THE ACCOUNTABILITY GAP:
CYBERSECURITY & BUILDING A CULTURE OF RESPONSIBILITY

TANIUM™

Nasdaq

"There are two implications of combining a low level of readiness and a low level of awareness in relation to cybersecurity vulnerability: the first is that you're inviting trouble; secondly, you may already be in trouble and not know it."

Ben Hammersley
Editor at large at *Wired* UK magazine and presenter of *Cybercrimes with Ben Hammersley* on BBC and Netflix

Executive Summary

The Accountability Gap: Cybersecurity & Building a Culture of Responsibility

Business and government leaders grapple daily with innovation's double-edged sword: as new technologies introduce unprecedented levels of efficiency, speed, and capability to the world, a new wave of cybersecurity risks immediately follow, threatening that very technology and the people who use it. In many instances, the technology organizations use to protect themselves has dramatically failed to keep pace with the speed and agility of modern threats, creating billions of dollars of damage from data breaches annually. But this is only half the story.

Less visible is the widespread lack of personal and organizational accountability for the protection of a company's most sensitive data. This accountability gap shows up as dissonance between corporate leaders' current awareness and readiness for cybersecurity challenges and where they need to be.

In "The Accountability Gap: Cybersecurity & Building a Culture of Responsibility," we worked with a global panel of cybersecurity subject-matter experts to define the seven inherent challenges that make up cybersecurity vulnerability: Cyber Literacy, Risk Appetite, Threat Intelligence, Legislation & Regulation, Network Resilience, Response, and Behavior. The research team at Goldsmiths, University of London developed a statistical model for scoring readiness, awareness and vulnerability for these challenges and assessed through a survey of 1,530 non-executive directors (NED), C-level executives, Chief Information Officers (CIO), and Chief Information Security Officers (CISO) across the United States, United Kingdom, Germany, Japan, and Denmark, Norway, Sweden, and Finland (Nordics). The intention of the study was to identify and understand where the gaps exist across all organizational levels around cybersecurity vulnerability from a people, process, and technology perspective.

We identified two vectors that make up cybersecurity vulnerability: knowing about the risk ("awareness") and having the ability to address it ("readiness"). The qualitative phase of this research focused on identifying the main challenges to achieving a high level of awareness and readiness. These served as key inputs into the quantitative study that plotted respondents on a cybersecurity vulnerability scale.

This study's principal conclusion clearly mirrors today's cybersecurity landscape: every organization is vulnerable to a cyberattack. This report uses measures of awareness and readiness to assess three degrees of vulnerability — high, medium and low — each of which indicate differing needs to take action. 90% of respondents have a medium-to-high cybersecurity vulnerability. Low awareness and low readiness make a company highly vulnerable to a breach. High awareness and high readiness mean low vulnerability, but as the research demonstrates, conditions may shift quickly to make a company highly vulnerable.

- 10% of the respondents have a high level of vulnerability and will likely reach crisis if they do not act quickly to address their cybersecurity posture
- 80% of the respondents have a medium level of vulnerability
- 10% of the respondents have a low level of vulnerability, but there are still risks

Our study findings illustrate the daily realities of low awareness and low readiness: 91% of NEDs at the highly vulnerable companies cannot read a cybersecurity report, preventing them from asking the right questions and validating the data that technical leadership provides. On the readiness side, 98% of highly vulnerable companies do not track devices on their network, leaving them unable to secure what they cannot manage. Combined with the 2 out of 5 respondents across NED, C-level, and CIO/CISO-level respondents who admitted they don't feel responsible for the repercussions of a cyberattack, it's easy to see why the Accountability Gap is growing.

Awareness

- 91% of the high vulnerable board members say they can't interpret a cybersecurity report
- Only 10% of the high vulnerable respondents agree that they are regularly updated with information about the types of threats to cybersecurity that are pertinent to their business
- The low vulnerable respondents are 31% more likely than the high vulnerable respondents to have assessed the likely losses associated with cyberattacks

Readiness

- 98% of the high vulnerable executives are not confident their organization tracks all devices and users on their system at all times
- 87% of the high vulnerable board members and executives don't consider their malware, antivirus software, and patches to be 100% up-to-date at all times
- Only 9% of the high vulnerable board members said their systems were regularly updated in response to new cyberthreats

We've defined vulnerability and its parts, but what challenges and failures bring vulnerability to your doorstep? Through a combination of one-on-one interviews and a quantitative survey, the study identified seven key challenges facing boards of directors and executive teams that predict an increased cybersecurity vulnerability. These are areas where people within organizations have the most work to do to move from high vulnerability to low vulnerability. They are as follows:

Awareness

- Cyber Literacy: Not understanding cyber-language and terminology
- Risk Appetite: Not being aware of the implications of a breach
- Threat Intelligence: Not receiving relevant information about threats
- Legislation and Regulation: Not briefing on compliance with government policy

Readiness

- Network Resilience: Not having proper visibility into your network, both devices and users
- Response: Not understanding how to prevent, detect, locate and neutralize cyberthreats
- Behavior: Not fostering a culture of responsibility and security across the organization

Why Accountability?

Corporate governance isn't the typical place people begin when speaking about cybersecurity. That said, with cybersecurity now a threat to the survival of a business, any organization that manages and maintains sensitive data should consider how the board oversees this risk. A lack of awareness and readiness defines the existential threat around cybersecurity. If an organization lacks confidence in its data and the right operational controls are not in place, yet boards don't understand enough to assess and oversee risk, who is actually accountable? An organization cannot leave the responsibility to technical leadership anymore: everyone from the top down should be held accountable for the consequences of cybersecurity vulnerability.

"At the board level, there is ignorance and a sense that 'techies' should take care of that. It is a technical problem, which is of course completely wrong," says Esther Dyson, a Silicon Valley investment visionary. "I have seen it bite people. They need to learn. More and more companies are looking for a cyber expert. Of course, having a cyber expert on your board does not mean much other than you might take it a little more seriously."

Our findings revealed a hesitance in NEDs, who did not consider themselves knowledgeable about cybersecurity, to speak up. To a large extent, cyber is still delegated entirely to those "techies," but board members are beginning to recognize their role in understanding the language and the issues around cybersecurity.

With so many attack vectors unknown, the fate of "business as usual" hangs in the balance. Operationally, recognizing that it is impossible to stop all attacks will allow a shift in focus from planning for failure, to learning from and reacting to failure. Even when an organization has the best technology in the world, if the people who are safeguarding that organization's most trusted information don't know how to be accountable and responsible, the company is still at great risk. "It's knowing which questions to ask, but it's also knowing what evidence looks like. And not even being able to interpret it, because a lot of that would be technical, but being able to demand proof that somebody can stand by their answers," says Kris McConkey, Cybersecurity Partner at PwC UK.

But there is cause for optimism. The report identifies actions all organizations can consider to reduce their vulnerability and close the Accountability Gap. Combined, they suggest that organizations develop all staff's experience – starting at the board of directors – in cybersecurity issues, and educate and innovate continuously with cybersecurity in mind. Open communication and accountability at all levels is key to a successful culture of responsibility, and these actions can serve as a north star for developing a holistic security posture that ensures your people, processes, and technology are set up for success. **Download the full report to read these actions.**

> "At the board level, there is ignorance and a sense that 'techies' should take care of that. It is a technical problem, which is of course completely wrong."
>
> Esther Dyson,
> Silicon Valley investment visionary

Disclaimer The research obtained ethical approval from Goldsmiths, University of London and received informed consent from all research participants in our qualitative exploration.

All quantitative survey participants were anonymized.