SIDLEY AUSTIN LLP

SIDLEY

BEIJING BOSTON BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG HOUSTON LONDON LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

Cybersecurity: Board Preparedness

Cameron F. Kerry

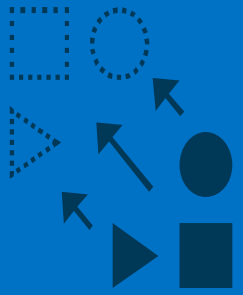
March 10, 2016

Threat and Risk Models

Attacks

Cybercrime

Military, political & economic espionage



Insider threats

- Risk Assessment
  - Identify
  - Analyze
  - Evaluate
- Risk Management
  - Prevent
  - Prepare
  - Respond
  - Recover

SIDLEY AUSTIN LLP
SIDLEY

The Actors

THREATS	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
						
MOTIVATION	Hacktivists use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

The Anatomy of a Hack

SIDLEY AUSTIN LLP
SIDLEY

Who Is Responsible for the Threats?

- Global organized crime
- Hackers
- “Hacktivists” (hackers with a cause, e.g., Anonymous)
- Careless employees
- Malicious insiders (e.g., Snowden, disgruntled and departing employees)
- State-sponsored actors (China, Russia, Iran, etc.)

What Laws Are Involved?

- GLBA, FTC Act, HIPAA, FCRA, etc.
- Executive Orders
- An expanding array of federal agencies: FTC, SEC, CFTC, CCC, FFIEC, FCC, etc.
- State information security laws and regulation requiring “reasonable” security
- Data breach notification laws
- Negligence standards
- International data protection, data breach notification, and data security laws

NIST Cybersecurity Framework

- Five core functions for dealing with cybersecurity risk:
  - identify, protect, detect, respond, recover
- Voluntary framework
- "Attestation" of compliance being developed by private sector
- NIST released request in December 2015 for information on implementation of NIST and whether there is a need for a Cybersecurity Framework 2.0.

NIST Framework Is Major Call to Action

- Aimed at helping organizations:
- (1) **identify** cybersecurity risks and vulnerabilities
- (2) **protect** critical infrastructure assets
- (3) **detect** the occurrence of a cyber event
- (4) **respond** to a detected event
- (5) **recover** from a cyber event
- Draws on, correlates and does not supersede existing standards: ISO, COBIT, prior NIST publications, etc.
- Defines “implementation tiers” (via self assessment)

SEC Commissioner Aguilar on NIST

- Boards should consider NIST Cybersecurity Framework for industry standards and best practices for managing cybersecurity risks
- While Framework is voluntary, many expect it will be baseline for best practices for assessing legal or regulatory exposure or for insurance purposes:
  - "At a minimum, boards should work with management to assess their corporate policies to ensure how they match-up to the Framework's guidelines."

Cyber Risks and the Boardroom: The SEC's Expanding Role

- 2009: Amended rules to require disclosure about board's role in risk oversight
- 2011: Guidance on disclosure of cyber-risk
- June, 2014: Commisisoner Aguilar speech on need for board engagement
- February, 2015: OCIE *Examination Report*
- March, 2015: Roundtable with Chairman White
- April, 2015: DIM *Cybersecurity Guidance*
- September, 2015: OCIE *Risk Alert*
- September, 2015: Enforcement action against R.T. Jones

"Risk Oversight Is a Key Competence of the Board"

- Investors need disclosure about board's involvement in risk management process and relationship between board and senior management in managing material risks
- Directors on notice to address risks associated with cyber-attacks:
  - Not only significant business disruptions, substantial response costs, negative publicity, lasting reputational harm, threat of litigation, but also
  - Derivative lawsuits against companies, officers and directors alleging liability for failing to take adequate steps to protect company from cyber-threats
  - proxy advisory firm urged ouster of most Target Corporation directors because of alleged "failure…to ensure appropriate management of [the] risks" regarding December 2013 cyber-attack

Board Preparedness

- Prepare company for inevitable cyber-attack and resulting fallout
- Primary distinction of cyber-attack is speed needed for response to detect and analyze event and prevent further damage
- Board needs to dedicate time and resources to confirm management response is consistent with best practices in same industry
- Plan should contemplate need for internal and external disclosures (including customers and investors)
- No substitute for preparation, deliberation, and engagement on cybersecurity

What Boards of Directors Can and Should Be Doing to Oversee Cyber-Risk

- SEC does not mandate any particular structure
- Many boards lack necessary technical expertise
- Audit committee may not have expertise, support, or skills to add oversight of cyber-risk management
  - Consider mandatory cyber-risk education for directors; add members with relevant technology background
- Consider separate enterprise risk committee
  - Dodd-Frank Act already requires large financial institutions to establish independent risk committees
  - Some non-financial institutions have chosen to create such risk committees

Board and C-Suite Oversight

- Regular reporting on threats, planning and execution
- Ask: How do we stack up against NIST Framework? Against peer companies? Against (relevant) government expectations?
- Assign clear responsibility for cybersecurity function, including senior internal staff and outside consultants
- Cybersecurity is not just an IT issue; it requires a broad team
- Demand accountability
- Insist on testing the system (internal and penetration)
- Provide sufficient resources

Legal Considerations

- Keep up with fast-moving policy, public and litigation developments
- Identify legal obligations; preserve privilege
- SEC disclosures and public filings
- Data breach notification requirements
- Data security laws in US and EU for personal information (MA, other states, etc.)
- SEC and FTC expectations for information security, tracking and Internet of Things
- Sector-specific regulatory requirements
- Contractual obligations

Outside Resources

- Identify outside resources, including
  - Forensic analysts to identify and remediate cyber-attacks
  - Cyber consultants to enhance cyber-control systems
  - PR and communications specialists
  - Legal specialists
  - Information Sharing and Analysis Centers (ISACs); industry associations
  - Government agencies for coordination and advisory purposes

Paper Trail and Planning

- Comprehensive internal cybersecurity program
- Written information security plan
- Document organizational response to NIST
- Incident response and notification planning
- Business continuity planning to deal with serious cyber-disruption
- Address supply chain security
- Secure relationships with vendors and third parties
- Engage forensic experts, PR consultants, lawyers – in advance

Key Cybersecurity Questions to Ask

- Do we know what IP assets, records, data, systems are essential to protect?
- What past incidents have we experienced? Why? Are our incident response procedures effective and well understood throughout the organization?
- Do we have an up-to-date cybersecurity risk assessment in hand? Written information security plan?
- Who is responsible for cybersecurity? Who is monitoring NIST developments and best industry practices? Sufficient resources?
- Is Board of Directors adequately focused on cybersecurity; has it established satisfactory internal controls and governance structures?
- What do we need to include in our SEC filings on cybersecurity?
- Do we know what existing and prospective laws apply to cybersecurity?
- Are we participating in appropriate information sharing?
- Do we know what our contracts say about cybersecurity; do our existing customer / vendor contracts protect us on cybersecurity?
- Are we “critical infrastructure” operators? Do we have relevant government contracts? Do we have cleared persons?

SIDLEY AUSTIN LLP

SIDLEY

Questions?

Cameron F. Kerry: 617-223-0305 ckerry@sidley.com

www.Sidley.com/InfoLaw

This presentation has been prepared by Sidley Austin LLP as of January 27, 2016for educational and informational purposes only. It does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking personalized advice from professional advisers.

BEIJING BOSTON BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG HOUSTON LONDON LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.