Cybersecurity in the Boardroom

BoardEffect

Housekeeping

Webinar will last 45 minutes (15 min for Q&A)

Session is being recorded

Phone lines are muted – please ask questions through the Q&A box

Follow-up email after the session will include the recording, resources, and a short survey

BoardEffect

Presenter

Dottie Schindlinger, Executive Director, Diligent Institute

- Heads the corporate governance research arm and think tank of Diligent Corporation at diligentinstitute.com.
- Co-author of Governance in the Digital Age: A Guide for the Modern Corporate Board Director, ©2019, Wiley & Sons.
- Co-host of The Corporate Director Podcast.
- Fellow of the Salzburg Global Seminar, Corporate Governance Forum.
- Vice Chair of the Board of Alice Paul Institute.
- Founding team member of BoardEffect.

Topics We'll Cover Today

- Overview of the board's role in cyber risk oversight
- Review some of the latest stats and trends in cyber risk
- Discuss how boards can be better prepared for cyber incidents

Cyber Risk by the Numbers

"Up fourfold"

Increase in cybercrime since March 1, 2020, as reported by the FBI in April 2020

$6 Trillion

Cybercrime economy as of 2021

$137 Billion

Global spending on cybersecurity by 2022

62%

Of businesses experienced phishing and social engineering attacks as of 2018

5%

Only 5% of companies' folders are properly protected

56 days

Length of time before a breach is detected on average in 2019 – down from 416 days in 2011.

Check out "Have I Been Pwned?" haveibeenpwned.com

Varonis, with data from various sources; and from FireEye's 2020 M-Trends report.

BoardEffect

Anatomy of a Breach – What We Know So Far…

- July 15, 2020 attack focused on small number of “high profile” accounts
- Attack was carried out by young, relatively unsophisticated attackers
- Scheme used social engineering on a Twitter employee to gain access
- Internal dashboard gave Twitter staff broad access to all accounts
- Attackers made over $100k in Bitcoin before the scheme was shut down
- Twitter lost $1.3 Billion in market value in trading the following day
    - **Lots of coverage, but a good summary is on Business Insider, with more detailed coverage in Motherboard**

Cybersecurity vs. Cyber Resilience

Cybersecurity – programs and processes in place to protect hardware, networks, and data from cyber incidents

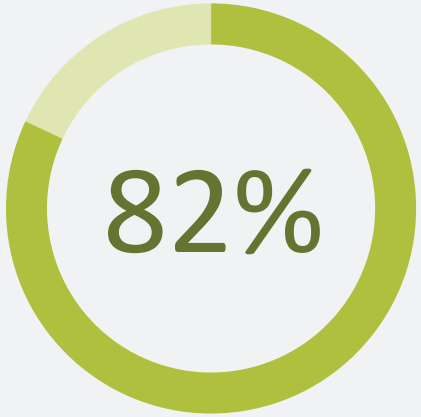
Cyber resilience – the ability to withstand a cyber incident, including:

- Programs & processes in place to ensure operations can continue with minimal disruption both during & after an incident
- The speed and agility of the organization's response to cyber incidents
- The ability of the organization to retain & rebuild the trust of stakeholders after a cyber incident occurs

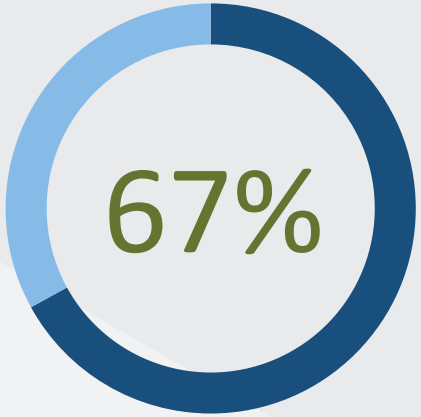
Are Boards of Directors Cyber-Ready?

BoardEffect

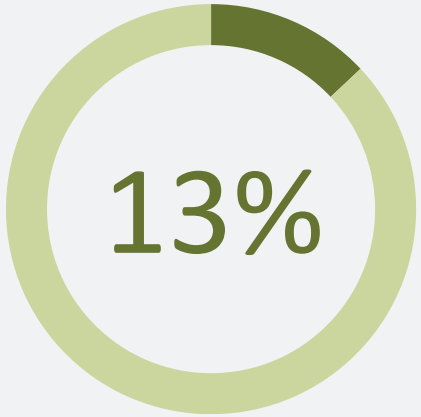
Are Boards Cyber-Ready? Example: School Boards…



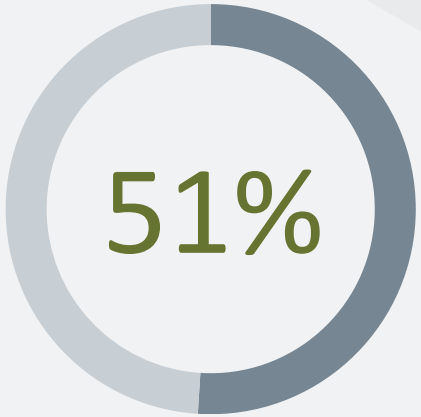
School boards have **never conducted a security audit** of board communication



School boards **don't require cybersecurity training**



IT/Data security teams that oversee the **security of board communications**



School boards **"don't know" if there is a cyber crisis plan** in place; another **39% know there isn't one.**

NSBA 2018 Cyber Risk Report: School Board Communication at Risk

BoardEffect

What methods do boards use to communicate?

92%

use personal email to communicate with fellow directors & management, at least occasionally

The Price of Convenience, NYSE & Diligent, 2017

Are boards required to participate in cybersecurity training?

62%

said “No”

The Price of Convenience, NYSE & Diligent, 2017

BoardEffect

What Is the Board's Role in Cyber Risk Management?

BoardEffect

What's the Board's Cyber Risk Oversight Responsibility?

- Part of the board's "Duty of Care" is to ensure customers are treated appropriately, and their data is maintained securely
- Recent/new legislation includes strong provisions –
  - Big fines/penalties for organizations that demonstrate negligence (or willful misconduct) on data privacy (e.g., EU-General Data Protection Regulation (GDPR), NY Department of Financial Services Cybersecurity Regulation, California Consumer Privacy Act)
  - Shareholders/stakeholders increasingly holding leaders accountable for data breaches
  - Example: Shareholders sue for data breaches

NACD Cyber Risk Oversight for Board Members – 5 Principles

1. Understand and Approach Cybersecurity as an Enterprise-wide Risk Management Issue, Not Just an IT Issue
2. Understand the Legal Implications of Cyber Risks as They Relate to the Company's Specific Circumstances
3. Have Adequate Access to Cybersecurity Expertise and Give Cyber Risk Management Regular and Adequate Time on Board Meeting Agendas
4. Set the Expectation That Management Will Establish an Enterprisewide Risk Management Framework With Adequate Staffing and Budget
5. Management Discussions Should Include Identification of Which Risks to Avoid, Which to Accept and Which to Mitigate

2017 NACD Cyber-Risk Oversight Handbook: Principles and Practices for Corporate Boards

Five Questions for Directors to Ask

- How are the company's cyber risks communicated to the board, by whom and with what frequency?
- Has the board evaluated and approved the company's cybersecurity strategy?
- How does the board ensure that the company is organized appropriately to address cybersecurity risks? Does management have the skill sets it needs?
- How does the board evaluate the effectiveness of the company's cybersecurity efforts?
- When did the board last discuss whether the company's disclosure of cyber risk and cyber incidents is consistent with SEC guidance?

  - Source: Council of Institutional Investors

Questions?

BoardEffect

Thank you!

BoardEffect