Bridging the Security Governance Divide in Utilities
About Me

- Energy Security Advisor to utilities, regulators, integrators, energy start-ups
- Member:
  - GTM GridEdge Exec Council
  - ISC-ISAC Corporate Board
- SME Contributor to:
  - DOE Electricity Subsector-Cybersecurity Capability Maturity Model (ES-C2M2) & Risk Management Process (RMP)
  - NISTIR 7628 Guidelines for Smart Grid Security & NIST Critical Infrastructure Security Framework (CSF)
  - NARUC Cybersecurity Guidelines for State Regulators
  - DOD Software Assurance Working Groups
  - MIT Future of the Grid Report
- Founder of Smart Grid Security and DOD Energy blogs
Agenda

- New News
- Defining Security Governance
- Government Governance Guidance
- Utility CEOs and CISOs
New News

• FERC tells NERC we need new physical controls - stat!

• Financial Services realizing an OT problem of sorts: Windows XP in ATMs

• Target announces it’s time to get a real CISO

• DOE EAC Security Governance success
Security Governance Defined
(at the individual business level)

- Management through measurement and improved communications (vs. guessing, hoping, etc.)
- Including security considerations in all business decisions
- Organizational update actions that signal culture change to all stakeholders
Government Perspective
Energy: the most critical of all critical infrastructures
The security of the grid is so important we’ve assigned government agencies to watch over it.
Recent Government Guidance

Federal government wants to see senior leadership playing a more active role in security risk management.
Utility Perspective
That was Then: How Utilities (& others) Secured IT Pre-Smart Grid

Protected PCs

Protected IT networks

Protected physical assets
This is Now

EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS. POWER PLANTS. IPHONES. WIND TURBINES. REFRIGERATORS. VOIP PHONES.

TAKE A TOUR  FREE SIGN UP

DEVELOPER API
Find out how to access the Shodan database with Python, Perl or Ruby.

LEARN MORE
Get more out of your searches and find the information you need.

FOLLOW ME
Contact me and stay up to date with the latest features of Shodan.
Organizational blind spots - Senior leaders & org structure dictate what’s visible
Most utilities are still organized to meet yesterday’s threats
Security Questions CEOs Should be able to Answer

- Do I have the right security organization for my enterprise and is it aligned with our overall governance structure?
- Do we have contingencies ready for major cyber security or privacy incidents?
- Can I trust the integrity of the data that’s running our business?
- How do I communicate effectively to my board on security & privacy matters?
- Am I making the right/best investments in security?
- Do I have a complete and accurate inventory of all assets requiring protection?

© 2013 Bochman Advisors
Bridging the Utility Cyber Security Gap

CEO & Board of Directors

Security Leadership
Bridging the Utility Cyber Security Gap

CEO & Board of Directors

Security Leadership

Other players & stakeholders

CFO
GC
VP Risk
VP Customer
VP Operations
CIO/VP IT
Bridging the Utility Cyber Security Gap

Drivers for Increased Understanding & Collaboration

- CFO
- GC
- VP Risk
- VP Customer
- VP Operations
- CIO/VP IT
Drivers for Increased Understanding & Collaboration

1. Increasing interconnection of important systems
Drivers for Increased Understanding & Collaboration

1. Increasing interconnection of important systems

2. Security breaches viewed as material risk
Drivers for Increased Understanding & Collaboration

1. Increasing interconnection of important systems
2. Security breaches viewed as material risk
3. Greatly heightened awareness
Drivers for Increased Understanding & Collaboration

1. Increasing interconnection of important systems
2. Security breaches viewed as material risk
3. Greatly heightened awareness
4. Attacks growing in strength and frequency
CEOs: 2 Bridge building places to start
1: A new governance board or committee
Or add security to existing board or committee
2: A new security position outside of IT & closer to top
It could go here
Or here …
Feb 2014: Alliant recently created an executive-level opening company for overseeing cyber and physical security.

The position is designed to bring cyber issues out of the weeds of the IT shop, where CEOs generally don't tread.

Alliant Energy
CIO Patricia Kampling
CISOs: Bridge building places to start

CTO Erich Gunther
Approaches that Fail

- Attempt to explain issues technically
- Deluge with statistics
- FUD and “The Sky is Falling”
- Using regulations to fix problems
Approaches that Work

- Best practices catalog for practitioners
- Value props w clear business metrics
- Security built into all processes & quality system
- Visible lines of ownership & responsibility
- Risk based model CEOs, lawyers, regulators, insurers can trust
Do these things

• Improve communications skills
• Get better versed in core business you’re/we’re protecting
• Take business value and risk management approach to security
good things happen when they meet

CEO
Grow the Business

Reduce Business Risk

Corporate Governance

Cultivate Desired Culture

CSO
Facilitate/Integrate with Business

Set & Enforce Security Policy

Security & Resiliency Staffing & Training

Promote Security-Aware Culture

Security informs & supports business decisions

Security controls align with corp risk tolerance

The human elements of security risk are managed

Both lead by example with a focus on communication
Thank You

ab@bochmanadvisors.com
781.962.6845