THE ACCOUNTABILITY GAP: CYBERSECURITY & BUILDING A CULTURE OF RESPONSIBILITY

TANIUM™

Nasdaq

CONTENTS

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."

> "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

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.

> *"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

Cybersecurity Vulnerability Defined

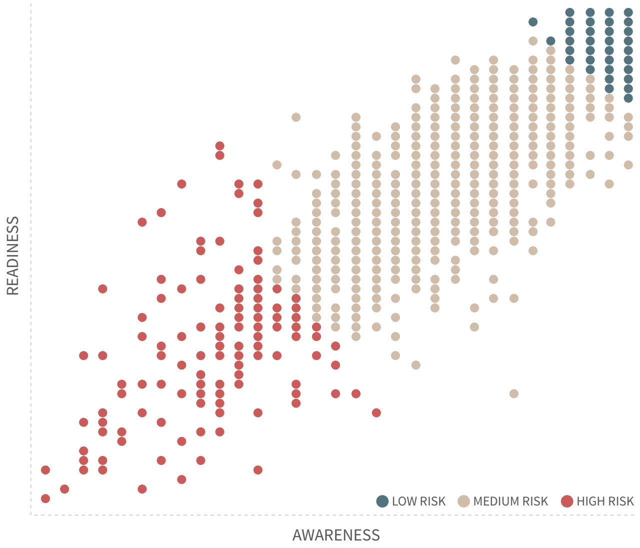
What Makes an Organization Vulnerable

Most board members are not cybersecurity experts. Nor do they have to be. However, if an organization is data-intensive, and the cost of a breach is high in terms of financial, reputational, and/or regulatory impact, they should treat cybersecurity vulnerability as seriously as they would any enterprise risk.

“You should have a cyber risk committee or expand the charter of one of the other standing committees, such as the Audit Committee, to cover cyber risk. If the potential impact of cyber risk is high, and you do not treat it as an enterprise risk, then I would say you are remiss in terms of how you are operating as a board and you have a potential oversight gap.” - Eric Brown, CFO & COO, Tanium

In this paper, we define cybersecurity vulnerability as both a lack of awareness of cybersecurity challenges and a lack of readiness to address those challenges in a way that minimizes business risk and impact. High vulnerability = low awareness (a lack of understanding of the actions required to obtain good cybersecurity posture) and low readiness (a lack of controls that should be in place to ensure good cybersecurity posture). The graph below represents where the study respondents surveyed fall on the vulnerability scale.

CYBERSECURITY VULNERABILITY SCALE



▲ *The red dots represent companies that are highly vulnerable to a cybersecurity breach. Without taking immediate action, these companies could likely be in a crisis situation. The beige dots represent companies that have medium vulnerability to a cybersecurity breach. These companies are doing many things well but still have room to improve, and could fall into a crisis situation if the areas of vulnerability identified are not addressed. The green dots represent companies that have low vulnerability to a cybersecurity breach, yet it’s important to note that every company is vulnerable on some level and even companies that are aware and ready need to remain vigilant to shifts in both external factors and internal risks.*

> “You should have a cyber risk committee or expand the charter of one of the other standing committees, such as the Audit Committee, to cover cyber risk. If the potential impact of cyber risk is high, and you do not treat it as an enterprise risk, then I would say you are remiss in terms of how you are operating as a board and you have a potential oversight gap.”
>
> Eric Brown,
> CFO & COO, Tanium

Our 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 NEDs, 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.

2 out of 5

respondents across NEDs, C-level, and CIO/CISO-level respondents admitted that they didn't feel responsible for the repercussions of a cyberattack.

This combination 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 "the techies" anymore: everyone from the top down must be accountable for cybersecurity vulnerability.

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.

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

Let's explore these concepts in more detail.

Awareness

Challenge 1: Cyber Literacy

Most Fortune 500 companies and global organizations have dedicated IT crisis management teams in place, but there remain important decisions that need to be made by the board. Therefore, it is important to ensure both the C-suite and the board have the right information necessary to their role to make informed decisions.

Unfortunately, when there is a lack of cyber literacy present in the C-suite and the board, the cybersecurity dialogue is often one-sided. The technical executive states a technology risk position, but it rarely leads to substantial debate around the table, resulting in a mechanical board update process versus an opportunity for board leadership. There often exists a sense that cybersecurity is a technical problem that should be handled exclusively by technical teams, but a company's awareness and readiness are negatively affected when a board is unable to articulate its expectations and challenge the executive team to remain within defined risk boundaries. Our research found that 43% of all respondents can't interpret a cybersecurity report at the same level as a financial report. Imagine if a board's Audit Committee couldn't interpret a financial report?

91%

of the most vulnerable board members can't interpret a cybersecurity report.

The cyber literacy problem is two-fold. "It's knowing which questions to ask, but it's also knowing what evidence looks like. It's not even just being able to interpret the information, because a lot of that would be technical, but also being able to demand proof that somebody can stand by their answers," said Kris McConkey, Cybersecurity Partner for PwC UK.

> "It's knowing which questions to ask, but it's also knowing what evidence looks like. It's not even just being able to interpret the information, because a lot of that would be technical, but also being able to demand proof that somebody can stand by their answers."
>
> Kris McConkey,
> Cybersecurity Partner
> PwC UK

▼ This table shows the percentage of respondents who indicated that they are cyber literate. In all countries, NEDs scored the lowest for cyber literacy.

	NEDs	C-Level Executives	CIOs/CISOs
United States	59%	77%	78%
United Kingdom	66%	76%	86%
Germany	61%	69%	74%
Japan	38%	56%	77%
Nordics	50%	55%	55%

Table 1: Cyber literacy by region and role

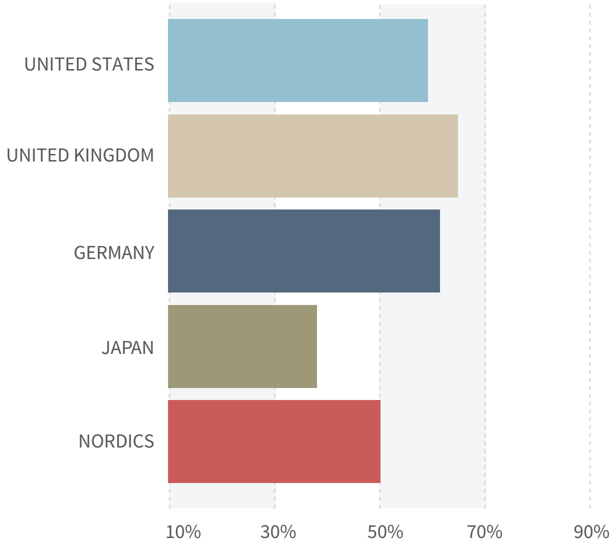
Board members have a fiduciary responsibility to act in the best interest of the company, which in part relies on an understanding of and confidence in the information used as the basis for decision-making. As McConkey suggests, having a baseline understanding is to know what questions to ask and, when a response is provided, to know what evidence looks like to support the conclusion. “I’ve been involved with a lot of board meetings where there are very generic questions asked and the answers really aren’t able to be evaluated,” said David Damato, Chief Security Officer at Tanium. “Answers like: ‘we are very secure’ or ‘we are getting thousands of alerts and responding to them.’ These answers really mean nothing. They have to take it deeper. There is likely some training that needs to go on at the board level, but more importantly a standardization of the types of metrics that are reported to the boards is necessary.”

We outline a few sample metrics to consider adding to board level reports later in this paper.

Only 8% of the highly vulnerable board members reported being updated with information about cybersecurity threats, and only 50% reported receiving cybersecurity training. Most qualitative interviewees suggest that basic training for NEDs – whether tailored on induction or continuous development – should include case studies and real world analogies free of technical jargon to help illustrate the risks to an organization. Technical executives can ease the way to allocate resources for a strong cyber response management plan by providing the board with:

1. An overall understanding of the threat landscape
2. An accurate identification of company assets and associated risk levels
3. A clear explanation of the costs incurred for security relative to risk mitigation for the business

Graph 1: Proportion of all NEDs that understand the language of cyber by region



In the graph above, you'll see Japanese NEDs have the biggest gap in knowledge. The study found the high vulnerable NEDs are 12.5 times less likely than the low vulnerable to understand cyber language.

Challenge 2: Risk Appetite

Only 68% of respondents have assessed the likely losses associated with cyberattacks. Of the most vulnerable, only 13% report to have assessed loss.

Risk appetite is the level of risk that a company or organization is willing to take in the pursuit of its objectives, and can be considered the combination of both the desire to take on risk and the capacity to do so. Risk should not be avoided, since doing so would stifle innovation and hinder value creation; however, risk does need to be managed to an acceptable level. The board of directors has the responsibility for deciding the company's risk appetite, including with regard to cybersecurity risk. In a world where everyone needs to accept that a breach will likely occur, a company's risk appetite assessment needs to be tactical: which investments are you willing to make to detect an issue and how will you remediate a breach quickly?

"In determining risk appetite, the board should define its commercial objectives and understand all of the risks including legal, operational, competitive and reputational that might impact those objectives. Only then can the board express the levels of risk that are desirable. They've then got to continue to understand the likelihood and impact of key risks across the entire company – and monitor that the executive continues to operate within the established risk appetite," said Joan Conley, Senior Vice President and Corporate Secretary, Nasdaq.

Assessing risk appetite is a cornerstone of a good cybersecurity posture: low vulnerability respondents are nine times more likely than high vulnerability respondents to be aware of and understand the implications of a breach. Risk assessments are important to understand the risk exposure against the board's risk appetite. Of the most vulnerable respondents in the United States, only 45% of C-suite executives have gone through risk assessments related to cybersecurity. Across the regions, only Germany comes in with slightly higher numbers at 50% of C-level executive respondents having gone through a cyber risk assessment, with the Nordics and the United Kingdom trailing at 35% and 29%, respectively. While there are indications that the C-suite is taking cyber risk more seriously, the data still shows room for improvement across all regions in taking accountability for this risk.

There are questions that board members can learn to ask and probe to ensure the management team is adequately considering whether cybersecurity is part of the overall business operations and resource allocations. For example:

ONLY

68%

of respondents have assessed the likely losses associated with cyberattacks. Of the most vulnerable, only

13%

report to have assessed loss.

1. What is the company's level of cyber risk and what sources and types of sensitive data inform this assessment?
2. Has the company created a baseline cyber risk assessment, and is there an ongoing process to map improvement over time?
3. Is there a cyber breach response plan or crisis management plan?
4. What information will be shared with the board regarding cyber risk—is there a regular process to review status with the CIO at a board committee level?
5. Should we appoint a lead director within the Audit Committee, formally expand the charter of the Audit Committee to include cyber risk, or is our cyber risk deemed high enough to create a separate, standing Cyber Risk Committee?
6. What is the cost of cyber risk management in comparison to the cost of a data breach—have we looked at breaches in our industry to understand what the all in costs of a breach are?
7. Should the company consider a Cyber Security Insurance Policy or other new classes of security technology to mitigate risk and costs?

> "In determining risk appetite, the board should define its commercial objectives and understand all of the risks including legal, operational, competitive and reputational that might impact those objectives. Only then can the board express the levels of risk that are desirable. They've then got to continue to understand the likelihood and impact of key risks across the entire company – and monitor that the executive continues to operate within the established risk appetite."
>
> Joan Conley, Senior Vice President and Corporate Secretary, Nasdaq

Once risk appetite is determined, executives should then consider taking an inventory of the kinds of threats that could be posed against their organizations. Recognition of your assets and of the threats related to those assets is an enormously important and challenging part of the process, and it never ends. Consider mergers and acquisitions due diligence, for example. One of the greatest unknowns, and risks, when acquiring a company is the cybersecurity vulnerability that comes along with it. "We are constantly auditing any potential acquisition that we make for the security implications," said Guy Allen, Head of IT Change Delivery & Enterprise Architecture, Cath Kidston. The board should have a continuous audit and risk assessment process in place to consider the top risks and monitor the mitigation plans in place, as well as include cyber risk assessment as part of any acquisition due diligence.

Generally speaking, a certain amount of risk is necessary to make profits and achieve commercial objectives, so risk assessments are now frequently including liability and insurance to ensure financial exposures are limited as much as possible. This differs by country, but overall every board and executive team should know the value of their assets and build the appropriate level of insurance around them. Insurance does not, of course, mitigate all risks. Security breaches invariably have a significant impact on the reputation of the company[1] and in turn this is likely to have a significant financial impact, whether through attrition of confidence in the company share price or through customers leaving.

Recent discussions have suggested that damage to reputation can have more impact than the financial damage of the cyberattack itself. While this may be true in an increasingly regulated environment where public disclosure creates negative

[1] https://www.pac-online.com/cyber-attacks-really-do-negatively-affect-company-reputation

public sentiment, the better the response and the faster the ability to deal with it, the less long-term impact there should be on reputation. As such, there is an important interlinking between an incident response plan and a plan to mobilize your response teams. This includes opening up the data for investigation as quickly as possible to response teams in order to isolate and remediate the issue. Efficient breach response plans should deal with accessing the tools required to manage the brand but, more importantly, public facing problems will seem normal and/or manageable when they are dealt with openly and efficiently.

What different businesses in different contexts and geographies perceive as risk will have a huge impact on risk appetite itself. For example, in Japan there are cultural and geographic aspects which impact risk appetite. Japan, being physically isolated by a surrounding ocean, has had a sense of physical security through isolation. This physical isolation, and the resulting sense of security and safety, informed the culture for a long period of time. The concept of cybersecurity presents a huge challenge to a culture where physical security came for almost free of charge.

	NEDs	C-Level Executives	CIOs/CISOs
United States	41%	66%	78%
United Kingdom	45%	67%	79%
Germany	47%	62%	64%
Japan	43%	53%	75%
Nordics	42%	43%	66%

Table 2: Positive awareness of implications of a breach by role and region

While it should be no surprise that the C-level executives and CIOs/CISOs are generally more aware of the implications of a breach than NEDs, the data , as seen above, suggests that more needs to be done to narrow the knowledge gap from the NED community. For example: NEDs across most regions are less aware than C-level executives and CIOs of the implications of a breach (see table above). In these regions less than half of NEDs felt accountable or aware of the implications of a breach. Understanding the implications of a breach should be table stakes for any board member.

Challenge 3: Threat Intelligence

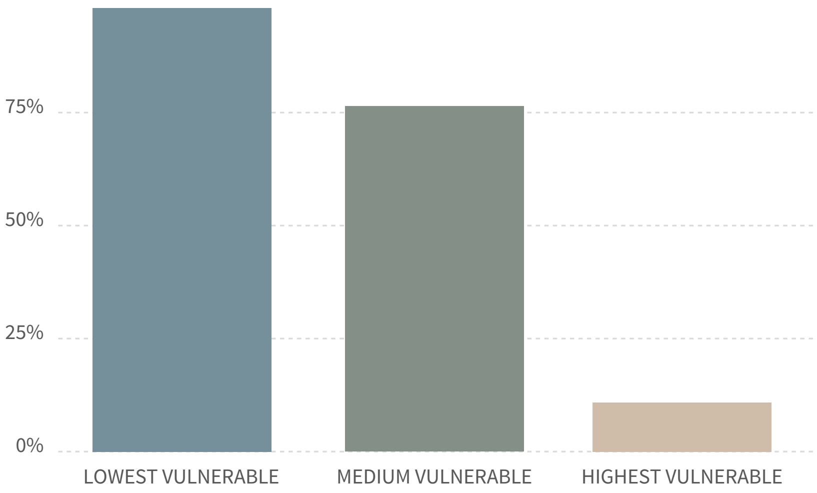
Only 9% of the most vulnerable NEDs said their systems were regularly updated in response to new cyberthreats.

Not receiving regular, relevant threat intelligence may result from a lack of systems in place to disseminate this information and to determine relevance to the business. This challenge must be overcome to ensure there is a genuine flow of threat intelligence through risk governance to the board.

Staying current on the threat landscape should be a specified role(s) in the company, charged with monitoring the most current information: where are the latest threats, what types of threats are they, how are they funded, what are the trends, and whether or not they are pertinent to your organization. This information then needs to be communicated up to executives and NEDs in a digestible manner. "As you keep adding more and more non-traditional devices to your network, from refrigerators to connected cars, it doesn't matter how many cyber special agents there are in the FBI investigating cyber crime," said Andre McGregor, Former FBI special agent and Director of Security at Tanium. "There's always going to be more, either criminals or vectors, that need to be investigated – more so than the number of people that could investigate."

The study revealed only 10% of the highly vulnerable respondents were regularly updated with information about the types of threats to cybersecurity that are pertinent to their business.

Graph 2: Percentage of respondents who receive regular threat intelligence updates



ONLY

9%

of the most vulnerable NEDs said their systems were regularly updated in response to new cyberthreats.

THE STUDY REVEALED ONLY

10%

of the highly vulnerable respondents were regularly updated with information about the types of threat to cybersecurity that are pertinent to their business.

A culture of responsibility often requires a more real-time dashboard reporting approach to keep the board and executives materially up to date. Talking to and collaborating with industry peers and producers of threat intelligence is an increasingly common practice that helps keep companies ahead of the game. For a large organization, there are usually multiple security operation centers around the globe that continually monitor events 24/7. This work is a daily form of vigilance that keeps all systems in sync with the most up-to-date threat intelligence as threats emerge. “There are so many parties out there that are looking to attack your organization for various reasons, whether they are state sponsored or just competitive hacks, that they are changing the game every day,” said T.K. Kerstetter, Chief Executive Officer, Boardroom Resources LLC and Host of Inside America’s Boardrooms. “This is the kind of thing that you must stay on top of, and there must be some kind of regular evaluation to be able to make sure that you are giving yourself the best chance to mitigate a cyber incident.”

> The board has a responsibility to protect the company as a whole, but they should understand that hackers may target them personally as a way into the organization.

Taking stock of the current threat landscape through risk assessment is critical, and it is the starting point to determine whether or not your current arrangements are adequate or if improvements are necessary. Part of creating a threat profile includes:

1. Mapping where your data centers are
2. What controls are in place
3. How networks are segmented

This allows organizations to begin to overlay threat actors’ capabilities against your organization. You can then work out if there are exposing under-protected paths through that network, and use that information to identify gaps. The conclusions of such an assessment are likely to be of interest to the board and/or the risk committee allowing them to monitor where the capabilities sit vis-à-vis their defined risk appetite.

There are two aspects to consider when thinking about an attack itself: what are the ways the attackers succeed and what will they do once they have access? Organizations need to think about these two questions as separate issues. The primary attack vectors aren’t just the devices themselves: they could include the key executives in the company. “If you are a hacker and you want to attack an organization, what you would typically do first is look into the executive level because they’re high profile, and then look to every correlation that exists on the web,” said Louis Modano, Senior Vice President, CISO and Global Head of Infrastructure Services.

The board has a responsibility to protect the company as a whole, but they should understand that hackers may target them personally as a way into the organization. If the board represents a weak entry point to the company itself, then it is important that staff brief them on the threat regularly and ensure the right controls are in place – whether it's process or technology-related – to mitigate or respond to vulnerabilities. It's unlikely to be a matter for the board as a whole, but should be part of each of the director's tailored education programs.

As well as remaining vigilant over up-to-date threats, an organization's response plan should change as a result of the changing threat landscape. Patches, malware and antivirus updates, at a minimum, should be applied continually as new threats emerge. If your response plan provides a role for the board of directors, it is important that they are briefed on relevant changes so they can be put into action as needed.

Challenge 4: Legislation and Regulation

The highly vulnerable are 54% less likely than the least vulnerable to be aware of forthcoming regulatory changes on cybersecurity and how to comply with them.

THE HIGHLY VULNERABLE ARE

54%

less likely than the least vulnerable to be aware of forthcoming regulatory changes on cybersecurity and how to comply with them.

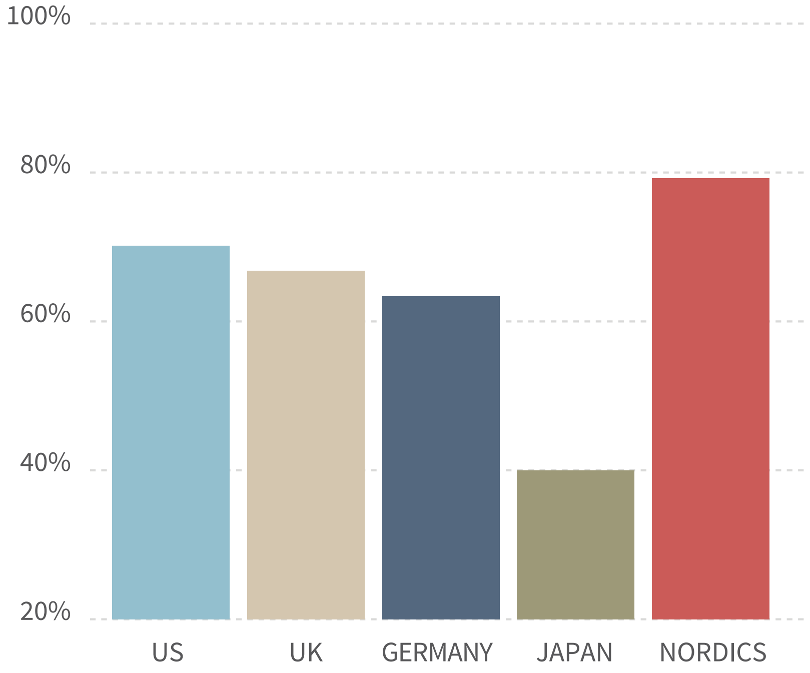
Regional government policy is one area where board members should reach out to other companies and government agencies to understand their responsibilities and how different companies deal with these measures. The U.S. breach disclosure policy and the new EU legal provisions[2] on breach disclosure will impact the management of a firm's reputation; therefore, board members first need to know what constitutes a major breach in order to understand its far reaching implications.

"Part of vigilance means how well we engage with government agencies. For two reasons: one, there are expectations as they give out new regulatory requirements; and two, we rely on them to assist us when and if there are threats that are occurring in the financial industry," said Louis Modano Senior Vice President, Chief Information Security Officer and Global Head of Infrastructure Services, Nasdaq.

- 67% of NEDs are regularly briefed on legislation and regulation
- Highly vulnerable Nordics are 47% less likely than the low vulnerable to provide relevant data to the authorities within 24 hours of a breach
- Overall, NEDs in Japan scored the lowest with only 40% of all NEDs receiving regular briefings. Nordics NEDs reported the highest number with 79% being briefed on legislation and regulation.

[2] http://europa.eu/rapid/press-release_IP-15-6270_en.htm
& https://ec.europa.eu/digital-single-market/en/news/network-and-information-security-nis-directive

Graph 3: Percentage of NEDs who are regularly briefed on government policy



Challenge 5: Network Resilience

98% of the most vulnerable executives are not confident their organization tracks all devices and users on the system at all times.

This is a staggering data point and illustrates one of the primary security risks to an organization. Without proper visibility into the devices and users running on or accessing the network, there is no way to track and manage IT assets to ensure they are configured properly and have the right patch levels and software versions. Without this ongoing visibility, the network is left vulnerable to attack. For this reason, security has become a critical pillar of network resilience, which is defined as the ability to maintain an acceptable level of service in the face of faults and challenges to normal operations.

98%

of the most vulnerable executives are not confident their organization tracks all devices and users on the system at all times.

In a cybersecurity context, challenges to normal operations can range from simple configuration errors to targeted attacks that could create a network or business service outage, or restrict employee access to data and systems. With the rise of connected devices and an ‘anywhere, anytime, on any device’ approach, the most frequent attack vector into the corporate network has become the endpoint. An endpoint could be a laptop, desktop, virtual machine, server mobile device, or even Point-of-Sale systems or ATMs. In the Internet of Things world, it’s anything with a chip. CIOs and CISOs need to have confidence in their visibility into the devices and users on the network at all times, and the ability to collect this data in a timely and continuous manner should be viewed by executives and the board as a key cybersecurity vulnerability risk indicator. The variance between high vulnerability and low vulnerability respondents underscores this point further: the most vulnerable respondents are 17 times less likely than the least vulnerable to track all devices and users in their system.

The first step in increasing network resilience is continuous visibility by incorporating technology which enables IT and security teams to accurately track the devices, the software running on them, and the applications they are using to transmit data both within and off the corporate network. This should be an automated approach which enables the operational teams to collect this data quickly. Given the pace of rapidly evolving cyberattacks, this now means having the ability to collect this data in seconds. The next step is setting a baseline for compliance, including standard configuration settings, patch levels, and approved software and versions. Once you have a baseline established, automation is a scalable way to not only monitor and identify deviations from the baseline, but also remediate or bring devices back into compliance. This is both a reactive and proactive process to address threats as they arise - for example, deploying a patch against a known system vulnerability - as well as part of good ongoing cyber hygiene.

Good cyber hygiene includes ensuring all software, versions, patches and security updates are in place on devices and that configuration errors are flagged and fixed quickly. This is another key risk area that separates the highly vulnerable from the rest. 87% of most vulnerable board members and executives don’t consider their malware, antivirus software and patches to be 100% up-to-date at all times. Compare that to the entire study - 38% of all respondents don’t consider their malware, antivirus software and patches to be 100% up-to-date at all times.

Network resilience also includes having a defined IT change management process in place to minimize the risk of service disruptions and system downtime related to system issues. Given the interdependencies of the IT infrastructure on business services, changing one element may create an unintended ripple effect on another business service. While standard changes usually can wait to go through the standard change process, security attacks may require emergency remediation measures such as deploying critical system updates and patches. Organizations should have an emergency security-focused change management process that spans across both security and IT teams.

87%

of most vulnerable board members and executives don’t consider their malware, antivirus software and patches to be 100% up-to-date at all times.

Challenge 6: Response

Only 10% of the most vulnerable respondents are aware of the steps needed to take appropriate actions to prevent, detect, locate and neutralize cyberthreats. Compare this to the most vulnerable NED respondents and it drops to 8%, likely due to cyber literacy issues previously discussed. With CIO respondents it drops even further to 2%, which is an alarming statistic given the technical functions within an organization should have the most expertise in this area.

Preventing 100% of attacks is virtually impossible with a threat landscape that is constantly changing, a perimeter that has been blurred and a myriad of prevention-based legacy security tools which only capture a small fraction of modern attacks. Therefore, a shift from a prevention-based strategy to one of rapid detection and response is occurring in the market, including technology to detect, contain and remediate issues, and actionable cyber incident response plans. Adequate response plans should be holistic across both people and technology. It is not sufficient to only have the right tools in place to alert and identify problems, but it is also important to have the skill set to be able to leverage the technology to more effectively deal with cyber issues. Ryan Kazanciyan, Chief Security Architect at Tanium agrees, stating, “When you equip smart people with technology that lets them apply their know-how, their concepts, and their skills across an environment, you really allow them to be more successful and effective at their goal. That’s what good technologies should do.”

ONLY
10%
of the most vulnerable respondents are aware of the steps needed to take appropriate actions to prevent, detect, locate and neutralize cyberthreats.

Simulations are another good exercise to help everyone in the company, including NEDs, understand where the response plan is likely to fall down and what needs to be improved. Throwing the environment into crisis mode can uncover the realities of the situation for board members and executives. The top leadership has to understand the risk to the business and through this lens will understand the budget that needs to be applied. As Marco Gercke, international expert in the field of law related to cybercrime, cybersecurity and director of the Cybercrime Research, suggests, “I’ve seen members of the board that had challenges making the right decisions in those simulations - but with the experiences from those simulations they have way more routine in real crisis situations. This is part of the deal. If you want people to deal with crisis, you need to put them in crisis.”

> “When you equip smart people with technology that lets them apply their know-how, their concepts, and their skills across an environment, you really allow them to be more successful and effective at their goal. That’s what good technologies should do.”
>
> Ryan Kazanciyan,
> Chief Security Architect,
> Tanium

As people become more tech-savvy and the scenarios develop, simulations must also become more reality-based. Louis Modano describes red teaming as “an effort where you either hire a third party or you have someone on the inside look for ways to access your environment the way a hacker would - looking for gaps and vulnerabilities and behaving like a hacker, then taking the learnings from that simulation and using them to remediate the issue.” Simulations are perhaps the best way to evidence a company’s vulnerabilities in a way that will resonate with boards. Nasdaq's Joan Conley suggests “the board has enterprise risk as a key priority and will likely say that running a simulation either at a local level or a global level may be large and costly, but it is so important to provide comfort that the systems and controls are fit for purpose. It’s much better you test your system than somebody else.”

Simulations should be followed by a post-mortem to reset the baseline, as well as develop a feedback loop to learn from failure. While the details of a cyber incident response plan sit with the operational side of security or the CIO/CISO directly, the CEO and board approves the budget for the response plan, including software and baseline audits. The financial and strategic risks associated with a cyber breach exponentially increase the longer it takes to access the data required to isolate the issue and treat the problem. Such risks need to be clearly identified and defined for the CEO and board members. Alongside in-house simulations, systems, controls, and policies must be constantly updated and stress tested, forming a loop of continuous improvement. Support from third parties can be invaluable, and also provides a level of independence and challenge that might be missing from in-house testing. Independent testing is often helpful in the board discussion, ensuring the board remains confident in the current control environment.

NEDs are at arm's length from daily company operations, and it's quite reasonable to expect them to have less detailed knowledge of how to respond to cyberthreats. However, it is necessary to ensure they are properly educated so they are equipped to make informed judgments as to the adequacy of controls, and to challenge them. It is also important that the board understands its particular role, if any, during an incident. Continuous education is necessary, as are simulations involving the board as necessary for the scenario. The way to recognize cybersecurity vulnerability is to learn from experience and to become progressively stronger over time, ensuring enterprise resilience. It's better to simulate the failure before it happens so you're a little more prepared to respond.

Challenge 7: Behavior

Only 17% of the most vulnerable respondents understand the risks to company's systems that can come from employees. This is compared to least vulnerable where 100% understand the risks.

All employees in a company should understand cybersecurity risks and how to be responsible and aware to mitigate the risk of opening the gateway for threats, both external and internal. Traditionally, employees have understood cybersecurity as belonging to an individual or group. Shifting that perception to acknowledge cybersecurity is everyone's responsibility within an organization, no matter where they sit, is the first step toward behavior change.

Executives and NEDs, in addition to providing leadership and ensuring there is a culture of responsibility, should ensure appropriate budgets and resources are allocated to cybersecurity awareness training for all employees. This gives the CISO and security team the best possible chance to ensure that individuals are behaving responsibly and contributing to tackling cybersecurity risks consistently with the company risk appetite.

A further aspect of behavior management is the need to balance the relationship between the security team and the IT team, in terms of resources, training, technology accountability, and a shared sense of responsibility. These teams - while often separate organizationally and with separate agendas - need to work together to achieve the company's objective of prudent risk management. There is still a fallacy that technology that will solve every issue. In reality, most of the security issues are caused by some kind of human error or by a basic hygiene issue that could have easily been identified and corrected with the proper tools, shared visibility and joint collaboration across these teams.

ONLY
17%
of the most vulnerable respondents are aware of the steps needed to take appropriate actions to prevent, detect, locate and neutralize cyberthreats.

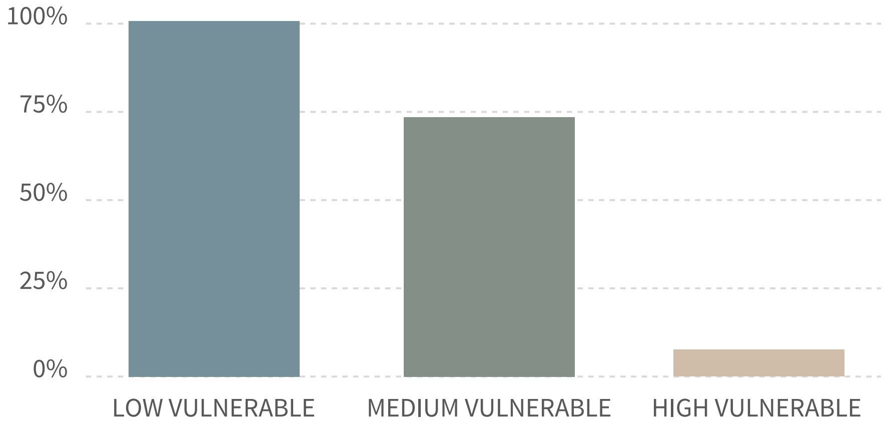
The imperative should be to ensure that individuals are aware of and ready for the potential threats to the entire company and recognize that anyone's actions can provide a gateway for a threat. To achieve this, a credible tone from the top is important, as is the cascading of that culture throughout the management layers, augmented by employee training.

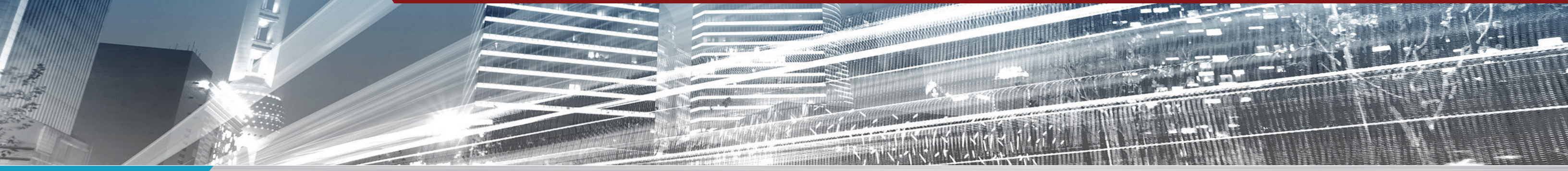
Consider doing a baseline audit of your employees' activities and risk. Getting a baseline audit is not just about understanding risk to your IT assets - it's also about understanding your workforce, your products and your daily routines to know where risky behavior might lie. Create an employee risk profile and wrap security around it. There is a psychological argument that creating a risk profile is a healthy thing to do because then people don't feel like they are being policed and they don't feel like they are being restricted. They feel like the organization is treating them like an adult. Then you can also use that to drive awareness. You might see that certain people on certain teams, for example, have riskier behavior around social media, or are more likely to play games that induce risk. Then you can target awareness raising messages around those particular issues.

Personalizing security is considered an important step in ensuring everyone in the organization is involved in a part of its cybersecurity; that is in creating a culture of security. Much has been written about the success of 'gamifying' as a means to involve people. Andre McGregor explains this concept: "Telling somebody how their sleep schedule operates helps them to know their limitations and to know their strengths. Similarly, you can tell someone their risk score in a way that they understand that they need to better in certain places or they are excelling and can support other employees that are lacking. You can also share trends and motivate people to get a higher score."

Organizations need to lead the charge understanding where the largest sources of vulnerability exist internally and empower employees - technical and non-technical alike - to build security into their daily work. This is a practice employed by organizations that are at the lowest vulnerability. The least vulnerable respondents are 8 times more likely than the most vulnerable to have identified the sources of their highest vulnerabilities and empowered employees on security. The CIO and the CISO are logical organizations to spearhead this effort internally.

Graph 4: Creating a culture of security among the different vulnerability groups





Cybersecurity Vulnerability: What Can We Do About It?

This section provides actionable recommendations that can be used to create a meaningful two- way dialogue aimed at reducing cybersecurity vulnerability and ultimately building a culture of responsibility fueled by vigilance, openness and innovation.

1. Create a Culture of Vigilance: Acknowledge that cybersecurity is a fundamental threat to the business

It’s very easy for a company in the low vulnerability category today to quickly become a high vulnerable company tomorrow. People, processes, and technology together are the cornerstones of a culture of vigilance. “They need to work together. A lot of companies have the tools in place to be able to alert and identify that they have an issue, but then they don’t have the skill set in-house in order to deal with it,” says Tanium's Andre McGregor. Awareness and readiness are moving targets: know what you don’t know and never stop re-evaluating your people and skills, processes and technology: good threat intelligence, response plans and future planning make up the best possible defense.

2. Create a Culture of Openness: Increase cyber literacy and knowledge, starting at the top

It is important to foster an environment of transparent communication in which cybersecurity can be talked about openly. Use case studies and training to improve the levels of understanding at the leadership and board level, and if necessary bring in expertise to help address the gaps in knowledge. Work collaboratively with governments, non-government organizations, and peers to understand the latest security threats and ways to work together to put out fires. The research shows that we need to move to a culture of openness: one where we strive for transparency and maximum visibility. Admit that hacking is inevitable, but breaches are not. Strong response plans, employee training targeted to each level in the company, cultivating knowledge and sharing information are crucial elements for strengthening cybersecurity. Specifically, companies should be focused on improving information flow across the organization (including the board). Nasdaq's Louis Modano supports this approach, “It is about really understanding, from an industry standpoint, what is going on. So it means being active with the different industry consortiums as they are all fighting the same fight.”

Boards need to know what questions to ask in order to understand the state of cybersecurity of the business. These can be supplemented by detailed in-house or externally facilitated briefings for directors to ensure they have the skills to provide adequate oversight. Board members need to learn how to ask questions the same way they do for financial concerns and, in some cases, certain board members responsible for cyber should be given extended training. Fundamentally, you need to help create a common language that all executives can understand. Assessing competence of board members to ‘read’ a cyber report and to discuss its contents could be a feature of annual board evaluations to identify proactively where effort should be targeted to continuously improve skills.

Kris McConkey adds, “The language barrier is something that needs to be closed from both sides….At the same time, there needs to be cross-skilled non executives to ask questions exactly same way that they would of financial concerns.”

- Regularly educate staff on cyber hygiene practices and their personal responsibility to information security
- Regularly conduct cyber wargaming exercises and extend the results to the business
- Conduct a business impact assessment (BIA) and ensure non-technical leadership understands cybersecurity's impact on the business
- Evaluate and update protocols to communicate with staff quickly when an issue arises
- Conduct annual board evaluations to proactively identify where effort should be targeted to continuously improve cyber skills. For example, assess board members' ability to 'read' a cyber report and to discuss its contents
- Create a standard set of metrics and a scorecard for easy month-over-month and year-over-year benchmarking (See sample metrics in No. 3)
- Conduct an annual "Cyber 101" board education session led by information security leaders and/or a third party, and follow up with a glossary of terminology in lay-terms
- Consider expanding your board's Audit Committee to encompass both Audit and Risk, as well as adding a cyber risk member to the committee who has deep background and knowledge of cybersecurity and how it relates to and impacts the organization
- Develop a three year security plan, which allows the board to understand and track progress of planned improvements to mitigate identified risks
- Provide to the board an overview of:
    - Top organizational risks and controls/plans to limit such risks
    - Alignment with industry frameworks and/or defined security strategy
    - Cyber insurance coverage and policies

3. Create a Culture of Innovation: Right team? Right technology?

PwC's McConkey adds: "One of the failings of the security industry or rather the industry as a whole, is that we're effectively taking all the same business processes that we've been using for the last 20-30 years, and trying to add more and more layers of technology on top to patch all the holes."

If widespread education about the detrimental impact of cybersecurity is step one, then an honest, holistic look at the technology you use to keep safe and run the business is step two. The reality is that most modern security tools are just abstracted versions of themselves from the past two decades. Are they able to answer basic questions like, "How many devices are on my network?" or "which machines are running vulnerable applications?" Simple logic states that you cannot secure something that you don't know exists. To create a culture of innovation, start simple and scale fast.

- Complete a proper risk assessment and communicate most critical risks to the board, including:
    - Mean time to detect (i.e. how long did it take to detect a security issue)
    - Mean time to respond/remediate (i.e. how long did it take to resolve an issue)
    - Mean time to patch critical security vulnerabilities (i.e. how long does it typically take for the organization to successfully patch a vulnerability)

- Comparison of penetration testing / red teaming activities year-over-year (i.e. are third party assessments less effective at hacking company resources over time)
- Amount of downtime associated with security related events or activity (i.e. how impactful is security to the business)

- Complete an information security tools assessment, making sure you have the right technology, considering:
  - Data: What kind of data does each tool provide, latency of data, and how the data is used?
  - Coverage: What type of issue does each tool help prevent or how does it help to respond?
  - Redundancy: Do your tools have overlapping functionality? How does each tool fit into your current security process and workflow?
  - Scale: Does each tool perform the functions expected of it vs. your organization's requirements? Does it provide visibility and control over every critical IT asset on your network within seconds to minutes?
  - Reliability: Does each tool perform the functions expected of it for your organization’s particular needs?
  - Cost: How much does the tool cost to operate and maintain? What level of training and specialized skills are required? Does it deliver a clear ROI?

Appendix A: Research Methodology

The research identified five research aims in relation to cybersecurity:

R1 What makes up vulnerability?

R2 What makes you vulnerable?

R3 What are the differences in vulnerability between role and region?

R4 What are the benchmarks of cybersecurity vulnerability?

R5 What can you do about it? (actionable recommendations)

We adopted a mixed methods iterative approach combining qualitative engagement with quantitative analysis to meet the research aims. Each activity informed the others from bottom up in Figure 1. The desk research developed our understanding of the cyber global landscape, framing more specifically the question what is cybersecurity vulnerability? We then interviewed subject matter experts on cybersecurity and cybersecurity in business. This informed the basis for fleshing out the awareness and readiness of cybersecurity; we identified a series of 'challenges' that indicate with cybersecurity issues. These challenges were further refined through interviews with non-executives and executives of Global 2000 companies across the five regions.

Collectively, these interviews, along with qualitative exploration informed the development of a scale for measuring vulnerability. We tested the scale through a survey that gives us objective metrics into relative levels of 'Awareness' and 'Readiness' by different individuals, and in different regions.

RESEARCH METHODOLOGY

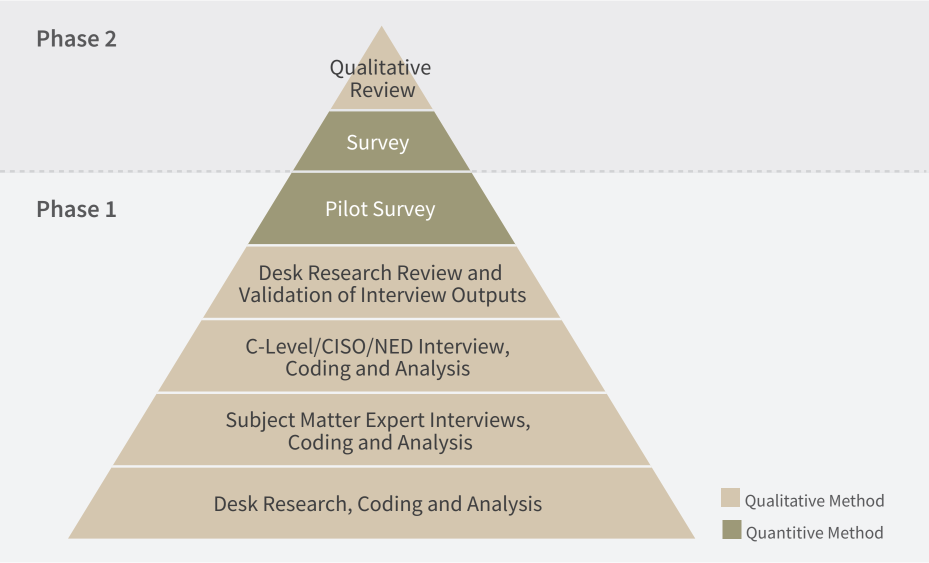

Phase 2
Qualitative Review
Survey
Phase 1
Pilot Survey
Desk Research Review and Validation of Interview Outputs
C-Level/CISO/NED Interview, Coding and Analysis
Subject Matter Expert Interviews, Coding and Analysis
Desk Research, Coding and Analysis
Qualitative Method
Quantitive Method

Figure 1: Research methodology and methods of analysis

The study began with a qualitative exploration on the theme of cybersecurity broadly, and more specifically in business informed by our central research question - what are the factors affecting the cybersecurity vulnerability?

In Phase 1 we undertook qualitative research: desk research to understand the background and current state of the cybersecurity discussion and then interviews with ten subject matter experts who are leaders in the field of cybersecurity.

Using a grounded coding analysis we identified 15 key factors that constituted cyber awareness and cyber readiness. We validated these factors through a further 10 expert interviews with C-levels, CISOs and Non-Executive Directors (NEDs) across the five different regions identified. The validation interviews were coded and analyzed for strength of each of the challenges.

The result of this process led to the development of a scale for measuring vulnerability. A pilot survey tested the results of the qualitative research. Phase 1 concluded that there are seven key factors —framed as 'challenges' to awareness of cybersecurity issues and readiness to deal with cybersecurity issues thus creating our scale for measuring vulnerability.

The Phase 2 large scale quantitative questionnaire surveyed a total of 1530 respondents across the five geographical regions identified and the three roles. All respondents have more than 500 employees. The survey allowed us to 'map' similarities and differences in 'Awareness' and 'Readiness" in executive and non-executive levels, as well as in the different regions.

Appendix B: How We Measured Vulnerability

A 16-question survey was constructed comprising two questions for each of the seven challenges identified by the qualitative research; one assessing Awareness and one assessing Readiness. The specific questions were arrived at by discussion between the qualitative and quantitative teams, narrowed down with the help of a small pilot survey, and then refined further by the team. Each of those questions was on a 7 point scale with each point named (from 1= Strongly Disagree to 7= Strongly Agree.) For some of the analysis, these questions were simplified into Yes/No answers, by considering responses 5-7 (tend to agree, agree and strongly agree) as Yes, and responses 1-4 (strongly disagree, disagree, tend to disagree, neither agree nor disagree) as No. In addition, the questionnaire asked 12 yes/no questions.

1530 responses were received and analyzed, from five countries/regions and three roles. All participants were required to answer all questions.

Initial examination of the responses showed that three of the Awareness questions were unsatisfactory statistically. (The three related problems were that they did not make a satisfactory contribution to reliability as measured by Cronbach's alpha; they did not correlate in the expected direction with the other answers; and in at least one case, there was evidence that it meant different things to different respondents.) With these three questions removed, the Awareness and Readiness questions showed satisfactory reliability (as measured by Cronbach's alpha).

Awareness and Readiness were calculated from the average of the relevant questions. Vulnerability was calculated from the mean of Awareness and Readiness, then reversed in direction so that higher scores represented higher Vulnerability. We also created categories of Vulnerability, by defining the 10% of highest scores as High Vulnerability, the 10% of lowest scores as Low Vulnerability, and the remaining 80% as "Mid".

We found that Awareness and Readiness were very strongly correlated, as shown on the scatterplot in the report. We investigated how Awareness, Readiness and Vulnerability varied between different countries and roles resulting in high, medium and low vulnerability.

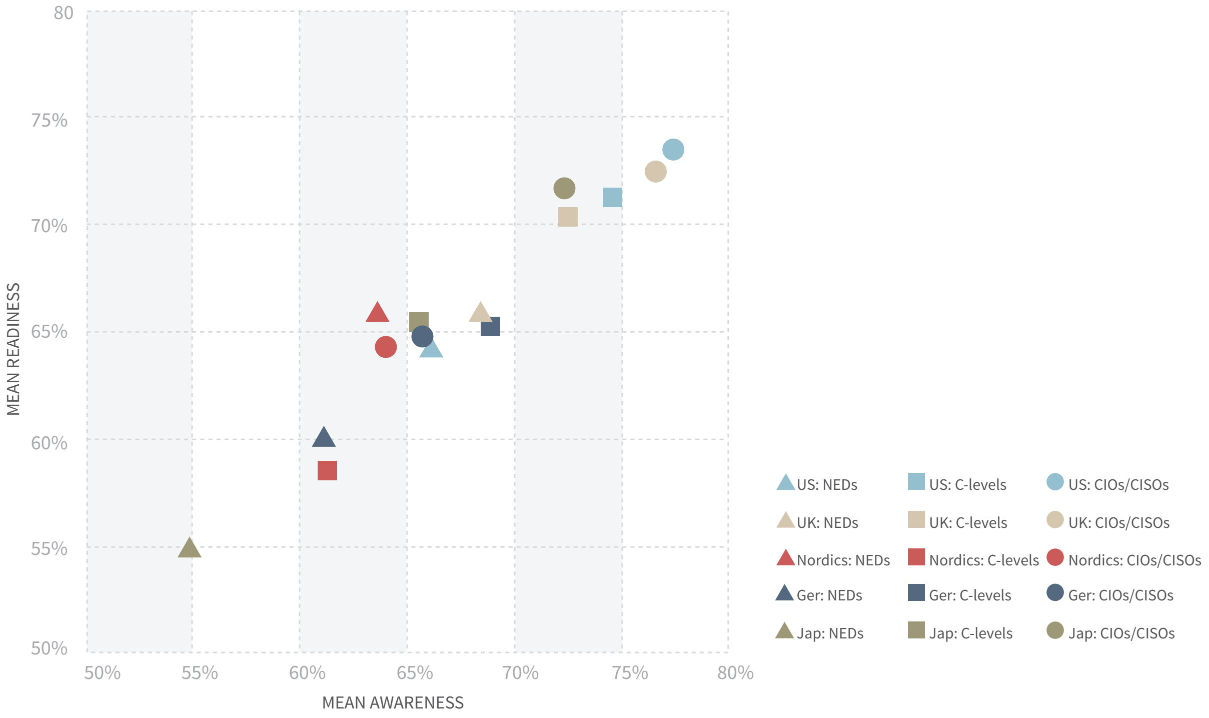
We also investigated how the answers to the Yes/No questions (and the survey questions converted to Yes/No answers) differed, depending on Vulnerability (categorized as High/Mid/Low), job role and country.

Appendix C: Awareness and Readiness Across Levels and Regions

Understanding regional differences

There are regional cultural differenced in understanding what ’awareness’ and ‘readiness’ are and companies must consider the cultural nuances in the cyber landscape, cyberthreats and cybersecurity. Our survey evidences regional differences in respondent’s vulnerability scores, which is discussed in detail in chapter 3. Overall Germany, Japan and Nordics have the highest percentage of vulnerable respondents with NEDs being the most vulnerable overall across all regions. It will be interesting to see how this landscape changes once the European legislation on cybersecurity, approved on December 8, 2015 by the Network and Information Security (NIS) directive, comes into effect. It is predicted that this directive will improve cybersecurity capabilities in member states. Our research showed a significant difference in vulnerability scores between Germany and the UK. Further research has the potential to show whether such regulations have a significant impact in cyber vulnerabilities in business.

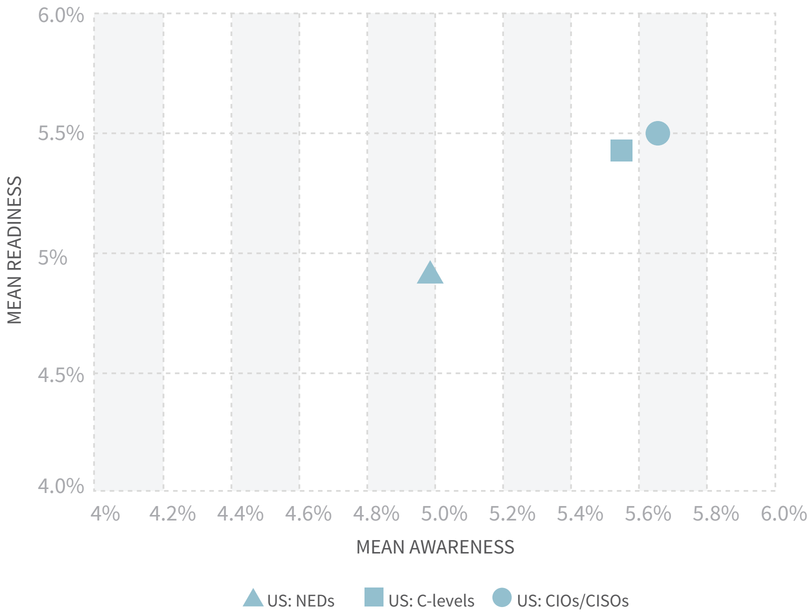
Graph 5: Distribution of vulnerability by region



Graph 5 above indicates the average readiness and awareness by region and role. Remember that high awareness and high readiness leads to low vulnerability while low awareness and low readiness results in high vulnerability. The medium category indicates that a company can have relatively high awareness and low readiness or some factors in place to be ready but not really aware of the extent of the issue.

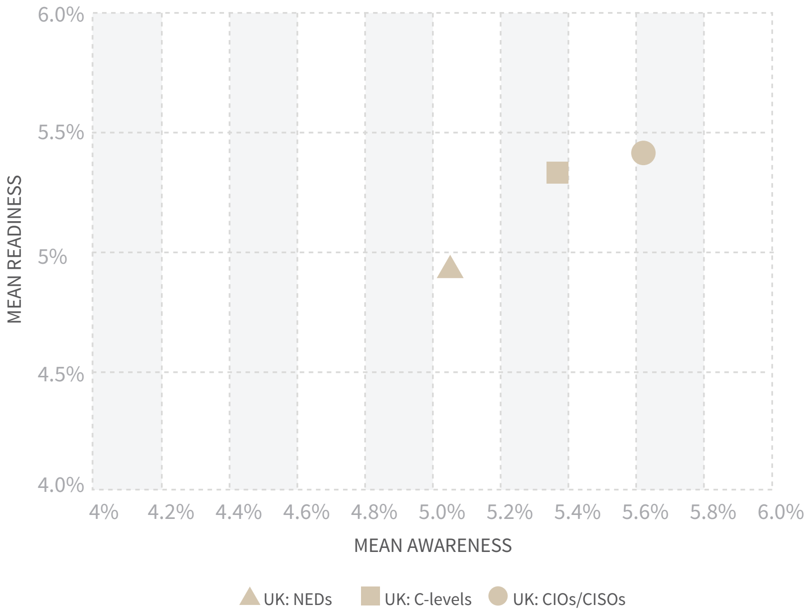
Japanese NEDs, Nordic C-Levels and German NEDs show high vulnerability and, not surprisingly, US and UK Operational security officers show low vulnerability. The other NEDs are all situated in the medium vulnerability area.

Graph 6 indicates the average position in the US



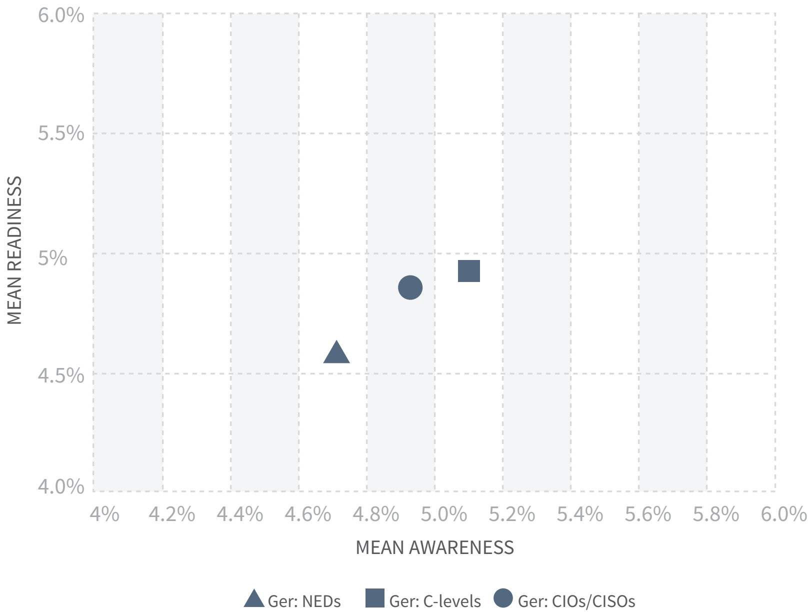
In the US, CIO/CISO and executives show an average low vulnerability. NEDs have medium vulnerability.

Graph 7 indicates the average position in the UK

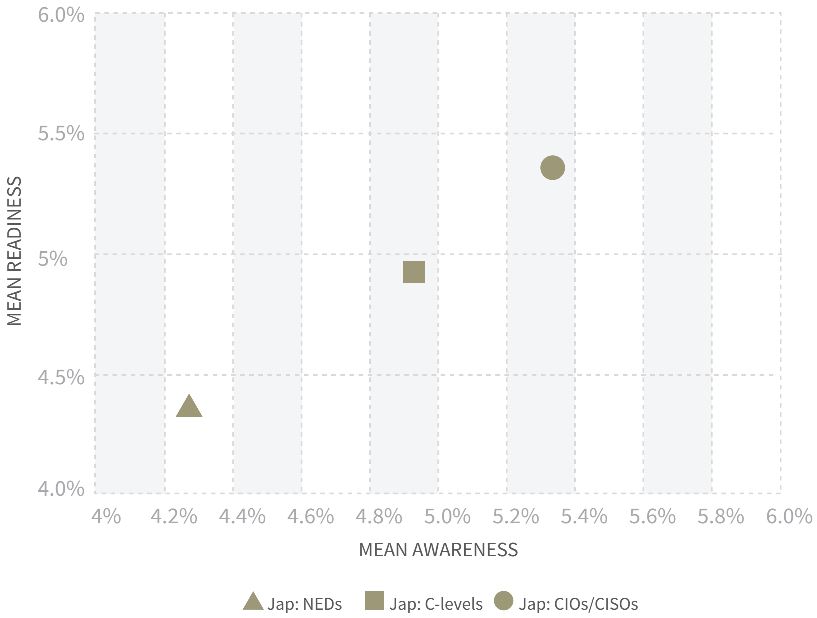


The UK shows a very similar profile to the US, where executives show low vulnerability while NEDs have medium vulnerability.

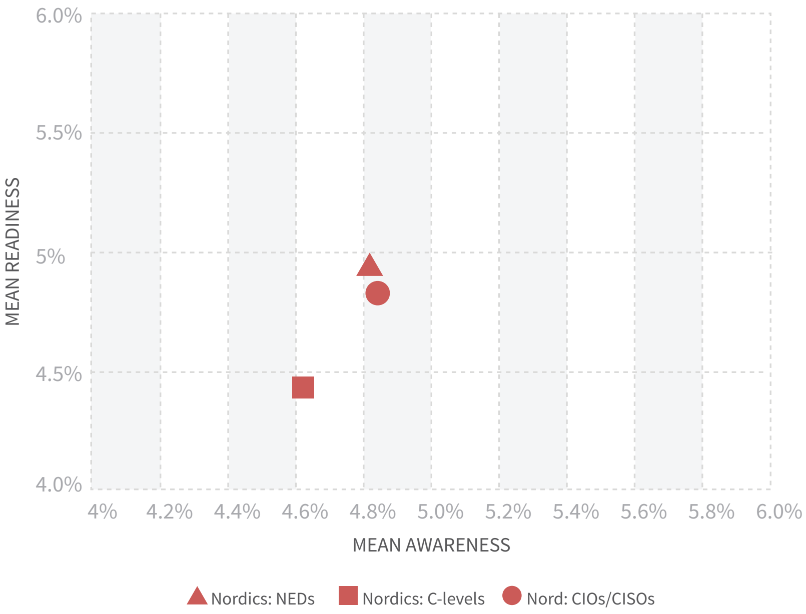
Graph 8 indicates the average position in Germany



Graph 9 indicates the average position in Japan



Graph 10 indicates the average position in the Nordic region.



A note on regional policies

United States

President Obama has identified cybersecurity as one of the most serious economic and national security challenges. Nationally the main strategies are to defend Department of Defense networks, systems and information, defend US national interests, and provide cyber support to the military. The most recent strategy, released in April 2015, outlined the main threats to cybersecurity will come from persistent low level attacks that could damage individuals of firms, as well as targeting industrial systems, and intellectual property.

The data suggested that the US was the least vulnerable of all the geographic regions; however, the complex US regulatory context is a challenge when tasked with understanding and mitigating vulnerabilities across the country. The US has about 20 sector specific national privacy or data security laws, and hundreds of such laws among its 50 states. California alone has more than 25 state privacy and data security laws.[3] In addition, a large range of companies are regulated by the Federal Trade Commission (FTC).

European Union

On December 8, 2015, the European Commission passed a new legislation known as the Directive on Network and Information Security. This was the first EU-wide cybersecurity legislation, and applies to companies which qualify as

[3] https://oag.ca.gov/privacy

‘operators of essential services’ – that is businesses with an important role for society and the economy. Companies will be required to take appropriate measures to resist cyberattacks, and they will have to report serious incidents — such as online booking systems or cloud service providers being unable to grant users access to their content — to the relevant national authority.

Member States will need to ensure that the provisions of the Directive are in place in their national legislation. The Directive intends to improve cybersecurity by providing a standard set of rules, and also by improving co-operation between Member States, encouraging them to exchange information and best practices. For this, a network of Computer Security Incident Response Teams will be set up, whose function will be to promote effective cooperation on specific cybersecurity incidents, and sharing information about risks.

Appendix D: Acknowledgements

The research was directed by Dr. Chris Brauer at the Institute of Management Studies, Goldsmiths, University of London and led by Dr. Jennifer Barth and Dr. Yael Gerson. Research assistance was provided by Alison Wilson, Ana Beatriz Alencar and Zainab Hammoud and graphics by Meng-Yao Chuang.

The project team from Nasdaq included Melissa MacEwan, Jeremy Skule, Blake Stephenson & Ryan Wells. The project team from Tanium included Jennifer Johnson, Tony Larks, Scott Rubin, Matthew Mullin & Kristin Sauchak.

We would like to thank the many subject matter experts that participated in the research for their time and commitment to the topic. Contributors included:

Tanium

- Eric Brown, Chief Financial Officer (CFO) and Chief Operating Officer (COO)
- David Damato, Chief Security Office
- Ryan Kazanciyan, Chief Security Architect
- Andre McGregor, Former FBI special agent, Director of Security

Nasdaq

- Brad Peterson, Executive Vice President and Chief Information Officer (CIO)
- Joan Conley, Senior Vice President and Corporate Secretary of Nasdaq
- Louis Modano, Senior Vice President, Chief Information Security Officer (CISO) and Global Head of Infrastructure Services, Nasdaq

INDUSTRY EXPERTS

- Kris McConkey, Lead for cyber and insider threat intelligence, detection and incident response, PwC
- Ben Hammersley, Editor at large at Wired UK magazine, and presenter of Cybercrimes with Ben Hammersley on BBC and Netflix.
- Guy Allen, Head of IT Change Delivery & Enterprise Architecture, Cath Kidston
- Dr Jessica Barker, Cybersecurity consultant, looking at the human side of cybersecurity.
- Professor Marco Gercke, international expert in the field of law related to Cybercrime, Cybersecurity and ICT and director of the Cybercrime Research Institute
- TK Kerstetter, Chief Executive Officer, Boardroom Resources LLC and Host of “Inside America’s Boardrooms”
- Esther Dyson, Silicon Valley investment visionary
- Nicola Horlick, British investment fund manager, CEO Bramdean, Chairman Rockpool, CEO Georgina’s Restaurants, CEO Derby Street Films
- Matteo Berlucchi, CEO, Your.MD
- Knut Molaug, Chief Executive Officer at Green Mountain AS. Green Mountain design build and operate high security, robust wholesale colocation data centers.
- Youki Kadobayashi, Associate Professor in the Graduate School of Information Science, Nara Institute of Science and Technology, Japan
- Troels Oerting, Group Chief Information Security Officer (CISO) at Barclays
- Stephen Page, Non-executive director of the National Crime Agency, non-executive director of the British Standards Institution, and a board member of the British Library

Survey respondents provided by Survata.

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.