

Cybersecurity as a Risk Management Protocol

Emphasizing the Director's Role in Assessing and Addressing These Risks

Lessons Learned: Case Studies / Best Practices

Cybersecurity: Boards' top agenda item

Focus: Cyber risk reduction

Preparedness: 2 elements (Proactive + Reactive)

Cybersecurity: Context 2016

- National Security issue: \$500B - \$5T each year (*one third of U.S. GDP*) *BLACKOPS Partners Board*
- "The Cybersecurity Industry is Fundamentally Broken" *RSA President*
- "Cyber Crime is the Greatest Threat to Every Company in the World" *IBM CEO*
- "The Greatest Transfer of Wealth in History" *NSA and U.S. Cyber Command former Director*
- 11% average annual IT budget increase / 400% increase in data breaches in 2015 / 90% breaches not included / 95% data breaches caused by human intervention
- Increasing breach incidents and severity: increased board exposure
- Accelerated organizational, personal, financial and reputational risk

Proactive Measures - Risk reduction - Risk mitigation - Case Studies

Board Risk: Personal - Company - Shareholder

'Active Oversight' - Protect shareholder value: revenue, profit, trade secrets, innovation

Regular board awareness and action briefings with active intelligence

Board: third-party retainer / fulfills SEC requirement

CyberLaw

Board Hygiene and Cyber assessments

Organization: Ongoing Awareness Certification

Cybersecurity SOP & Insider Threat Program

Include contractors, vendors, supply chain

Documented cybersecurity plan

Documented breach (Tabletop-TTX) exercise

Reactive Measures

Board: third-party, unbiased (*no products*) cyber advisor retainer

Enact breach response: It will happen

Reaction time and message proven critical to protecting brand (reputational) and financial risk

Include entire supply chain

Key Takeways

- Board's 'Active Oversight' role
- Effective risk reduction must be proactive
- Must be a company-wide effort: no longer an IT-only issue
- Ongoing preparedness: both Proactive and Reactive
- Never assume your organization is safe
- Stay current on Cybersecurity issues at the Board level
- Take corrective action: policy change, culture change, funding allocation

Director Cyber resource: 'Follow Us' on LinkedIn for current board Cyber coverage feed

https://www.linkedin.com/company/blackops-partners-corporation?trk=company_logo

