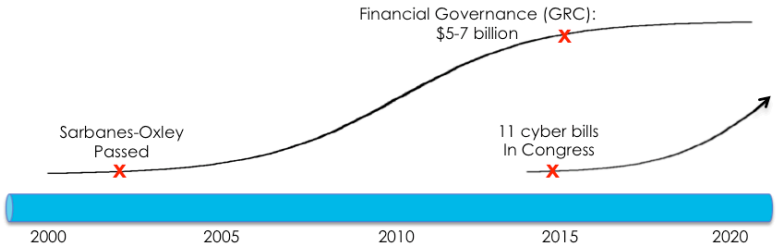
How to Address Cybersecurity Governance

"...directors could or should be held personally accountable for cyber security breaches..."

– SEC Commissioner Luis Aguilar in the Harvard Law School Forum

Post-breach regulatory actions and shareholder lawsuits threaten to pierce the personal corporate veil that shields directors from liability. Statements from the SEC, actions taken by the FTC, and rulings by the courts increase the likelihood that directors will become targets after a breach if they have not exercised prudent oversight and duty of care.

Directors have begun to realize how critical their oversight of cybersecurity preparedness has become. In a recent survey of 276 directors by the New York Stock Exchange, 60% say they expect an increase in shareholder suits, and 72% expect increased government regulation. For example, the Cybersecurity Disclosure Act recently introduced in Congress would require each company to report whether it has a cybersecurity expert on its board, and if not, to explain what alternate steps it is taking to protect its systems from cyberattacks. Are we possibly facing the equivalent of Sarbanes Oxley for cybersecurity?



	Financial Governance	Cybergovernance
Instigation	Rash of highly publicized frauds (e.g. Enron, WorldCom)	Rash of highly publicized breaches (e.g. JPMorgan Chase, Target)
Motivation	Restore loss of public and investor confidence due to financial scandal (INTERNAL THREAT)	Restore loss of public and investor confidence due to cyber breaches (EXTERNAL THREAT)
Challenge	Mitigate financial risk	Mitigate cybersecurity risk
Solution	Stricter financial governance laws	Stricter cybersecurity governance laws
Driver	Senate Banking Committee	SEC, FTC, FINRA, CFPB
Outcome	Sarbanes-Oxley Act (2002)	11 bills currently in Congress (2015)

"It's critical that we start to demystify cybersecurity for the director community. Directors don't need to be technology experts, but they must play an effective role in cyber-risk oversight."

–Ken Daly, CEO, National Association of Corporate Directors

How to Empower the Board

Cybergovernance does seem to be tracking the path that financial governance followed before the Sarbanes-Oxley Act passed in 2002 (see diagram above). With the number of cybersecurity compliance bills being introduced in Congress, knowledgeable observers believe that passage of a significant cybergovernance compliance bill is not far away.

Two alternatives have emerged to help boards oversee cybersecurity risk mitigation more effectively:

1. **Add a cybersecurity expert to the board.** This has worked for several large companies. An obstacle, though, is the dearth of available talent. The 2014 Cisco Annual Security Report projected a 500,000 to 1,000,000 person global shortage in the number of IT security professionals. Also, few cyber experts have the experience to deal with other board issues, and overly close technical direction can introduce significant board liability if the board is overly prescriptive.
2. **Demystify cybersecurity for current board members.** Given that technology alone won't solve the problem, emerging insight suggests that other elements can make boards more effective in overseeing cyber risk, namely, broader engagement and continual monitoring.

   While cybersecurity technology continues to improve, all stakeholders (e.g. HR and Procurement) must begin taking measures to avoid introducing new sources of risk from employees, partners, and vendors. Introducing a governance model based on the NIST Framework can facilitate business-level communication among directors, executive management, and security professionals about the entire organization's cybersecurity responsibilities.

   Continually measuring and monitoring of progress using a common NIST-based model can keep directors apprised of the organization's initiatives, and it can protect them from post-breach suits that allege a lack of prudent oversight. Rapid assessment, continuous monitoring, and using a common risk index can provide boards and insurers more insight into cyber maturity.

How to Protect the Board

How can a board oversee cybersecurity more effectively and protect itself from liability?

1. **Resolve to get involved in cybersecurity oversight.** A cyber event may outweigh all other forms of risk; not exercising duty of care can incur significant liability. Prudent oversight requires understanding and tracking steps that should be taken to mitigate cyber risk, yet without the board's prescribing the technologies used.
2. **Know the relative maturity of your cybersecurity program.** It is as much a fiduciary duty as reviewing financial progress. Many boards don't include cybersecurity as a regular agenda item. Even those that do may view reports that focus on arcane security metrics and tactical technology issues. Insist on ways to assess and track improvements in enterprise-wide cyber attack readiness that don't require board members to have deep technical expertise.
3. **Clarify your D&O provider's cyber coverage.** Providers of Directors' and Officers' Insurance are challenged by the lack of data to assess inclusion of cyber coverage. Some have "carved out" cyber risk already. Ask management to regularly review D&O coverage and to assess cyber maturity regularly so it can be reviewed and tracked by the board.

Provided by Cybergovernance Journal

CybergovernanceJournal.com publishes online articles each week regarding issues relevant to effective board oversight of cyber risk.