mimecast

# Behind the SCREENS:

## The Board's Evolving Perceptions of Cyber Risk

PART I

# Cybersecurity Enters the Boardroom - and So Does Economic Volatility

**The modern work surface is marked by interconnection: Hybrid working models have transformed the way organizations operate, changing how people communicate, share data, and collaborate.** Teams can work from virtually anywhere, thanks to email and more recently, collaboration tools such as Microsoft Teams and Slack.

CISOs and other security leaders sounded the alarm on elevated cyber risk due to the modern work surface, and thanks to well-publicized cyberattacks that are growing in both volume and sophistication, the C-suite and board have taken notice.

While email remains the primary attack vector targeted by threat actors, collaboration tools have introduced a new threat surface for cybercriminals to infiltrate, creating even more risk for security leaders to manage. It has thus become increasingly critical to ensure business communications remain protected, especially given that the volume of email-related threats **increased in 82%** of organizations **over the last 12 months**.[1] A common misconception of many business leaders today is that the use of well-regarded, though disparate, security solutions is sufficient to ensure their business communications are safe and secure. However, the risk of experiencing multi-stage, multi-vector cyberattacks such as ransomware and business email compromise (BEC) – along with the devastating effects they can have on a company's revenue and reputation in the face of looming economic volatility – remain but a click away.

Cybersecurity – and the notion that cyber risk is business risk – must permeate employee behavior. Cybersecurity is everyone's responsibility, and CISOs must drive this message forth to the board to recognize and react.

To learn more about current perceptions of cyber risk by the C-suite and board, we spoke with **78 leaders from 12 countries** to dig deeper into their efforts to articulate risk and what leadership must do to work protected, even as cyberattacks proliferate.


Email-related threats have increased in **82%** of organizations over the last 12 months.

[1] Mimecast *State of Email Security* 2023

PART II

# Cyber Risk Equals Business Risk

**Keep cybersecurity - and the link between cyber risk and business risk - front of mind in board-level communications.**

Though it may sometimes seem like cybersecurity operates in a vacuum, the wider business context in which they take place can deliver shockwaves. For instance, cyber risk is forecast to keep increasing in the medium- and long-term, in reports at the World Economic Forum's (WEF's) annual meeting in Davos. In fact, 2023 is the first year in which cyber risk made the top 10 list of long-term concerns in the WEF's annual Global Risks Report. The new rating heralds the longevity of the current wave of cyberattacks.[2] "Widespread cybercrime and cyber insecurity" is listed as No. 8 on the list of risks ranked by severity, behind global issues related to climate change, natural disasters, and involuntary migration — but ahead of geoeconomics confrontations and environmental damage. It is promising that some boards are now regularly discussing the risks posed by increases in cybercrime. These macro challenges are growing by the day, introducing a host of new considerations for individual businesses.

**"We're ahead of other banks, I believe, because a number of board members have strong cybersecurity expertise. The biggest advantage of this is that these specific board members can educate other board members on cybersecurity related matters."**

*IT and Infrastructure CTO, financial services, 1,000+ employees, United Arab Emirates*

**"I feel the board considers cyber risk to be just another business risk but that has a higher potential impact. The main difficulty, as I see it, is that it's very hard to quantify cyber risk without a significant breach, and it all turns on a dime once there is one."**

*CIO, consulting sector, 1,500+ employees, APAC*

One consideration, for example, is that many CISOs recognize there is a knowledge gap on their boards, which places CISOs at a disadvantage when they need to prove ROI on cybersecurity initiatives.[3] Another major consideration is that in the face of economic volatility, when most companies around the world tighten their belts in every area of business including marketing, sales, and general technology, it can introduce even greater cyber risk due to shadow IT or outsourcing to untrustworthy third parties. Cyber risk isn't just an IT problem – it's a critical vulnerability that directly equates to overall business risk. With record-high inflation rates, more complex cyberattacks, and geopolitical tensions, companies simply can't afford a weak security architecture that leaves them susceptible to data breaches and puts their organizational stability in jeopardy.

2. Global Risks Report 2023, World Economic Forum
3. Cyber Chiefs Face Scrutiny and Challenges in 2023's Uncertain Economy, *Wall Street Journal*

# PART II

Even with a looming recession and a board-level cybersecurity knowledge gap, most security leaders in this survey believe they need a budget increase of **10% to 20%**, and they feel they're likely to get it. Indeed, in frequently attacked sectors like critical infrastructure or finance, cybersecurity spending is unlikely to be cut.[4] But to improve those chances, cyber leaders must clearly communicate the risks and the critical role cybersecurity plays to protect the business; they should also expect greater scrutiny regarding their spending. The cost of a breach will outweigh any cost savings measures the board might wish to take.

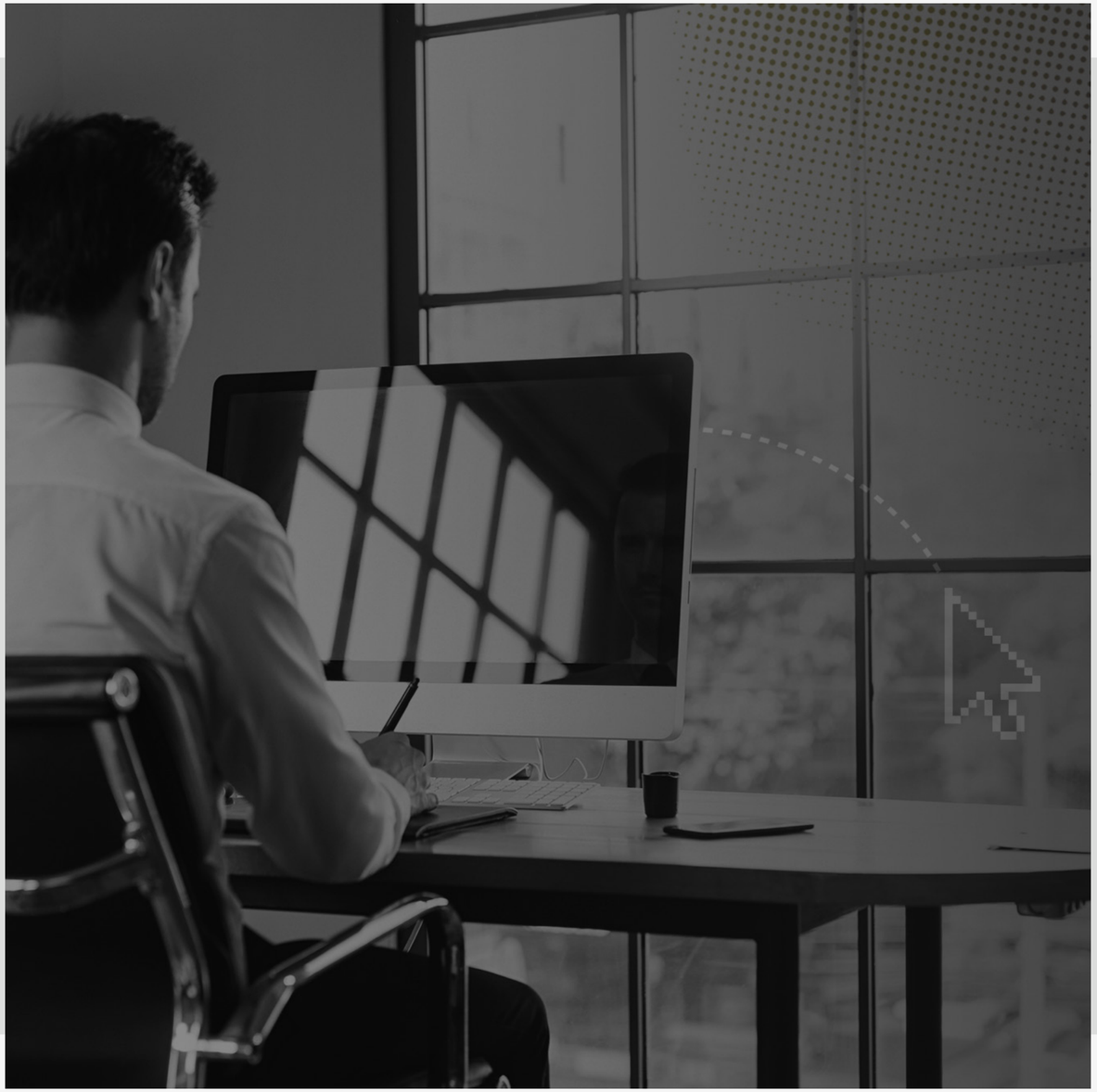
While technology downtime equating to lost sales can be quantified, the reputational damage done to brands that suffered a cyberattack is not easily measured but can't be underestimated; the loss of customer trust due to the years it takes to build it can be devastating.

Mimecast's Brand Trust report shows that **61%** of consumers would lose trust in their favorite brand if that brand disclosed personal information to a spoofed version of its website; the loss of trust directly reflects a loss of revenue as over half (**57%**) of respondents would stop spending money with their favorite brand if they fell victim to a phishing attack.


of consumers would lose trust in their favorite brand if that brand disclosed personal information to a spoofed version of its website


over half of respondents would stop spending money with their favorite brand if they fell victim to a phishing attack


[4] Cyber Chiefs Face Scrutiny and Challenges in 2023's Uncertain Economy, *Wall Street Journal*



**"Sometimes they do not understand the cost of a particular kind of attack. That's when I have to open up my business brain (leaving aside my technical and security know-how) and attempt to convey the quantification of the loss to them and if we are potentially under threat."**

*CTO, entertainment industry, <500 employees, Singapore*

Additionally, threats from cybercriminals continue to grow more sophisticated and persistent while a smaller talent pool forces employers to ask more of cybersecurity analysts and engineers; against this backdrop, hiring and retaining cybersecurity professionals has become exponentially more difficult. On average, cybersecurity roles take 21% longer to fill than other IT jobs, and there's an annual shortfall of tens of thousands of cyber roles to be filled.[5] These growing demands are leading to more stress, burnout, and resignations.

The most cyber-savvy board members understand that investing in cybersecurity isn't just about mitigating the chance of a cyberattack today. Maintaining cybersecurity investment enables companies to preserve their brand's reputation, reduces the risks of regulatory fines and lost sales in the event of a successful attack, and minimizes the stress cybersecurity employees face, effectively reducing turnover of a highly specialized skillset that's difficult to find. In short, investing in cybersecurity equates to good business.

**"...it can be challenging to retain talented cyber experts. Cyber resources are limited, and we need to figure out a way to keep the people we've hired or trained for the future. We currently lack skilled workers by roughly 30%, which is an issue – and in this industry, you won't find good resources at a reasonable price. The budget for cybersecurity is adequate but because there are so many untrained people, it's difficult for us to hire workers."**

*CFO, financial services, 1,000+ employees, South Africa*

5. CyberSeek

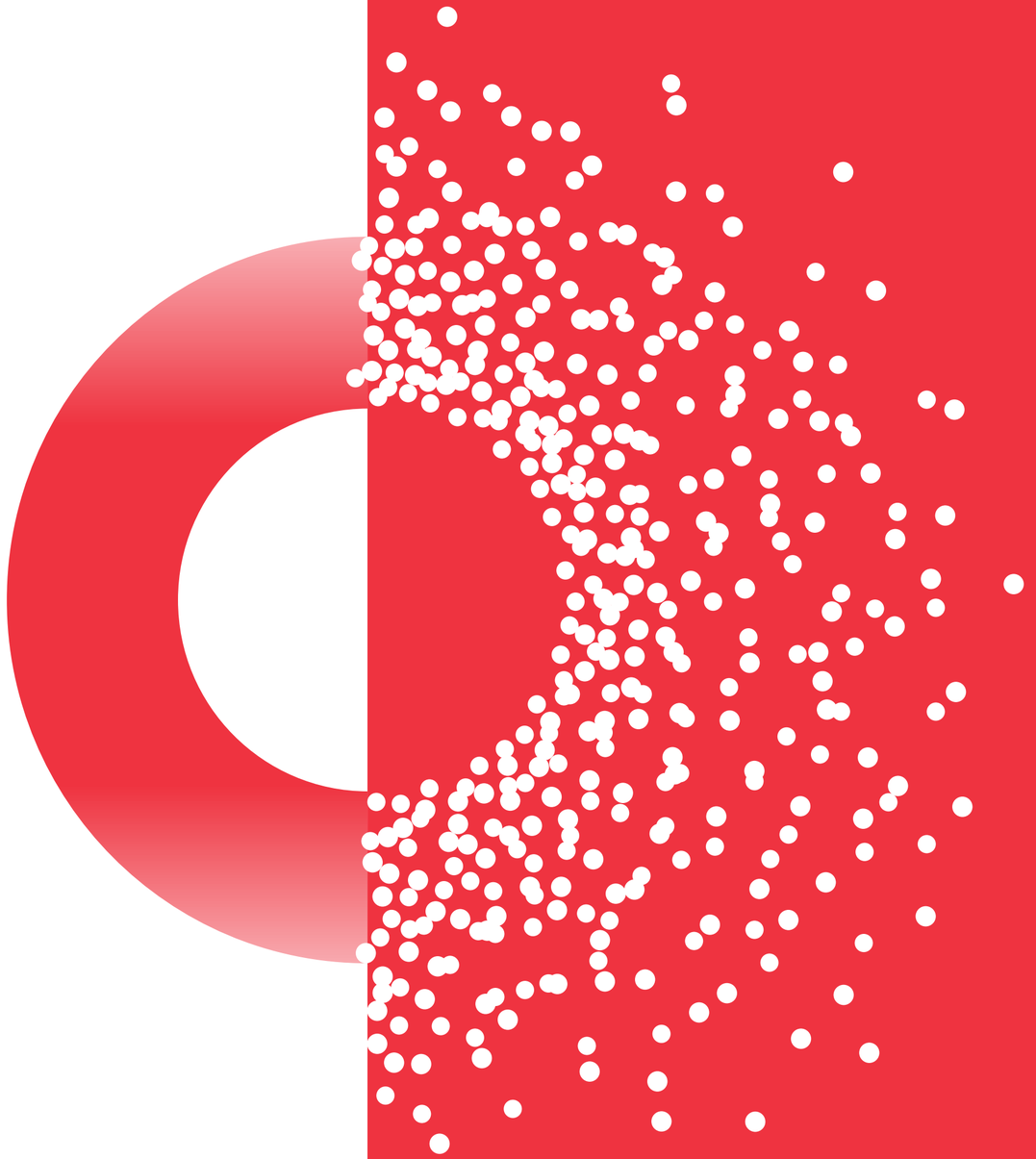
To highlight the connection between cyber risk and business risk, C-level respondents recommend:

1. Avoid jargon while working to demystify the mid- to long-term risk that cyber threats can present.

2. When communicating the benefits of investing in best-of-breed solutions, link cyberthreats to business outcomes. Some leaders recommend avoiding focusing on how an attack happened and instead zoom in on why it happened – for instance, heavy reliance on a monolithic security provider.

3. Devise mechanisms that allow you to align cyber risk with the overall business risk in order to create a built-in cybersecurity functionality.

4. Avoid turning every incident into a crisis – be tactical when framing cyber risk to the board so they can accurately quantify it without requiring a breach to drum up urgency.



"My advice to CISOs is to not turn everything into a crisis. Be judicious with what you raise to avoid becoming 'noise'. Keep your powder dry for the big incidents you want to raise and get the board and senior leaders to influence change."

*CISO, tech sector, 180,000+ employees, United States*

PART III

# Value and Efficacy Via Layered Cybersecurity Framework

**Implement tools that cover your business' needs, while also considering organizational size, complexity, and sector.**

Businesses are operating in a complex, volatile environment while enduring more sophisticated threats; in response to these market conditions, CISOs are being forced to scrutinize budgets and cybersecurity technology through the well-known "people, technology, and process" lens.

More than **90% of cyberattacks** come through email, bringing a reminder that risk tolerance and risk management frameworks should be frequently revisited by identifying the business' mission and the resources to be protected, as well as regularly communicating the state of cybersecurity risk to stakeholders. CISO-led tabletop exercises are another tool that improve companies' cybersecurity posture and incident response plans, and when properly communicated, can help employees better understand the consequences of poor cyber hygiene.

From a technology standpoint, CISOs must seek more coherent, comprehensive, and automated ways to view activity, protect against data exfiltration, and act faster to limit attack impact. It's no longer enough just to invest in security tools – in fact, many organizations have experienced bloated or disconnected security environments over time.

**"We have a refined risk management approach that focuses on technology processes and cyber control frameworks and financially supports the team by investing in systems, infrastructure, and new technologies to secure and stable platforms to mitigate any emerging threats."**

*IT and Infrastructure Support Analyst (Direct report to CISO, Team Lead), Australia, 1,000 employees*


More than 90% of cyberattacks come through email

PART III

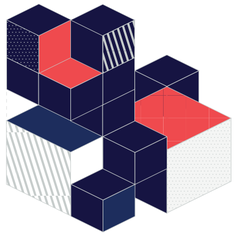
Instead, it's critical to make way for tight integrations and layered security frameworks to protect data across the organization and throughout its lifecycle while avoiding the trap of a highly attacked monolithic security platform like Microsoft 365. Indeed, security vendors must meet the needs of businesses that expect more or better functionality for the same cost, which puts a premium on solutions that focus on integrations to prevent and minimize attack impact. An effective way to do this is by maximizing the partnerships businesses have with existing vendors, such as technology API programs or alliances; in fact, **8 in 10 companies** are more likely to work with a cybersecurity vendor with an open API platform.[6]

**"As a CIO, I must ensure that the organization has the most up-to-date systems and technology that will offer a strong foundation for mitigating cyberattacks."**

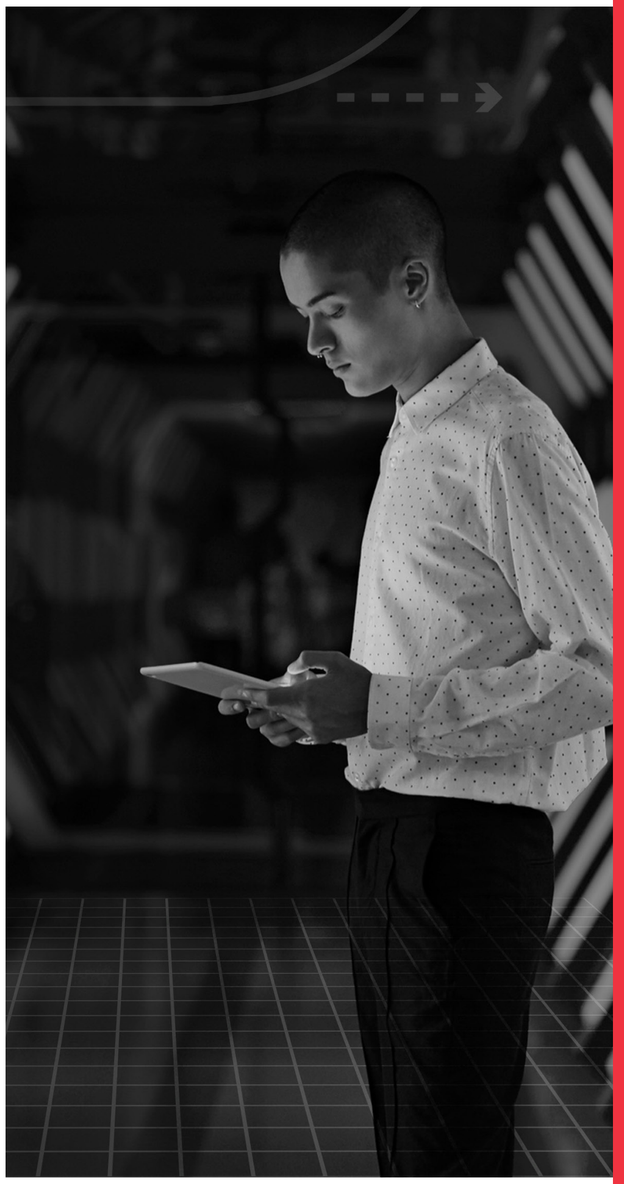
*CIO, financial services, Germany, <1,000 employees*

The aim is to create a defense-in-depth model that enables cybersecurity teams to detect and remediate cyber threats quickly. A collection of best in class security products that share data and analytical insights, offering true layered security that helps SOC teams link prevention, detection, investigation and response across tools and businesses. This kind of model is a welcome departure from even the best single vendor solutions that can allow attackers to take root, undetected, in security environments.

Additionally, to augment this approach and retain talent by reducing SOC fatigue, many companies are investing more in automation tools. But skilled employees are still needed to implement and manage these layered, automated tools.



**8** in **10** companies are more likely to work with a cybersecurity vendor with an open API platform.



"The first would be to discuss the approach to defense-in-depth, from the highest level to the bottom of the organizational pyramid. It is necessary at every level to know cybersecurity. And what our organization is doing to keep ourselves safe."

*CTO, Singapore, entertainment sector, <500 employees*

6. Mimecast *State of Email Security* 2023

**To strengthen security postures via layered cybersecurity frameworks, C-level respondents recommend:**

1. Determine the main threats to the business and create a risk profile of the organization. Email-based attacks such as phishing and account takeover are hugely concerning, so picking a solution that factors in the industry sector, security environment complexity, and regulatory environment is key.

2. Maximize vendor relationships to produce a defense-in-depth model that is as lean as possible.

3. Once the risk profile is complete, develop a cybersecurity framework addressing all the main concerns and build out the cybersecurity layers needed to combat the identified threats. Implement key performance indicators, then monitor and adjust the framework accordingly with input and involvement from the corporate board.

4. In more complex environments, security leaders can prevent data loss with fewer resources by applying more intelligence via machine learning technologies and traditional analytics; they can also apply more automation, including offloading repetitive manual tasks that can drain cybersecurity employees and exacerbate the skills shortage.



"In board meetings, we emphasize developing a strong IT infrastructure along with staff with good cybersecurity knowledge. The discussion involves all the parameters of IT infrastructure, security surveillance, data centre virtualization, firewall migrations, and what new process can be added to our current set-up to protect our business from any data breach."

*CTO, pharmaceutical industry, 1,500+ employees, Canada*

PART IV

# Phishing Protection is a Team Sport

**Secure your organization by protecting against phishing and investing in security awareness training for employees.**

Email-based attacks are on the rise at three out of four companies, and the same number are bracing for serious consequences from such an attack in the coming year.[7] In response, the C-suite has become attuned to creating a company-wide security culture,[8] more specifically, investing in awareness training in tandem with layered cybersecurity frameworks to minimize the likelihood of a successful attack.

> **"Our board understands that email is still one of the main attack vectors, which is why we have had significant investment in email security."**

*CISO, retail sector, 1,000+ employees, UK*

Email is an appealing attack vector for cybercriminals due to its ubiquity and volume both inside the workplace and out. And even with best-of-breed cybersecurity solutions, human error will always leave a gap for attackers to walk through.

> **"Email is currently the biggest threat, and phishing emails are the most common way of stealing information from the organization. It's one of the highest risk areas and the most concerning area for me. We had a phishing emails attack before that resulted in the hacking of people's mailboxes, and we report such scenarios to the Information Commissioner's Office (ICO)."**

*Director of Technology, public services, 1,000+ employees, UK*

Phishing is one of the original cyberthreats, and it persists because attackers can continually adapt their approach. What's more, automation tools and phishing kits are making it easier for a less skilled cybercriminal to cast a wider net, which can cause greater damage to businesses. Against the backdrop of the global pandemic, the recent *State of Email Security* report revealed that a full **97% of businesses** have experienced phishing attacks, and **59%** have reported a significant uptick in the phishing threats they face.

7. Cyber Risk and the C-Suite in the State of Email Security, Mimecast
8. Cyber Risk and the Board: Support Fuels Cyber Awareness Training, Mimecast

PART IV

**"It's human error, and you cannot analyze what's happening in a person's mind. We can only train employees not to click on unnecessary links, but it's up to them whether they take that seriously or not. So, as long as email compromise and phishing exist – and continue to work – there will always be a hole in cybersecurity."**

*CISO, retail industry,*
*1,000+ employees, Australia*

To mitigate these persistent and adaptable threats, CISOs are focusing on developing a security-aware culture throughout the entire business – inclusive of board members. But changing human behavior isn't simple or fast. Cyber awareness training and remediation efforts take time to yield results compared to the implementation of email security or other technology tools. That's why more leaders are realizing how valuable a culture that prioritizes cybersecurity is to long term safety. But creating such a culture requires persistence, creativity, and a highly visible commitment from leadership.

Supply chain vulnerabilities, the rise of online collaboration and the growth of digital networking are among the chief reasons the cyber landscape is becoming more treacherous. The explanation is simple: The intersection of communications, people, and data carries a tremendous amount of risk, as malicious actors exploit the modern work surface. Digital transformation efforts businesses were implementing prior to the pandemic were already subject to record-breaking numbers of data breaches. But with firms rapidly expanding their digital communications channels in the pandemic's wake, they also inadvertently widened the attack surface for bad actors to breach.

PART IV

**"At board level, I'd like to have more discussions around the psychology of dealing with cyberattacks such as ransomware attacks. Looking at the non-technology perspective of these events would be beneficial. We also need to discuss how we can make cybersecurity everyone's problem, not just the head of IT's."**

*IT Executive General Manager, Infrastructure, 2,500+ employees, Australia*

Simply knowing what a spam or phishing email can look like will only go so far. That's why contextual knowledge, and the full support of the business that security is everyone's responsibility, can help maximize the benefits of awareness training.

Organizations of all stripes are in a pivotal moment, and widespread change seems inevitable. But defining a strategy that addresses critical cybersecurity issues – from ensuring internal systems and customers are secure, to relieving the pressure on cybersecurity professionals – won't be an easy task. And it will require the active participation of not just the board, but every individual companywide.

**To protect against email-borne threats and develop a security-aware culture, C-level respondents recommend:**

1. Phishing is a concern that's not going away, no matter your business' industry sector, company size, or region. Ensure that everyone practices better cyber hygiene and feels safe to communicate potential cyber threats. These practices are a vital aspect of any business' ability to mitigate cyber risk.

2. Creating a security culture that permeates the board, C-suite, and all organizations within the business is a fundamental practice of decreasing cyber risk. For these foundations to be effective, it is imperative to make cybersecurity every employee's responsibility.

**PART V**

# The Bottom Line:

**A leadership role in cybersecurity has never been more complex:** Increasingly sophisticated, high volumes of attacks are infiltrating organizations due to the modern work surface, while hiring cyber practitioners continues to be a challenge. And yet, **the opportunity for CISOs to protect their organizations has never been better**: Keep the link between cyber risk and business risk front of mind when speaking to the board; avoid the trap of a monolithic security provider by implementing layered, best-of-breed cybersecurity tools; and secure against age-old threats like phishing with email protection and awareness training for employees. Security leaders must understand their risk profiles and communicate them well, simultaneously reducing the attack surface and maximizing controls.

Corporate boards are finally paying attention to cybersecurity, but they still have many other big priorities, such as a likely recession, climate change, and geopolitical uncertainty. So, more attention doesn't automatically translate into more money or benefits for cyber defenses. **More attention means more scrutiny** — but the opportunity to highlight cyber risk as business risk is here.

Security leaders must understand their risk profiles and keep the link between cyber and business risk front of mind when speaking to the board.

PART VI

# Methodology

**About the Results Included in This Report**

Survey participants worked at organizations ranging from under 500 employees (35%), 501 to 1,000 employees (33%), and those with more than 1,000 employees (32%).

These companies were spread across **five sectors**, including financial services (29%), healthcare (21%), public sector (15%), retail (15%), and entertainment (19%).

There were **78 survey participants** from companies in Australia, Singapore, France, Germany, Netherlands, Sweden, Denmark, United Arab Emirates, Saudi Arabia, Canada, United States, and United Kingdom.

# Work Protected.

Advanced Email & Collaboration Security

mimecast



**Mimecast: Work Protected™** Since 2003, Mimecast has stopped bad things from happening to good organizations by enabling them to work protected. We empower more than 40,000 customers to help mitigate risk and manage complexities across a threat landscape driven by malicious cyberattacks, human error, and technology fallibility. Our advanced solutions provide the proactive threat detection, brand protection, awareness training, and data retention capabilities that evolving workplaces need today. Mimecast solutions are designed to transform email and collaboration security into the eyes and ears of organizations worldwide.