They are coming for you! Security threats continue and no one is immune. Is your management prepared?

NACD Texas TriCities Program | November 5, 2015 | Houston, TX

SPEAKER KEY TAKEAWAY CONSIDERATIONS

Panelist | Kevin Mandia, President, FireEye
Panelist | Steve Rathgaber, CEO, Cardtronics

1. Assign Responsibility for Cyber-Risk at the Board Level

Should an incident occur, one surefire way to fail a third-party inspection or other external scrutiny is to have lingering questions about who is responsible for cyber-risk. If the board doesn't already have a committee devoted to security (sometimes combined with a committee tasked with addressing privacy issues and other cyber risks), consider forming one.

2. Determine the Risk Posture your Board Intends to Adopt

Once clear responsibility for cyber-risk has been established at the Board level, the committee assigned to address cyber risks must establish the corporate risk posture. In other words, how good do you want your cyber security program to be? Many companies assess their risk posture on an annual basis, taking into account recent incidents, changes in the law, industry practices, emerging threats and other changes. This assessment should include a realistic determination of how vulnerable the company is to attack, what types of attacks and attackers are most likely to be successful, and the kinds of data at risk. The assessment should also include recommendations for mitigating those risks so that the board can weigh the costs and benefits and determine what level of expenditure is appropriate.

3. Implement a Governance Framework that ensures Alignment in regards to Cyber Risks.

The company should implement a governance framework that requires compliance with legislation, regulation and best practices, including those specific to the company's industry and the type of data the company maintains. The framework should include prompt disclosures to the board in the case of problems and consistent interaction between the Chief Information Security Officer (CISO) and the applicable board committee. The framework may be proposed by the CISO, but third-party validation of the framework – both from a legal compliance and security perspective – is recommended. Also – the Board or Committee members involved in Cyber responsibility should determine how they intend to monitor and assess the corporation's security program.

4. Develop an Incident Response Communications Strategy.

Incident response is not the exclusive domain of the CISO. On the contrary, a company's incident response team should include members of several departments, including marketing (press relations), legal (compliance with breach notification regulations and general risk management), IT (impact on corporate systems), HR (internal communications), and executive management. An incident response strategy should include immediate notification of everyone on the incident response team, and implementation of a plan created prior to the incident when people aren't in crisis mode. Part of this plan will include external and internal communications, and a clear delineation of who is responsible for each task included in the plan.

Moderator | Suzanne Vautrinaut

President, Kilovolt Consulting, Inc. Major General, United States Air Force (Ret.)
Director, Wells Fargo, Symantec Corporation, ECOLAB Inc., Parsons Corporation

Moderator Notes - *When asked the "what should a Director read to get smart" question, I recommend…*

1. Read one of several good books (context), then
2. Review one or two of the available primers--several good ones;
3. Know about and discuss the government tool kits/standards with your management and potentially outside experts; and
4. Leverage government and agency websites & services as well as key industry Cybersecurity blogs (Your management/experts should be reading and your Directors should just be aware that they're available and ask how they're being leveraged.)

Good books for context...easy airplane reads:

- *Countdown to Zero Day* by Kim Zetter
- *Zero Day: The Threat in Cyberspace,* by Robert O'Harrow. It's a compilation of articles on various breaches from press reporting.
- *@War* by Shane Harris. It has good explanations of technical methods and events ...and works well for skimming chapters of interest.
- *Cybersecurity and Cyberwar* by PW Singer and Allan Friedman. A bit more academic, but thought provoking.
- *Inside Cyber Warfare* by Jeffrey Carr. While it is starting to be dated, it has a super explanation of hacker groups, background on Estonia/ Georgia attacks, and some of the legal/military considerations. Best if read by section...and a tougher read for folks just wanting context.

For primers or documents:

- The **NACD**, KPMG and PwC have very good Director Cybersecurity Primers for directors.
- In addition; DHS, NSA, my old AF command (24th Air Force), Symantec, Dell Secure Works, Mandiant and many others do "How To" and primers for personal and corporate use. Most are available on websites.
- Rich Baich and other experts just participated in a new book, which has been getting good reviews https://www.securityroundtable.org/the-book/

Tool kits and Regulatory guidelines:

- **NIST** framework (Which is also frankly a good C.Y.A. method since simply the fact of use is considered by DHS/FBI/Congress to be indicative of diligence.)
- **SANS Top 20**, which is a great personal and corporate checklist. Tony Sager was key in the development and collaboration internationally ...and remains a sage in the area.
- FFIEC also just published a new checklist.

Government and industry websites & blogs

- Cyber Resiliency Reviews: https://www.us-cert.gov/ccubedvp/self-service-crr
- Critical Infrastructure Cyber Community Voluntary Program: https://www.us-cert.gov/ccubedvp
- Cybersecurity Information Sharing and Collaboration Program: https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf
- Enhanced Cybersecurity Services**:** http://www.dhs.gov/enhanced-cybersecurity-services
- Information Sharing and Analysis Organization rollout:http://www.dhs.gov/isao
- National Initiative for Cybersecurity Careers and Studies: http://niccs.us-cert.gov

Industry blogs/sites: These are not specifically for Directors, but they can ask their cyber/IT professionals what they read and find useful...their folks should have a set of "go to" links along these lines for information, commentary and even breaking news on new IT security issues. Below is list of open Internet resources that many IT security professionals would read—at least a subset. None of these are 'secret' or require membership:
http://www.symantec.com/connect/symantec-blogs/sr
http://krebsonsecurity.com/
http://isc.sans.org/
http://thehackernews.com/
http://www.theregister.co.uk/security/

There is also specialty work, for example on infrastructure: *Aspen Institute on Critical Infrastructure Readiness*

NACD Board Leader's Summit in Washington DC held numerous Cyber programs. Visit the NACD Blog online or the NACD Online YouTube Channel to watch the individual sessions and download transcripts:

YOUTUBE: NACD Online

NACD Digital Director Programs: http://blog.nacdonline.org/category/the-digital-director/

- Putting a Boardroom Lens on Cyber
- Former Whitehouse CIO Discusses Data Hygiene and Cybersecurity

Dig deeper into leading practices by reviewing the Director's Handbook Series on Cyber Risk Oversight (Item 10688).

2016 NACD Cyber Summit June 15, 2016 | Chicago, IL

The speaker bios and additional resources on topics referenced in the program can be found at: https://texastricities.nacdonline.org/Resources/meeting.cfm