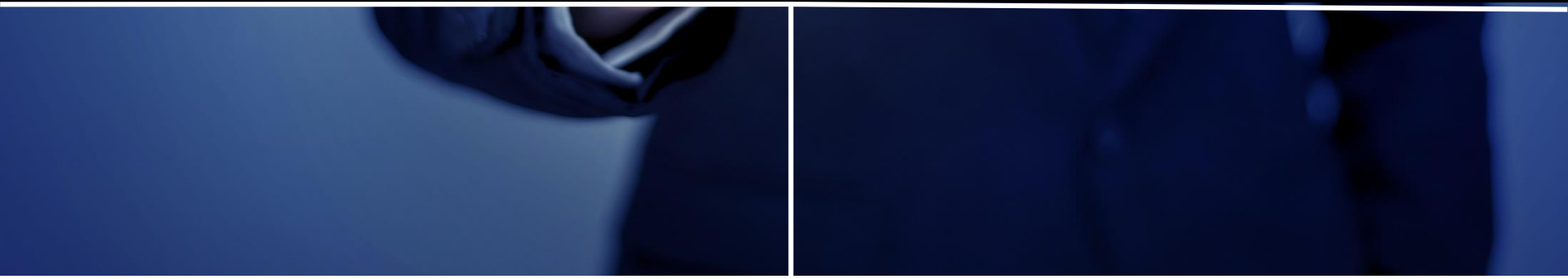
Cybersecurity:
5 Best Practices of Boards of Directors

with Gary Steele and Stuart R. Levine



proofpoint

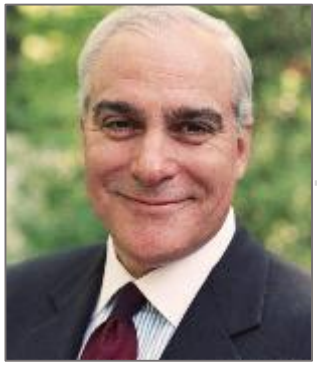
STUART LEVINE & ASSOCIATES

PASSAGEWAYS

Gary Steele

proofpoint

- CEO of Proofpoint, a leading cybersecurity company And founder in 2002
- Before joining Proofpoint, Mr. Steele served as the CEO of Portera and VP and GM of the Middleware and Data Warehousing Product Group at Sybase, Inc
- A leading expert on cybersecurity and has been seen on Good Morning America, Fox News, and CNBC
- He holds a B.S. degree in Computer Science from Washington State University



Stuart R. Levine

STUART LEVINE & ASSOCIATES

- Chairman and CEO of Stuart Levine & Associates LLC a management consulting firm for governance, strategic thinking, and C-Suite leadership
- Board governance expert, currently serving on the board of Broadridge Financial Solutions, as Chairman of Governance and Nominating Committee and member of the Audit Committee
- NACD Governance Fellow and was twice awarded the top 100 director by this organization
- Best-selling author of three leadership books published in 37 countries with over 1.2 million hard copies sold and his monthly thought-leadership articles are published in Forbes and The Credit Union Times

42 million

2015 estimated breaches worldwide

$2.7 million

average cost per breach

proofpoint

STUART LEVINE & ASSOCIATES

PASSAGEWAYS

The Cyberattack Impact on a Corporation: Increased Costs of Doing Business

- Insurance premium impact
- Credit worthiness
- Cultural disruption
- Transactional due-diligence impact
- Negative impact on customers from partner issues
- Your brand gets tarnished
- Your culture gets disrupted

proofpoint. STUART LEVINE & ASSOCIATES PASSAGEWAYS

Questions for the Board to Ask Management about Cybersecurity

- How will we know if we have been hacked?
- Has there been a full review of the inside threats?
- Do we understand IT deficiencies?
- Have we reviewed the NIST framework and evaluated our internal operations against this?

Questions for the Board to Ask Management about Cybersecurity

- Does the company have adequate cyber insurance?
- Does management have a plan and process in place to respond to a cyberattack?
- Are you testing your employee's understanding and preparedness for potential attacks through email and social media? ?

proofpoint

STUART LEVINE & ASSOCIATES

PASSAGEWAYS

NACD Blue Ribbon Commission

- Directors need to understand and approach cybersecurity as an enterprise-wide risk management issues, not just an IT issue.
- Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
- Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

NACD Blue Ribbon Commission

- Directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.

- Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

Cybersecurity: It's a Board Issue
In the Headlines

Target settles with banks for $39 million after epic data breach

TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack

TalkTalk

Disclosure investigations newest narrative in enterprise breach forensics

Enterprises risk becoming part perpetrator based on their reporting on hacks

YAHOO!

proofpoint

STUART LEVINE & ASSOCIATES

PASSAGEWAYS

From IT Security to Cybersecurity

- The board's role in understanding and monitoring cybersecurity risk has been underscored by a new breed of lawsuits holding boards of directors responsible for gaps in security.
- IT Security has evolved from a technical issue to a critical business issue.
- Cybersecurity needs to be a part of the audit committee's business risk framework.

Challenges for Boards

- An “IT silo” mentality exists that has relegated the protection of data and systems to the IT department.
- Boards tend to lack expertise in cybersecurity making it difficult to properly assess cyber risks and the risk management program put in place by management.
- There has been a focus on strengthening defenses through preventative security controls while ignoring incident detection and response capabilities.

Five Best Practices: One
Accept Responsibility

- Boards must ensure that cybersecurity is viewed as an enterprise risk issue, not just an IT topic and that the discussion of cybersecurity issues get adequate time on the board agenda and with management.

- Boards need to understand that a separate committee does not relieve the full board of its core oversight responsibilities.

Five Best Practices: Two
Set Expectations for Management Team

Boards need to set the expectation that an enterprise-wide risk management framework with adequate staffing and budget to oversee cybersecurity risks is a mandatory part of an overall risk management plan.

Five Best Practices: Three
Understand the Entire Scope of Risk

- Assess legal risk
- Consider industry-specific legal concerns such as in healthcare or banking industries
- Prioritize assets and sensitive data
- Consider cyber insurance
- Identify risk from third parties
- Anticipate change

proofpoint. STUART LEVINE & ASSOCIATES PASSAGEWAYS

Five Best Practices: Four
Assess Current Cybersecurity Practices

- Does management understand its responsibility for cybersecurity and have an adequate system of controls in place?
- Is the cybersecurity budget appropriately funded? Is the organization's enterprise risk management program appropriately staffed and resourced given the types of risk assessed?
- Are there clear policies and procedures in place in the event of a breach?
- Is the company's disclosure response in line with SEC guidelines and shareholders expectations?

Five Best Practices: Five **Plan and Rehearse**

- Review the current response plan.
- Conduct a “dry run” of a breach. Analyze what works and what doesn’t, and modify your plan as necessary.
- Create a rapid response team.
- Establish a relationship with law enforcement.

Document security and board meeting solutions

- Dropbox and email to be avoided
- Email bad for communications too
- Printed documents hard to track
- Notes and annotations
- Secure access anytime, anywhere, any device
- Document resource center

Watch 4 Minute Demo Video

OnBoard

proofpoint

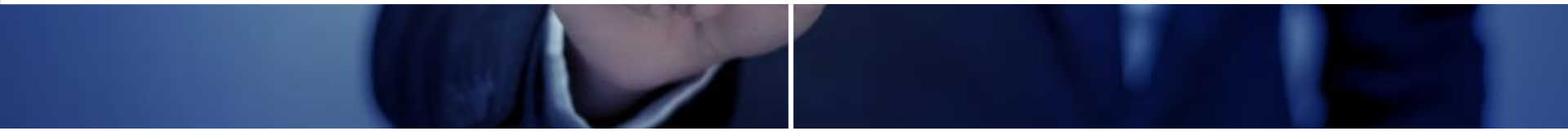
STUART LEVINE & ASSOCIATES

PASSAGEWAYS

Thank You

We are open for live questions!

Upon webinar completion there is a short survey



Gary Steele
CEO
gary@proofpoint.com
proofpoint.com

Stuart R. Levine
Chairman & CEO
slevine@stuartlevine.com
stuartlevine.com

David Alder
VP of Product
dalder@passageways.com
passageways.com

proofpoint

STUART LEVINE & ASSOCIATES

PASSAGEWAYS