Dusting off the Cyber Playbook

NACD Texas TriCities Program | November 4, 2016 | Houston, TX

SPEAKER KEY TAKEAWAY CONSIDERATIONS

Moderator | Jasen Meece, Partner, IBM Global Security Services

We have often heard that, "opportunity and risk are two sides of the same coin", but how an organization goes about dealing with risk is a leading indicator to their future success (or failure). Cyber risk is no exception. Yet for some reason this topic has been elusive over the years, mired down in micro technical plans to address a macro strategic problem.

All too often the risk is either not fully understood nor is capital expenditure appropriately focused on the greatest areas of cyber risk. Leaving us in our current state where breaches have become all too common. When looking to comprehend cyber risk there are many different perspectives based on many different vantage points, generally tied to the latest tech trend or most recent headline on who was last compromised. We are currently in a state of "breach fatigue"- so much unstructured, unquantified, and unqualified information on cyber risk coming at us daily, that folks are lost in the noise as to what is most relevant to act on.

To get a handle on how to best mitigate cyber risk, an organization must take a holistic view (inclusive of: technology, governance, process, people and metrics) and tie the subsequent cyber strategy to an execution plan. Not take a host of technology plans and try to shoehorn them into a cyber risk strategy.

The first step is to have a well-established Board of Directors approach for how and where an organization will focus its cyber efforts. This is not in place of a corporate cyber strategy, it's a compliment to it. One way is to look at it in a 4-phased model to help Boards accomplish this as follows:

- Cyber Maturity
- Metrics
- Quantification of Cyber Risk
- Visualization of Cyber Risk

Panelist | Casey Fleming, CEO, BackOps Partners Corporation

- Cyber will continue as the #1 Board agenda item
- Directors have a fiduciary role in Cyber 'Active Oversight'
- Directors and CEO's must be the change agents: Culture, Policy, Funding Allocation
- Effective risk reduction must be proactive - we are reactive today
- Must be a company-wide and personal effort: no longer an IT-only issue
- Ongoing preparedness: both Proactive and Reactive
  - Perform regular data breach exercises - facilitated by a qualified third-party
  - Regularly classify your key data and limit access to it
  - Include all third party vendors, contractors, suppliers, law firms
  - Practice Cyber hygiene both personally (family) and professionally

- Never be satisfied, 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

Panelist | Gary McAlum, Chief Security Officer and Senior Vice President, USAA
Director, Internet Security Alliance

Cybersecurity and Risk Oversight

1. There are many questions for the Board to ask when it comes to cybersecurity, but a good place to start is with these 3 fundamental questions.
    - "Who's in charge?" and are there clear lines of accountability and responsibility?
    - "Do we have an incident response plan?" and have we validated it?
    - "What keeps your CSO/CISO up at night?" and what are they doing about it?

2. The most significant driver of cybersecurity vulnerability, in my opinion, is complexity….more complex and interconnected technologies and business processes as well as increasing dependence on an extended supply chain. Failure to understand that this complexity must be understood and managed is often a root cause of cybersecurity risk.

3. "There are no cybersecurity silver bullets…today's cyber threats are too agile, too innovative, and too well resourced. A strong security program has many characteristics but the most important element is ensuring a culture of non-complacency.

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...staff 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/

NACD is preparing to launch a new cybersecurity certification online educational program in conjunction with Carnegie Mellon University among others. The new program will be announced in December! Stay tuned for more information!

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).

NACD Texas TriCities Chapter Past Program Page

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