TRANSFORM
Governance • Coaching • Consulting

Board Briefs – Director Education

Cyber Security

Dangers in the Brave New World

Board Essential Responsibilities

- Select, manage, compensate, coach and replace the CEO.
- Constructively engage in setting the strategic direction.
- **Oversee and monitor risks and results.**
- Orchestrate the succession of the Board.

Defining Cyber Security

The body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

Ref. What Is, Tech Target.com

Entering the Brave New World

Yesterday

Isolated Mainframes

Wired Networks

Accounting Systems

Local Control Terminals

Today and Tomorrow

Distributed and Cloud Computing

Laptops, Tablets and Cell Phones (BYOD)

Wireless Networks and Internet

e-commerce and Social Networks

Hacking, Cyber Crime and Terrorism

Integrated Digital Control Systems

Current Reality

High Profile Examples

- eBay
- Sony
- Target
- Home Depot
- JP Morgan Chase
- Goodwill Industries Int'l.
- Governments and military

Impacts

- Massive data breaches
- Identify theft
- Credit card breaches
- Theft of intellectual property
- Infrastructure threats
- Denial of service
- Embarrassing information

Small and Medium Business

Of 998 businesses surveyed, 74% experienced online bank fraud

- 85% related to credit card fraud
- 85% suffered unauthorized account access
- 19% unauthorized wire transfers
- 36% reported check fraud from stolen account information
- Individual losses ranged from a few thousand to $1.2 million
- 59% of the businesses were not reimbursed by their banks

Ref. 2012 Business Banking Trust Study, Ponemon Institute

Core Cyber Risks

- Customer harm – disclosure of personal and financial information
- Financial loss – fraudulent transfers
- Operations interruptions – system and equipment malfunctions
- Asset impairment – intellectual property theft
- Reputation harm – loss of market confidence

All organizations, big and small, are at risk!

Some Underlying Issues

- Slow software patch updating
- Internet browser vulnerabilities
- Installation of personal software
- Lax employee security practices
- Outsourcing weaknesses
- Professional hacking
- “Phishing” attacks
- Insider retribution

Protection and Mitigation

- Regularly update and enhance computer and network security.
- Continuously monitor and learn from breach attempts.
- Prioritize the greatest threats and invest accordingly.
- Implement data and control systems redundancies.
- Assess the adequacy of internal controls.
- Automate your defense responses.
- Investigate cyber risk insurance.

Ref. Adapted from Critical Security Controls for Effective Cyber Defense, CCS

The State of Cyber Security Governance

- Directors acknowledge that big data and cloud technologies are two areas that could use more of their attention.
- Only 26% of directors very much believe that management provides the Board with adequate information on IT strategy and risk mitigation for effective oversight.
- 38% of Directors now use external IT consultants (26% in 2012).
- Nearly half of Directors have not discussed their company's crisis response plan in the event of a security breach.

Ref. 2014 Annual Corporate Director Survey Highlights, PWC

Cyber Security Governance Principles

1. Understand and approach cyber security as an enterprise-wide risk management issue, not just an IT issue.
2. Understand the legal implications of cyber risks as they relate to your company's specific circumstances.
3. Obtain adequate access to cyber security expertise, and regularly provide time during meetings to discuss cyber risk management.
4. Require that management establish an enterprise-wide cyber risk management framework with adequate staffing and budget.
5. Discussions on cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

Ref. Cyber Risk Oversight Handbook, NACD

Expectations of your CEO & CIO

- Obtain expert assistance.
- Complete a detailed risk analysis.
- Identify the most important data assets.
- Implement appropriate protection measures.
- Learn from successful and attempted breaches.
- Develop performance indicators.
- Report candidly to the Board.

When Your Systems are Breached

- Murphy's Law – if anything than can go wrong, it will go wrong.
- Develop backup and contingency plans.
- Select your spokesperson.
- Determine your approach to transparency.
- Demonstrate leadership, creativity and flexibility.

Board's Role in Cyber Security

- Include as a key threat in your risk management process.
- Rely on both the CEO and the CIO for information.
- Identify specific risks and protection measures.
- Recruit Directors with appropriate expertise.
- Schedule regular cyber security audits.
- Monitor breaches and attempts, and learn.
- Plan ahead for a robust response to breach events.

Questions to Consider

1. How would describe the Board's current knowledge and awareness of cyber security issues?

2. What is your current confidence level in the organization's ability to deal with cyber risks and threats?

3. Which Committee should be tasked with cyber security details?

4. What steps should you take to improve cyber security?

Additional Services We Offer

We can help you take your Board to the next level by providing:

- Customized workshops and training
- Governance reviews and Board evaluations
- Strategy development and meeting facilitation
- Director orientations

Please contact us at:

- 613-692-4778
- jlevesque@transformgcc.com