability Corporation, and the Federal Energy Regulatory Commission
- Leverage the ES-C2M2 security governance areas to emphasize CEO and Board-level engagement
- Continue classified-level threat briefings targeted for the CEO and Board-level audience
- Identify industry best practices for engaging CEO and Board-level audience

VI. Best Resources

- DOE's Electric Subsector Cybersecurity Capability Maturity Model (ES-C2M2) http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model
- DOE's Risk Management Process (RMP) Guideline http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012
- Carnegie Mellon University's Computer Emergency Response Team (CERT) Governing for Enterprise Security Implementation Guide http://www.cert.org/governance/ges.html
- NARUC's Cybersecurity for State Regulators 2.0 http://www.naruc.org/grants/Documents/NARUC%20Cybersecurity%20Primer%202.0.pdf
- Cybersecurity Questions for CEOs https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf

VII. For more information, contact:

Chris Peters, Entergy, cpeter6@entergy.com

Andy Bochman, Bochman Associates, ab@bochmanassociates.com