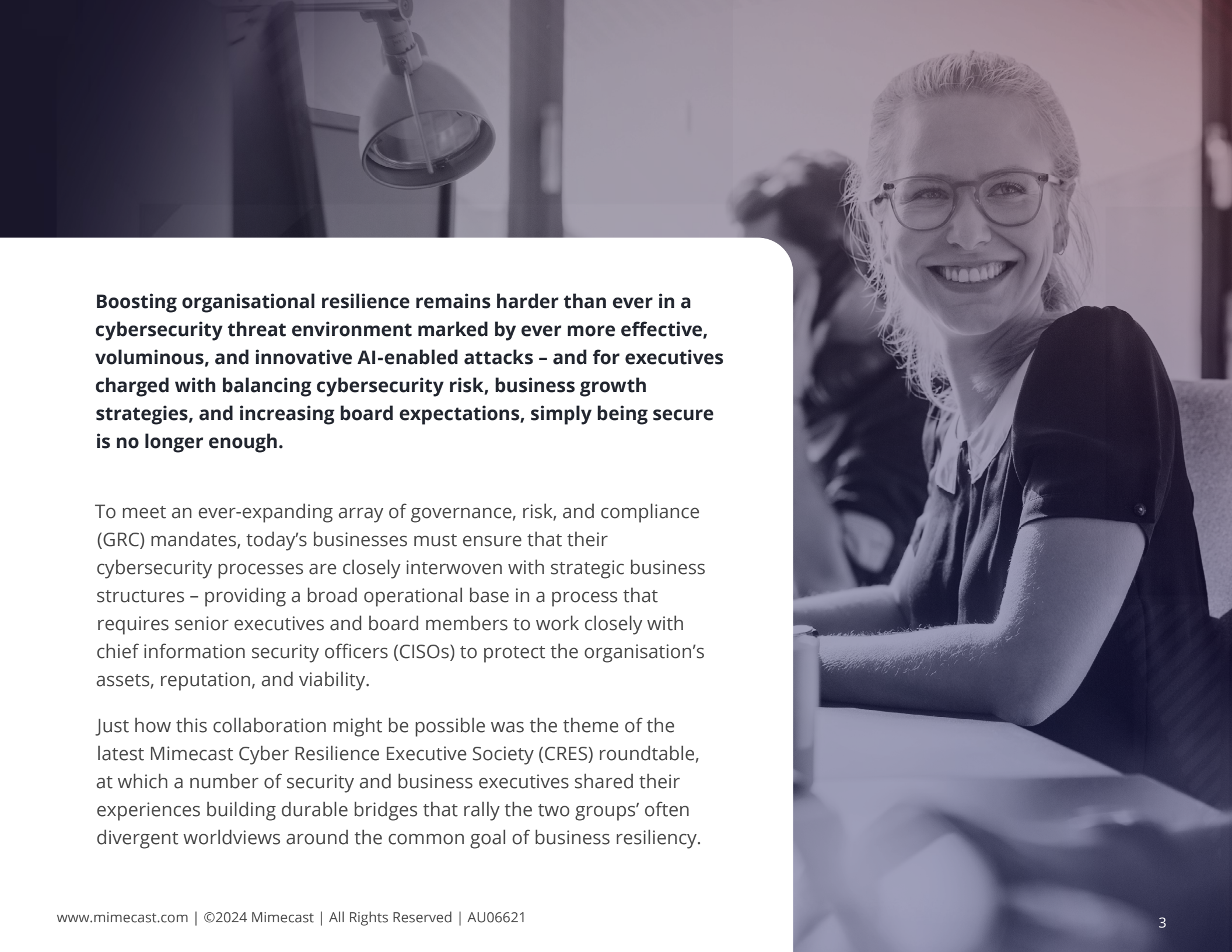


**mimecast**

# AI, human risk continue to challenge companies' cybersecurity maturity

*Find common purpose across the business,  
Mimecast's Cyber Resilience Executive Society recommends.*



A smiling woman with blonde hair and glasses is sitting at a desk in an office. She is wearing a dark blue short-sleeved shirt over a white collared shirt. The background is slightly blurred, showing another person and office equipment. The overall tone is professional and positive.

**Boosting organisational resilience remains harder than ever in a cybersecurity threat environment marked by ever more effective, voluminous, and innovative AI-enabled attacks – and for executives charged with balancing cybersecurity risk, business growth strategies, and increasing board expectations, simply being secure is no longer enough.**

To meet an ever-expanding array of governance, risk, and compliance (GRC) mandates, today's businesses must ensure that their cybersecurity processes are closely interwoven with strategic business structures – providing a broad operational base in a process that requires senior executives and board members to work closely with chief information security officers (CISOs) to protect the organisation's assets, reputation, and viability.

Just how this collaboration might be possible was the theme of the latest Mimecast Cyber Resilience Executive Society (CRES) roundtable, at which a number of security and business executives shared their experiences building durable bridges that rally the two groups' often divergent worldviews around the common goal of business resiliency.



CISOs are core to those relationships, providing a solid evidentiary base that illustrates the current and desired end state for organisational cybersecurity – something that can be difficult to attain amidst an ever-changing risk climate characterised by vulnerabilities in legacy applications, the challenges of securing new cloud infrastructure, unknown risk from the infrastructure of trusted third parties, and end users that are often creatures of habit no matter how much cybersecurity training they receive.

Ongoing Mimecast research has identified the cost of such shortcomings, with one Mimecast [survey](#) of more than 3,000 employees and 600 cybersecurity decision makers finding that although 94% of respondents said they had experienced a security threat through their chosen collaboration tools, just 9% of organisations monitor their employees' use of those tools.

That's a huge gap that leaves companies vulnerable to attack – and real-world feedback confirms that such attacks are common, with 54% of survey respondents reporting they had suffered loss of company data, 36% had lost potential customers, 32% had lost current customers, and 30% had seen their companies suffer reputational damage after a breach.

**94% of respondents said they had experienced a security threat through their chosen collaboration tools, just 9% of organisations monitor their employees' use of those tools.**

“The modern workplace has experienced explosive change in a short period of time,” Mimecast SVP of Product Management Sean Brady said, noting that the growth of hybrid work had made collaboration tools “essential to productivity – but cybercriminals know this and are increasingly seeking to exploit this.”

CISOs know this as well, which is why they need to actively engage with both executive and end-user communities, translating complex security risks into actionable insights that resonate with senior executives and the board.

Follow-through is particularly important, since the survey found that 85% of respondents believed their organisation had effectively communicated the security risks of collaboration tools to their employees – but just 10% of employees said they had received dedicated security training related to the tools.

## **Aligning business expectations with security reality**

This gap highlights the enduring challenges that organisations face in matching cybersecurity policy with action – and reinforces the importance of embracing cybersecurity practice as an integral part of company growth strategies; acknowledging the importance of robust training and awareness programs in addressing chronic issues around human error; aligning board expectations around cybersecurity with the organisation’s ability to provide adequate solutions; and proceduralising processes for regularly evaluating, adapting, and enhancing cybersecurity strategies to keep up with ever evolving security threats.

These four themes were regularly raised during discussions at the CRES meeting – painting a detailed picture of an Australian cybersecurity threat environment that echoes the global findings of Mimecast’s recent [Q4 Global Threat Intelligence Report](#), which identified extortion campaigns, geopolitical threats, and attacks on small and medium-sized businesses as the biggest threats to their cybersecurity defences.

Ongoing geopolitical disruption has fuelled a fluid threat environment in which, for example, more than 100 hacker groups have claimed participation in the Israel-Gaza conflict



alone – contributing to a heightened climate of attacks in which Mimecast blocked a record of nearly 250 million attacks against its customers' businesses in January alone.

That translated to as many as 31 and 32 threats per user (TPU) in small and medium-sized businesses, respectively, compared with 15 TPU in larger companies – a difference that reflects the relatively high number of responsibilities and system privileges typically and necessarily assigned to each SMB user.

"It is deeply concerning that nation-states are using cyber operations to gather intelligence on rival governments and attack critical infrastructure and information systems," Mick Paisley, chief security & resilience officer at Mimecast, said.

"Organisations must act to ensure they and their employees are protected against this continuing uptick in malicious activity."

The magnitude of this obligation, CRES attendees shared during the session, reinforces the importance of holistic strategies that address both technological and human factors – with organisations adopting proactive measures to mitigate risks, enhance resilience, and ensure continuity of operations.

**"Organisations must act to ensure they and their employees are protected against this continuing uptick in malicious activity."**

Among the specific strategies discussed were recommendations that business and technology leaders:

- Adopt a risk-based approach to cybersecurity.
- Conduct comprehensive business impact analyses to appreciate the potential impact of cyber incidents on critical functions and revenue streams.
- Position cybersecurity as a catalyst for innovation, customer trust, and competitive advantage rather than merely a cost centre.
- Prioritise compliance with relevant regulations and standards to mitigate legal risks and uphold customer trust.
- Develop robust incident response plans to detect, respond to, and recover from cyber incidents effectively.
- Allocate adequate resources to address evolving cyber threats and ensure investments align with industry benchmarks and best practices.
- Implement comprehensive training and awareness programs to educate employees about cyber threats and foster a culture of security.
- Mitigate third-party cybersecurity risks with thorough vendor assessments and due diligence processes.

## Walking the walk

Although the nature of the cybersecurity threat is continually changing, recent engagement with business and cybersecurity leaders suggests that many companies are successfully taking positive steps to improve business-IT engagement.

Mimecast's recent [State of Email & Collaboration Security Report \(SOECS\) 2024](#), which analyses the results of interviews with 1,100 security leaders worldwide, showed just how much progress has been made to date – and how much work is still yet to be done.

Reflecting progress in codifying companies' desired end-states when it comes to cybersecurity, nine out of 10 companies now have a formal cybersecurity policy in place – with 48% saying that strategy spans all key business functions.

Broad commitment to cybersecurity policy varied by industry, with financial services – in which 60% of companies had a fully integrated cybersecurity strategy – the highest, compared with media and entertainment companies where just one-third had done the same.

Yet 43% of respondents said responsibility for cybersecurity strategies is still being fobbed on to the IT department – an outdated approach that perpetuates the divide between business and IT objectives, often making it harder for security leaders to build consensus about the importance of organisational cybersecurity, or to secure adequate funding to make it a reality.

As intimated during the CRES meeting, human error remains a significant source of conflict within companies of all sizes and types, with many cybersecurity professionals still frustrated about insufficient funding, lack of organisational support, and senior management pressure to limit investments in security protections to high-profile collaboration platforms while other parts of the infrastructure are left underfunded.

As cybersecurity executives wrestle with management over the particulars of cybersecurity defence, the risk posed by human factors – which are still involved in nearly 74% of all breaches despite decades of education designed to address them – continue to challenge cybersecurity defences.

Attending CRES members readily admitted there was still work to be done in addressing human risk, and emphasised the importance of a range of initiatives that have proven most successful in building a strategy that is well integrated across business units.





Not only should employees receive regular training and awareness programs that are tailored to specific business units, for example, but attendees recommended involving employees in the development of that training, as well as in the development and implementation of cybersecurity policies and procedures.

Companies should also invest in human capital by allocating resources for employee training and development – with ongoing training and awareness programs educating employees about their roles and responsibilities during a cyber incident.

This inclusive approach helps foster innovation and reinforce the championing of success stories, creating a culture of innovation in which employees are actively encouraged to identify and address cybersecurity challenges before they are exploited by cybercriminals.

**80% express concern about the use of AI to attack their organisation**

## **Turn the AI challenge into a security opportunity**

No discussion about today's cybersecurity climate would be complete without a mention of the new threat posed by generative AI (GenAI) tools like ChatGPT and a host of similar tools that are – by improving spelling and grammar, simplifying the creation of malware applications, and enabling large-scale personalisation of phishing messages – actively helping cybercriminals become less conspicuous and more effective in targeting corporate and individual victims.

SOECS respondents highlighted a paradox in this respect, with 86% of security executives confident they will be able to respond to an AI-spawned attack as well as any other attack – even though 80% express concern about the use of AI to attack their organisation.

With GenAI, the most significant step change in cybersecurity attack method in years, businesses are well advised to take its rapid growth as a motivator for change – and to use the opportunity to extend cybersecurity across the organisation in ways they haven't been able to do in the past.

This includes, for example, the creation of cross-functional teams with representatives from a range of business departments – think IT, finance, operations, and HR, all of which will be targeted by AI-powered attacks in different ways.

By drawing out the commonalities in the exposure these departments face, business and cybersecurity executives will find it easier to find and build upon a common purpose – for example, by identifying critical processes and workflows into which cybersecurity can be integrated most seamlessly.

With AI catalysing an alignment of purpose across the business, cybersecurity leaders will find it easier to co-ordinate the many other elements of an effective cybersecurity posture – including regular risk assessments, development of cross-department incident response planning, stress testing of core systems, and definition of clear, agreed key performance indicators (KPIs) and metrics that enable benchmarking of security practices and tracking of change over time.

These and other initiatives, CRES attendees pointed out, contribute to the establishment of an ‘anti-fragile’ approach to cybersecurity that implements multiple layers of defence, including technical controls, policies, and procedures,

to mitigate the impact of cyber threats – ensuring at all times that cybersecurity considerations are integrated into business continuity planning and aligned with overall organisational objectives.

By building a commonly supported cybersecurity culture – and the technical and procedural infrastructure, data collection systems and regular tracking against best practices to support it – the consensus from the group was that any company to improve their cyber resilience if they take the right approach.

The key, participants ultimately agreed, is to approach cybersecurity as a clear and present danger to organisational integrity – and to use clear metrics to track and refine strategies for addressing this danger.

In this way, the roundtable participants agreed, organisations can enhance their cybersecurity posture, improve resilience to cyber threats, and safeguard their operations, assets, and reputation in an increasingly digital environment.