Cybersecurity at MIT Sloan

INSIGHTS ON CYBERSECURITY GOVERNANCE AND RISK MANAGEMENT FOR BOARDS OF DIRECTORS

Cybersecurity at MIT Sloan

RESEARCH BACKGROUND

FRAMING QUOTES

"Boards are still not prioritizing cyber like they should be…I think every company needs to live in a proper amount of paranoia about this, and we have turned into an economy that is driven by information – if we don't protect that, it is the equivalent of leaving the door of the store open at 1:30 in the morning and leaving anyone to walk in and take it." (#10 Board Member, Media)

"I think it is important for the board to get more active. It is part of the mission now: you should know this. Every company is a tech company! You can't say 'I don't want to know'. You need to know…Boards are freaked out…I can be found personally liable." (#2 Board Member, Multiple Industries)

"Every board knows that cyber is a threat and cyber is a risk. How they manage it is still the wild west." (#3 Board Member, Healthcare)

PROJECT OVERVIEW

- Boards of directors are **increasingly responsible for providing guidance and oversight on cybersecurity risk**; many boards are **unequipped to do so**.
- This critically important mandate introduces **novel challenges to what is already a complex governance environment**.
- Drawing on **in-depth interviews with board members and executives**, this research describes **four core cybersecurity challenges** that boards encounter and proposes **ten recommended actions** that boards can undertake in response.
- By employing these action items, **boards can optimize their ability to provide meaningful, effective governance** to address cybersecurity risk.

QUALITATIVE METHODOLOGY

DATA COLLECTION

35 total interviews conducted in two phases…

- **Phase 1:** 22 interviews with executives
- **Phase 2:** 13 interviews, a majority had direct board experience (see **INTERVIEWEE DETAILS** table below for more information)

Phase 2 interviews ranged 21–56 minutes.

- Averaged 37 minutes

Inductive coding analysis used to identify emerging concepts and themes.

INTERVIEWEE DETAILS

Interview	Interviewee Title	Industry	Interview Length (mins)
1	CEO	Finance	41:49
2	Board Member	Finance / Education / Tech	34:11
3	Board Member	Healthcare	50:24
4	CISO	Communications	56:57
5	Board Member	Technology	28:05
6	Board Advisory	Technology	47:40
7	Board Member	Food Services	25:21
8	Board Advisory	Multiple Industries	21:48
9	Board Member	Communications	38:25
10	Board Member	Media	27:05
11	Board Member	Finance / Tech / Insurance	35:36
12	Board Member / CEO	Multiple Industries	38:40
13	Board Member	Technology / Finance	45:59

EXAMPLE QUOTES

"Don't show up the CEO. If you have an issue, take it out of the meeting and bring it up. But in my case, we were quite good, but not great, so I brought it up during the board meeting. And I said, 'you put me on the board to be honest, so here is the honest answer'. And everyone took it well." (#11 Board Member, Multiple Industries)

"How much money would you bet that there is not a single person developing that SEC rule that has ever sat in a corporate boardroom or ever run a company? Do you want to take that bet? I have worked in the government. I have said…what everyone ought to do is they ought to spend at least two years at a high enough level in a government agency to see what the hell they do. Anyone that thinks expertise is lodged in the federal bureaucracy, I mean, God bless them, but it is just not true." (#12 Board Member / CEO, Multiple Industries)

RESULTS: CHALLENGES AND ACTIONS

FOUR CORE CYBERSECURITY CHALLENGES FOR BOARDS

CHALLENGE 1. BOARD ATTITUDES AND GOVERNANCE

CHALLENGE 2. BOARD AND EXECUTIVE DYNAMICS

CHALLENGE 3. BOARD EXPERTISE

CHALLENGE 4. CYBERSECURITY REGULATIONS

TEN RECOMMENDED ACTIONS FOR BOARDS

Action 1: Acknowledge that cybersecurity is an enterprise operational risk, and thus a concern for the entire board.	**Action 6:** Determine the board's appetite for bringing in cyber experts, in either a board member, advisory, or consulting role.
Action 2: Scrutinize the organization's cybersecurity maturity.	**Action 7:** Seek out cybersecurity training and education opportunities.
Action 3: Be clear on the possible (personal) consequences of a significant cyber incident.	**Action 8:** Know the cybersecurity and related privacy regulations that affect your industry, organization and countries of operation.
Action 4: Don't get into the weeds on cybersecurity.	**Action 9:** Appreciate that compliance with regulations doesn't (necessarily) equate with sufficient cybersecurity.
Action 5: Demand clarity and understandability in executive communications.	**Action 10:** Understand the tension between what cybersecurity regulations aim to achieve versus the business and legal implications following an incident.

JEFFREY PROUDFOOT, PH.D.
ASSOCIATE PROFESSOR OF IPM, BENTLEY UNIVERSITY
RESEARCH AFFILIATE, CAMS
JGPPHD@MIT.EDU

STUART MADNICK, PH.D.
PROFESSOR OF INFORMATION TECHNOLOGIES, MIT
FOUNDING DIRECTOR, CAMS
SMADNICK@MIT.EDU

MIT