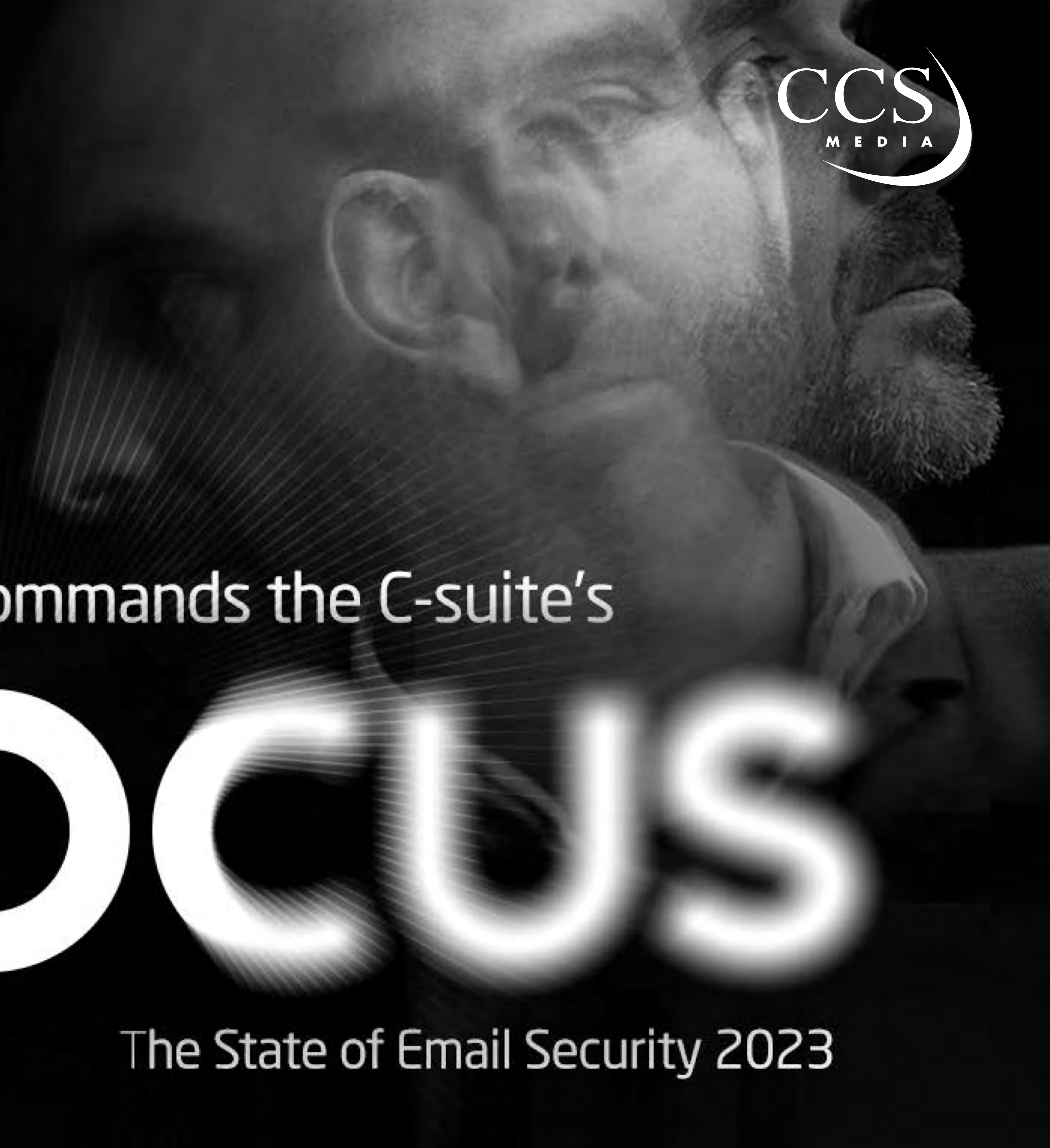
mimecast

CCS MEDIA



# Cyber Risk Commands the C-suite's FOCUS

## The State of Email Security 2023

# Breakthroughs at the Board Level

As companies grow more skittish over rising economic volatility and intensifying geopolitical tensions, a more conservative approach has spread to all areas of business. This especially includes the digital domain, where risks that senior executives endured a few years ago are now viewed as unacceptable.

Deloitte puts it this way: “The risk landscape is changing fast. Every day’s headlines bring new reminders that the future is on its way, and sometimes it feels like new risks and response strategies are around every corner.” Among the key challenges singled out by the corporate consultancy are the disruptions resulting from emerging technologies and shared risks associated with the networked economy. [1]

As cyber threats have multiplied, the global business community has become increasingly sensitive to the danger and is demonstrating a greater willingness to confront it — sentiments that come through loud and clear in Mimecast’s 2023 report on The State of Email Security, the seventh annual study of its kind.

Growing awareness of skyrocketing cyber risk shows up in other studies as well. An informal survey of business executives by Forbes sought to identify the most important risks facing corporate leaders in 2022. Despite climate change, inflation and the possibility of another financial crisis, the risk of a data breach headed the list.[2]

More evidence that concerns over cyber risk have assumed a new prominence in the C-suite comes from The Allianz Risk Barometer — an annual survey of corporate insurance experts, including brokers, underwriters and risk consultants — published by insurance giant Allianz Global Corporate & Specialty (AGCS). For 2022, the survey found that the threat of a cyber incident was the most important global risk facing businesses, well ahead of climate change, labor shortages and the possibility of a recession.[3]

**In the breakdown of our State of Email Security report that follows, the 1,700 CISOs and other information technology professionals surveyed bring the nature of the risks they face into sharp relief and present a realistic picture of the steps they are taking to overcome them.**

Data breaches are viewed as an even greater risk than climate change, inflation and another financial crisis.

# Key SOES findings 2023

## Email

Email usage continues to rise at **8/10** companies

●●●○

**3/4** have experienced an increase in email-based threats

## Cyberattacks

**59%** say cyberattacks are growing increasingly sophisticated

**2/3** were harmed by a ransomware attack

**97%** have been targeted by email-based phishing attacks

97

## Budget

**2/3** say their companies need to spend more on cybersecurity

●●○

## Monitoring

**98%** either have a system to monitor and protect against email-borne threats or are actively planning to roll one out

**92%** are either using or plan to use AI and machine learning to bolster their cybersecurity

**94%** think they need stronger protections than those that come with their Microsoft 365 and Google Workspace applications

94

99

## Cyber Awareness

**99%** provide some form of cyber awareness training to their workforce

**8/10** believe their company is at risk due to inadvertent data leaks by careless or negligent employees

## Collaboration Tools

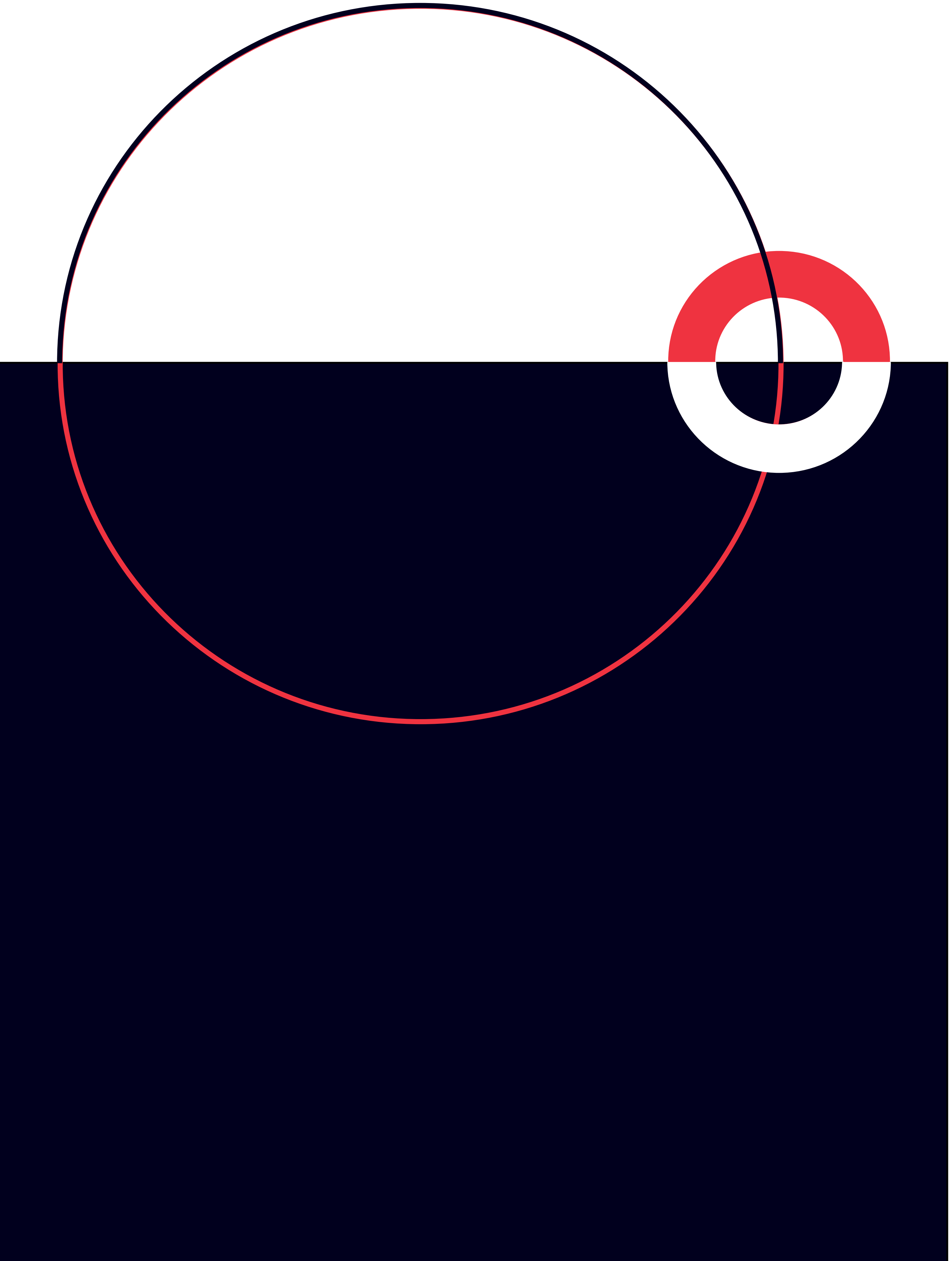
● ● ● ○

**3/4** collaboration tools are posing significant new security risks

**72%** expect to be harmed by a collaboration-tool-based attack

72

2



> **The explanation is simple: The intersection of communications, people, and data carries a tremendous amount of risk, as malicious actors exploit the interconnectedness of the modern work surface.**

## Contending with threats new and old

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 interconnectedness of the modern work surface.

Multi-stage, multi-vector attacks have become the norm, with criminals using one entry point to open the door to others. In today's networked business world, even small security shortcomings and mistakes can have a devastating domino effect.

2023

## 33 billion

electronic records are expected to be stolen [4]

## $8 trillion

Cybercrime is expected to cost the world $8 trillion. In economic terms, this is greater than the GDP of any country except the U.S. and China[5]

## $4.35 million

Globally, the average cost of a data breach is $4.35 million. The average cost in the U.S. is more than double that, at $9.44 million[6]

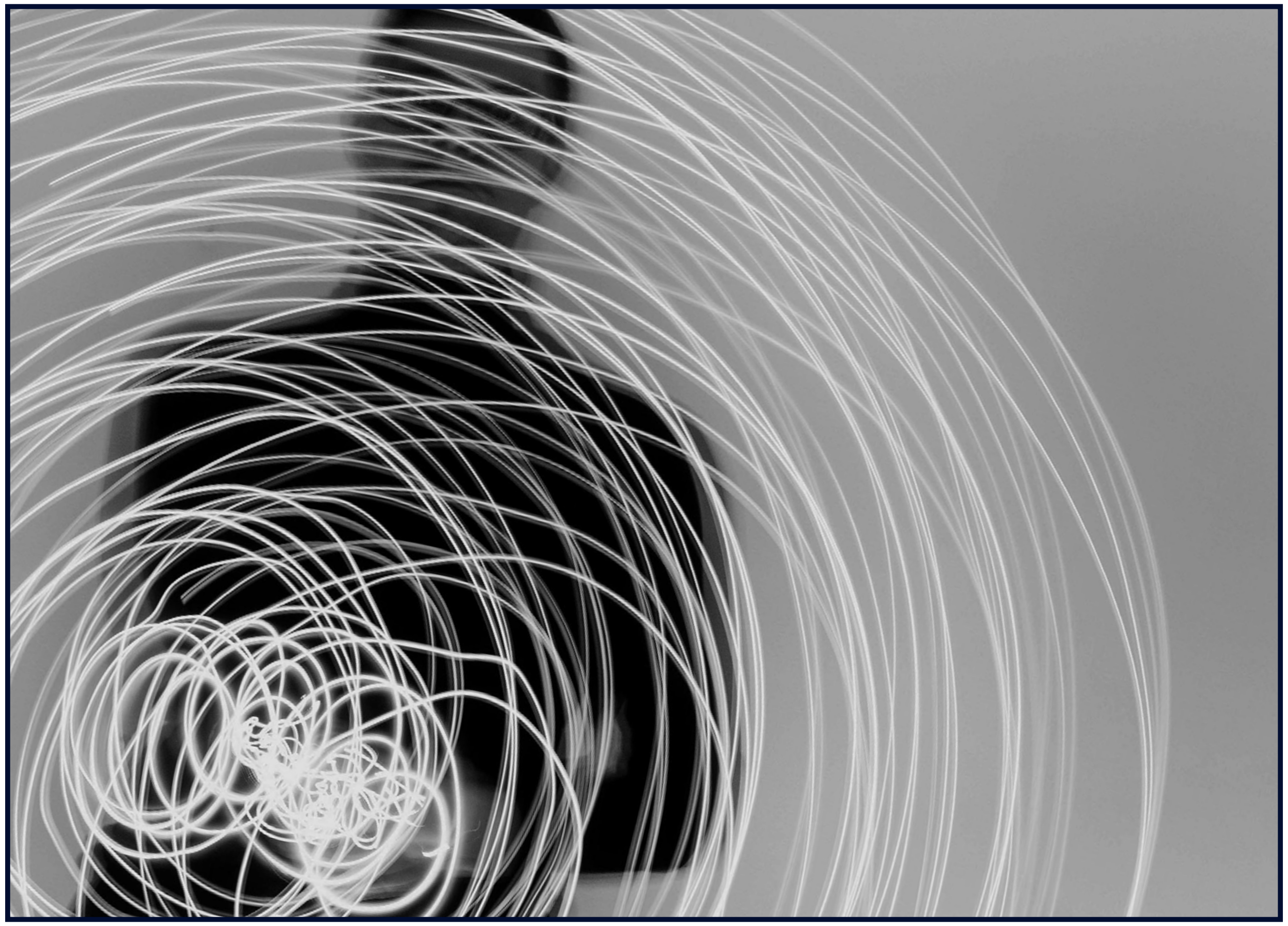
## 13%

There was a 13% rise in ransomware in 2022 — an increase as big as the past five years combined[7]

## 212 days

On average, it takes 212 days to detect a data breach and another 75 days to contain it[8]

**The cyber threats that have captured management's attention are daunting.**



## Email-based threats

For cybercriminals, however, email remains the primary route of attack; in fact, the State of Email Security (SOES) study found corporate reliance on email continues to grow at a rate outstripping the surge in email that took place at the outset of the COVID-19 pandemic — with 82% of companies reporting a higher volume of email in 2022, compared with 79% in 2021 and 81% in 2020. More email has led to more email-based threats, and three out of four (74%) SOES respondents say these have risen over the past 12 months.

But while the increasing number of threats is a problem, their growing sophistication poses an even greater danger.

Cybercriminals continue to refine and adapt their strategies, and malware kits on the dark web make it possible even for common criminals without technology smarts to employ highly sophisticated methods of incursion. Indeed, it is the increasingly sophisticated nature of the attacks they face that the 2023 SOES respondents singled out as their biggest challenge (59%).

**3OF4**

**three of four companies are bracing for serious consequences from an email attack**

The growing complexity of attacks is leading to a sense of foreboding on the part of the CISOs and other cybersecurity professionals who took part in the SOES survey.

Three-out-of-four (76%) expect an email-borne attack will have serious consequences for their organization in the coming year.

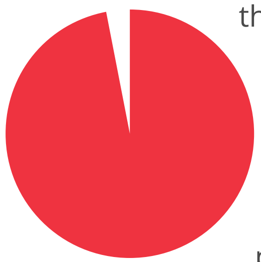
Of these, 7% believe that such an attack is “inevitable,” while another three out of 10 consider it “extremely likely.”

> **But while the increasing number of threats is a problem, their growing sophistication poses an even greater danger.**

## The terrible trio

**There are many different types of email-borne threats confronting these cybersecurity pros, but the three most prevalent are phishing, ransomware and spoofing. All told, 84% of security decision-makers have seen increases in at least one type of these attacks over the past 12 months, of which the most widespread is phishing.**

### Phishing



There were an estimated 255 million phishing attempts in 2022, a 61% jump over the prior year.[9] Worse yet, more than 70% of these emails were opened by the recipient.[10] Is there anyone anywhere who hasn't received a suspicious-looking email — or worse, an email that appears to be from a trusted party but isn't? This is why companies fear phishing — because it's easy to dupe someone into opening a malware-laden email and then sharing that email with another, spreading the threat. So, it's hardly surprising that 90% of corporate security breaches are the result of phishing.[11]

In the past year, virtually all of this year's SOES respondents (97%) have been the target of a phishing attack. The majority (59%) are experiencing more attacks than in prior years, and among large enterprises with more than 10,000 employees this is even more widespread, with 71% reporting a significant rise in phishing attempts. And among all respondents, 80% said they had experienced at least one attack where the threat had spread from one infected user to another.

### Ransomware

Two-thirds of this year's SOES respondents (66%) reported falling victim to ransomware, but in this case, it was smaller businesses that were affected more severely. Among companies with 250 to 500 employees, seven out of 10 respondents (70%) acknowledged that a ransomware attack had damaged their business, while 73% of companies with 1,000 to 5,000 employees admitted the same. Among large enterprises with a workforce of 10,000 or greater, fewer than half (46%) were harmed by ransomware.

Companies in certain industries also fell victim to ransomware more frequently. Among companies in the consumer services (87%), energy (83%), healthcare (80%) and media and entertainment (86%) sectors, more than eight in 10 were seriously damaged by a ransomware attack.

### Spoofing

Email spoofing remains a serious risk, especially for the public sector. Nearly all SOES respondents (91%) were aware of attempts to misappropriate their email domain, and close to half (44%) saw an increase in this type of activity in 2022. The increase was even more pronounced among government agencies and other public institutions, with 54% reporting more frequent email spoofing.

Web domain spoofing is also widespread, with companies uncovering repeated attempts to clone their websites. On average, companies identified 10 such attempts last year.

While most companies say they are at least minimally prepared to deal with spoofing, fewer than one-third (29%) say they are fully prepared to cope with illegitimate uses of their email domains (although this figure rises to 35% for companies with more than 5,000 employees). And while nearly nine out of 10 (88%) SOES respondents say their companies are interested in using Domain-based Message Authentication, Reporting and Conformance (DMARC) in the next 12 months to thwart email spoofing, well under one-third (27%) have actually deployed it.

# Collaboration Is a Double-Edged Sword

In the post-COVID era, the modern work surface  means that few  organizations can function without the use of collaboration tools. Software suites and their add-ons, such as Microsoft Teams, Google Workspace and Slack, integrate communications and messaging with project management functions. Designed to provide a central platform for data and document sharing, collaboration software helps businesses encourage virtual teamwork and work more efficiently, especially in the context of today's remote and hybrid work environments.

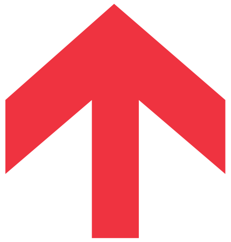
**3 of 4 companies expect to be harmed by a collaboration-tool-based attack.**

But while email remains the primary attack vector for bad actors, collaboration tools provide a new threat surface for cybercriminals to infiltrate. And this, in turn, creates even more risk for CISOs and their teams to manage.

## Collaboration Tools, Essential but Risky

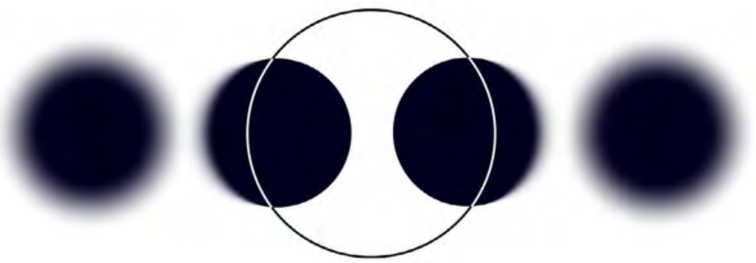
The 2023 SOES participants overwhelmingly agree (90%) that collaboration tools are essential to the well-ordered functioning of their companies. But two-thirds (67%) also say trying to keep pace with the number of collaboration tools their organizations use is an overwhelming proposition, and more than half (55%) complain that employees routinely download and use new tools that have not been vetted or approved by IT.

**At most companies (82%), use of these platforms continues to grow, and more than one-third of respondents (38%) say that the number of attacks due to collaboration tools is on the upswing.**



Even more tellingly, nearly three-quarters (72%) of SOES respondents say it is likely, extremely likely, or even inevitable that their organization will be negatively impacted by a collaboration-tool-based attack in 2023.

In line with this, three-quarters (75%) of respondents believe that collaboration tools pose new threats and create new security loopholes that urgently need to be addressed. This sentiment was even stronger among respondents at companies where the use of these tools significantly increased during the past 12 months (82%). And it was stronger still in the energy and media and entertainment sectors, where 87% of the respondents expressed grave concern about the risks arising from collaboration tools.



## Inadequate Safeguards

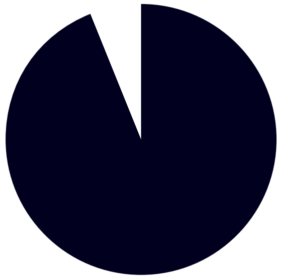
**SOES respondents harbor doubts that the security safeguards included with collaboration platforms offer adequate protection against the potential risks.**

Nearly two-thirds (62%) feel that most native collaboration tool security is insufficient to meet their needs. Almost as many (57%) know their own company's cybersecurity defenses are not capable enough to cope with the additional risks posed by these platforms.

It's also worth noting that when it comes to Google Workspace and Microsoft 365, there is near universal agreement (94%) that additional security measures are needed to supplement these platforms' native security functions.

To improve their defenses, there is a widespread sense that companies need to spend more on collaboration tool security. Two-thirds (66%) of the respondents believe that their organization needs to increase its budget for securing collaboration tools by an average of 8%. But, as we're about to see, these are not the only cyber protections for which more spending is needed.

# STRO
# NGER



94% of companies think they need stronger protections for their MS 365 and Google Workspace applications.

# Embracing Cyber Preparedness

CISOs have a powerful new ally in their efforts to bolster their companies' digital defenses: the corporate board.

As cyber risks have multiplied and business leaders are pressured to keep cyberattack headlines out of the news, corporate boards and C-suite executives have become much more alert to the threat and are displaying a new willingness to confront it.

**Respondents are sharply divided over the value of cyber insurance.**

## Uncertainty over cyber insurance policies

One subject over which SOES participants are sharply divided is cyber insurance — that is, whether such policies can serve as a substitute for developing a comprehensive cyber preparedness program. Many companies are skeptical of their value (50%), but almost as many (48%) see them as worthwhile additions to their safety net.

Different industries have widely divergent viewpoints on this. Less inclined to rely on cyber insurance policies are respondents from the business services (61%), construction (65%), consumer services (65%) and especially the energy (73%) sectors. But in other sectors, the majority of respondents strongly agreed that insurance provides a good degree of protection, including the IT and telecom industries (55%), healthcare (66%) and media and entertainment (66%). This split of opinion also holds true for companies of different sizes: A majority of midsize companies with 500 to 1,000 employees (59%) view cyber insurance as an integral part of their cyber preparedness, while six in 10 large enterprises (60%) do not.

Regardless of their size or sector, there is strong agreement (88%) among organizations that are inclined to reduce their reliance on these policies that they will need to compensate by investing more in their own cybersecurity defenses.

## Underfunding remains an issue

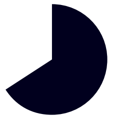
Unfortunately, rising cyber awareness has not yet resulted in cybersecurity budgets that can keep pace with today's rising threat level. While SOES respondents agree cybersecurity is getting more respect than previously, this doesn't always translate into dollars.

More precisely, two-thirds (66%) of the 2023 respondents said their organization's cybersecurity budget is less than it should be — roughly unchanged from the year before.

However, according to this year's group, the underfunding is relatively modest — slightly less than 8% on average. When viewed in terms of the cybersecurity systems that companies have deployed, the picture becomes more promising. Virtually all SOES participants (98%) have already deployed, are in the process of deploying or are actively planning to deploy systems to monitor and protect against email-borne attacks.

The size of most companies' cybersecurity teams appears to be on the rise as well. For instance, at organizations with 250 to 500 employees, nearly half (48%) have between six and 10 dedicated cybersecurity employees, while one-third (34%) have between 11 and 30 full-time cybersecurity professionals. And all of these companies have at least one employee assigned full time to cybersecurity duties.

At the other end of the spectrum, more than half of large enterprises with over 10,000 employees (53%) have more than 30 employees on their cybersecurity teams.



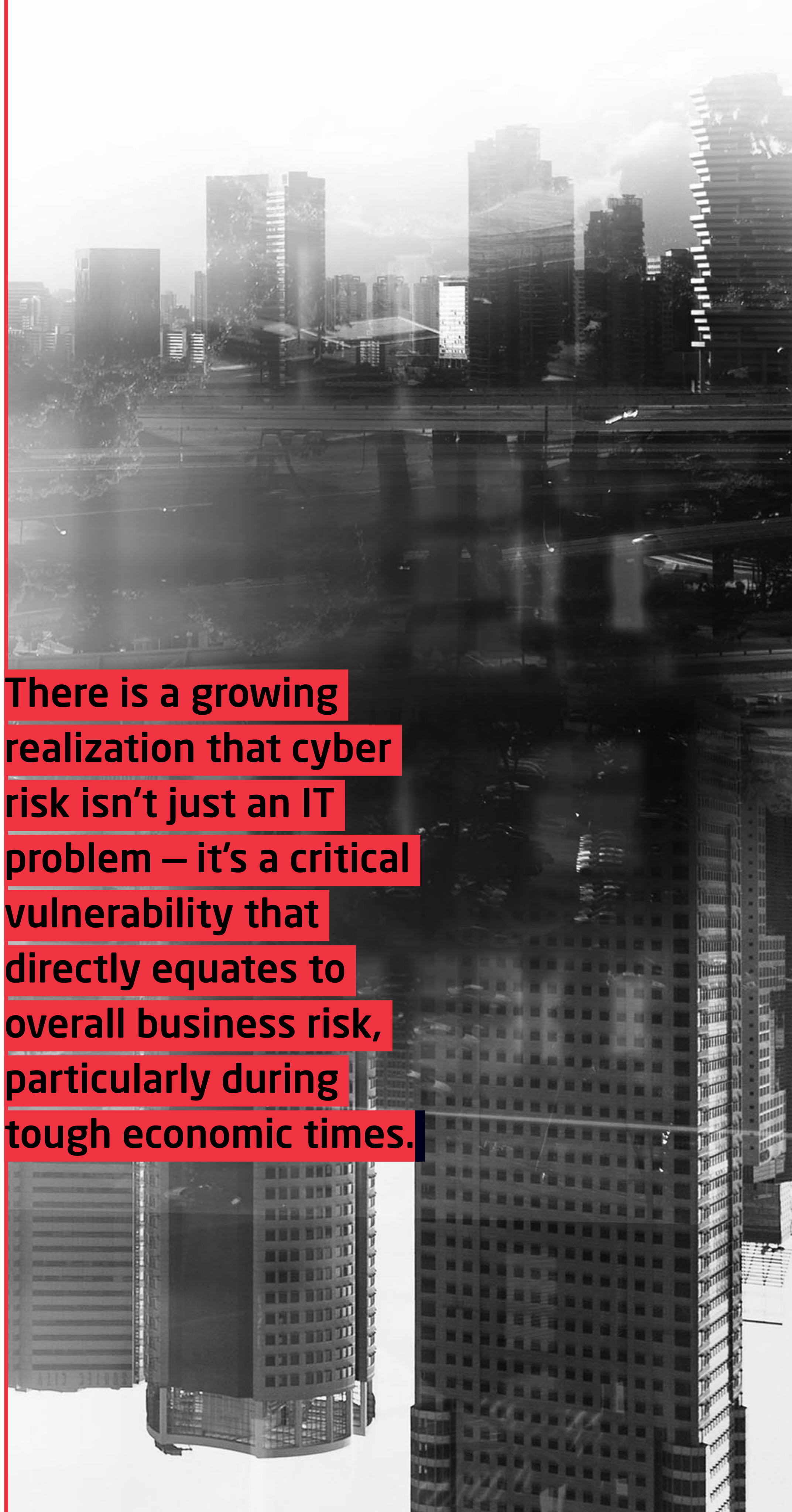
**66% say their company's cybersecurity budget is less than it should be**

# Growing Cybersecurity AWARENESS in the Boardroom

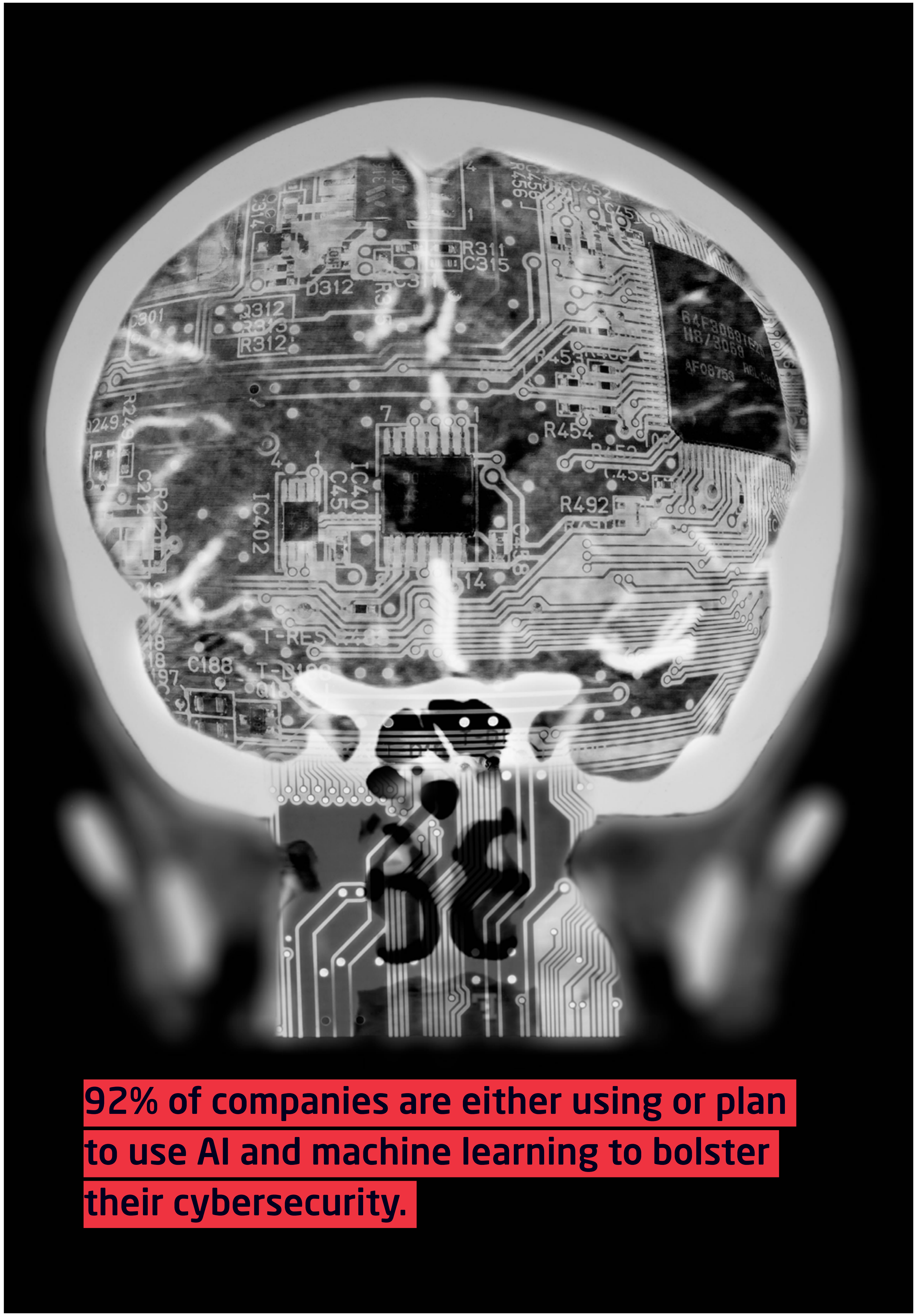
For years, CISOs and their fellow cybersecurity professionals have fought an often lonely battle to forge cyber resilience strategies that could identify and adapt to new threats. But they were often stymied by a lack of awareness in the upper echelons of their companies and a reluctance to spend more on what many executives regarded as costly insurance against a threat that might never materialize.

The COVID cybercrime surge, together with the modern work surface and a more fraught risk landscape in general, has prompted many boards to reconsider that stance. There is a growing realization that cyber risk isn't just an IT problem — it's a critical vulnerability that directly equates to overall business risk, particularly during tough economic times. Fundamental business decisions — such as mergers and acquisitions, third-party vendor contracts, right-sizing and supply chain partnerships — are now being shaped around levels of cyber risk.

CISOs typically struggle to secure the resources they need to put a more robust cyber resilience strategy in place. Now, however, with their boards regularly discussing the risks posed by the rise in breaches and cyber fraud, there is a growing sense that requests for more funding will get a warmer reception.



> There is a growing realization that cyber risk isn't just an IT problem – it's a critical vulnerability that directly equates to overall business risk, particularly during tough economic times.



92% of companies are either using or plan to use AI and machine learning to bolster their cybersecurity.

# Reducing Cyber Risk with Next-Gen Technology

**49% improved ability to block threats**

**48% faster remediation when an attack has occurred**

**50% more accurate threat protection**

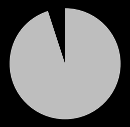
Underbudgeting may still be a fact of life for most CISOs, but as cyberattacks continue to mount both in number and complexity, artificial intelligence (AI) and machine learning (ML) are helping under-resourced cybersecurity teams stay ahead of the curve.

Nearly half of the companies interviewed (49%) are already using some combination of these technologies (compared to 46% last year and 38% the year before), and most of the rest (43% of the total) are planning to do so.

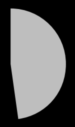
Among the organizations currently making use of AI/ML, more accurate threat detection (50%), an improved ability to block threats (49%) and faster remediation when an attack has occurred (48%) are viewed as the three biggest benefits.

Most SOES participants (81%) agree that AI systems that provide real-time, contextual warnings to email and collaboration tool users would be a huge boon. Twelve percent went so far as to say that the benefits of such a system would revolutionize the ways in which cybersecurity is practiced.

5



**Over 95% of all data breaches are due to human error**



**Close to half (48%) said that insufficient employee awareness of cyber threats would be their organization's biggest security challenge in 2023.**

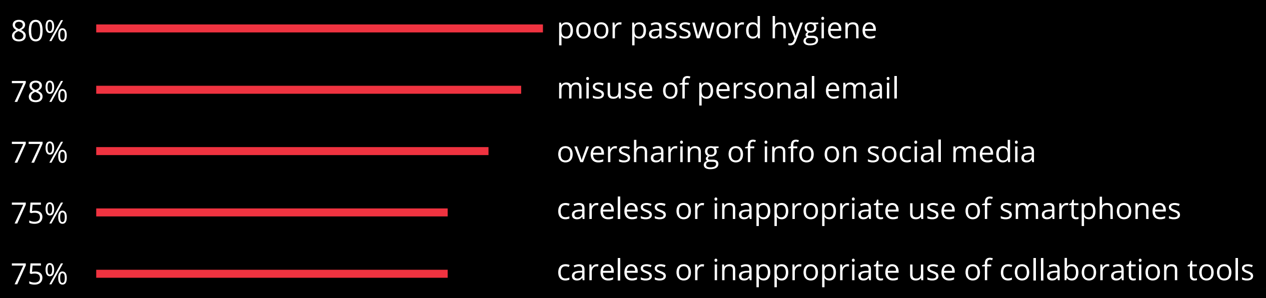
# Reducing Cyber Risk through Cyber Awareness

Here's a startling fact: Over 95% of all data breaches are due to human error.[12] And another: By some estimates, 97% of users can't recognize even a crude phishing email when they receive one.[13] This state of affairs leads to an obvious conclusion: The single most important step that any organization can take to improve its cybersecurity is to foster a culture of cyber awareness.

At every company, regardless of size, a basic understanding of the risks and most common types of attacks needs to become common knowledge. Employees at all levels must recognize that cybersecurity isn't just an IT issue, but something that affects them personally and for which they are directly responsible.

All of this is clearly supported by the SOES data, which shows that attacks that quickly spread from one infected employee to others are close to all-time highs. Eight out of 10 (80%) of the companies surveyed experienced attacks of this sort, the highest level in all but one of the seven SOES surveys — with the exception being last year, when 82% of companies reported falling prey to these attacks.

When asked what mistakes employees make that contribute to the spread?



# Fostering cyber ALERTNESS

The antidote to insufficient employee awareness is cyber awareness training that educates employees to the dangers and teaches them to recognize and safely manage the threats to which they are routinely exposed. Recognizing this, many C-suite executives and company boards are now advocating for greater cyber alertness, and virtually all of this year's SOES participants (99%) provide some sort of awareness training for their workforce.

The most effective training is on-going, engaging and based on educational best practices, and here too this seems to be increasingly reflective of the types of training that the SOES participants provide. For example, more than half (55%) conduct group training sessions with the IT or cybersecurity team, and 41% offer one-on-one training sessions as well.

Another highly effective form of training — interactive videos — is provided by close to half (44%) of the participants, and is even more popular among the largest companies with more than 10,000 employees (58%). There are exceptions though. In what appears to be a case of the shoemaker's children, fewer than a third (32%) of media and entertainment companies make use of training videos — the least of all sectors.

In terms of frequency, only a minority of companies (18%) provide ongoing training, but more than one-third (36%) provide it every month and close to as many (31%) provide it each quarter. So, all told, 85% of the SOES participants are providing awareness training to their workforce at least once a quarter. The trend line here is positive as well: Again with the exception of last year, when it was even higher (87% providing training at least once a quarter), the frequency of the training provided by the SOES participants has risen steadily over the past seven years.

What are the most important learnings from this year's SOES results?

# Top Ten Takeaways

## 1

### There's no risk quite like cyber risk.

The world stands to lose $8 trillion this year due to cybercrime. It takes more than nine months on average to discover and contain a data breach. Companies fear cyberattacks more than inflation and climate change. Is it any wonder that many CISOs feel as though they have a tiger by the tail?

## 2

### To tame the cyber threat, secure your email.

There's a good reason why email is the no. 1 attack vector for the cybercriminal set: Because that's where there are the most digital doors and windows for them to climb through. To wit, 82% of companies report higher volumes of email; 74% are seeing more email-based threats, and three-out-of-four (76%) are expecting to face serious consequences from an email-based attack.

## 3

### Collaboration tools are awesome, essential to modern work... and risky.

The use of collaboration tools has exploded, and that makes them another attractive target for the criminal set. More than a third of SOES respondents (38%) say that the number of attacks due to collaboration tools is on the rise; nearly three-quarters (72%) think their organization will be damaged by a collaboration-tool-based attack, and three out of four (75%) believe that the new threats posed by collaboration tools urgently need to be addressed.

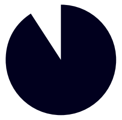
## 4

### To avoid getting phished, do a better job of training your users.

Phishing attacks rely on false pretenses and social engineering to deceive employees. But ongoing and engaging awareness training can teach them to spot and avoid these and other ploys. You can never provide too much cyber awareness training.

## 5

### Spoofing's a problem; DMARC's the answer.



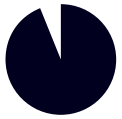
Nearly every company is getting spoofed (91%), and many are seeing an increase in this type of fraud (44%).

What they are not doing is taking advantage of DMARC, a robust and cost-effective protocol for ferreting out bogus emails. Protecting a brand is hard, and repairing a brand that's been damaged is even harder. This makes a proven solution like DMARC a no-brainer.

# 6

## Microsoft 365 and Google Workspace provide good security. Businesses need great security.

The layer of security provided by MS 365 and Google Workspace is too thin— at least according to 94% of SOES respondents.



In a world where nearly half of malicious email attachments are MS 365 files,[14] addition layers of protection are needed.

# 7

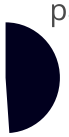
## An insurance policy can’t replace your own cyber preparedness plan.

It may make financial sense to insure against cyber risk, but even the best cyber insurance can only compensate for damage that’s already been done; it can’t prevent the damage from occurring in the first place. Only your own cyber preparedness plan can do that.

# 8

## Cybercriminals are using AI. So should you.

Nearly half of SOES participants (49%) are already using some type of AI/ML to improve their defenses.



They report a long list of benefits, including more accurate threat detection (50%), better threat blocking (49%) and faster attack remediation (48%). The writing is on the wall: With cybercriminals using AI to boost ransomware, email phishing scams and other attacks, cybersecurity leaders must to fight AI with AI.

# 9

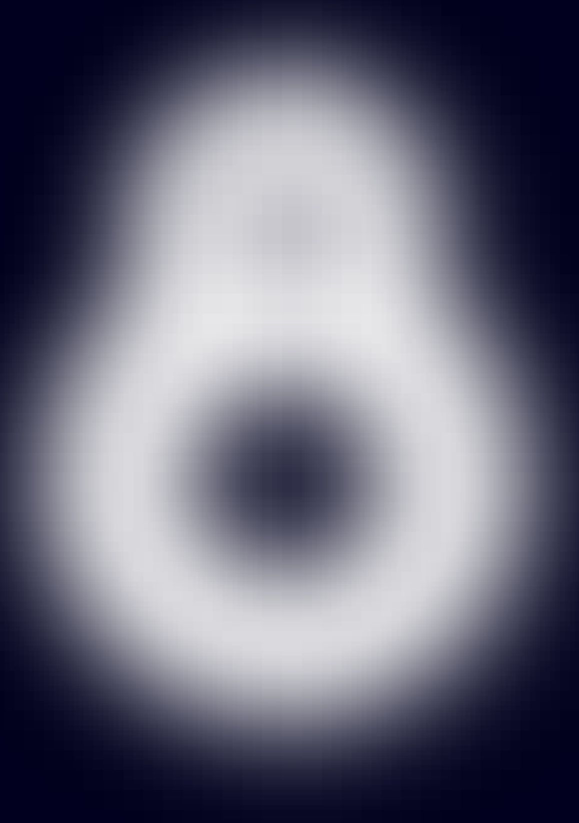
## It’s great to have the board’s attention. That doesn’t mean they will give you a bigger budget.

Corporate boards are finally paying attention to cybersecurity, but they still have many other priorities, such as a likely recession. So, more attention doesn’t automatically translate into more money for cyber defenses. Even so, shortfalls have fallen into the single digits, and requests for bigger budgets are given a serious hearing.

# 10

## Things are looking up. Did we mention you have the board’s attention now?

For years, CISOs fought to get their boards to take cybersecurity more seriously. Well, now they’ve succeeded, and the ball is in their court. Sure, there are risks involved. More attention means more scrutiny — but the opportunity to highlight cyber risk as business risk has never been greater. You have the access, now use it to make the case for greater cyber resiliency.



Around the globe, businesses are battening down the hatches against a cyber storm amidst a recession. There are limitations to their efforts, but more importantly their boards and top executives have begun to acknowledge the risk. This is pivotal, because once cyber preparedness becomes a business priority, it is only a matter of time before companies work out the ways and means to implement it.

**This year’s SOES report highlights their efforts. But the real takeaway is that by prioritizing the cyber threat, companies the world over have begun to contain it – even if eliminating it entirely remains a distant aspiration.**

# The Bottom line

SURVEY

**About the Survey Results Included in this Report**

This is the seventh consecutive year in which Mimecast has conducted an in-depth global survey on the current state of email security. For our 2023 report, we commissioned research firm Vanson Bourne to interview 1,700 information technology and cybersecurity professionals — the largest sampling since the study was initiated in 2016. The survey took place in October and November 2022, with respondents drawn from 13 countries: the U.S., Canada, the United Kingdom, France, Germany, the Netherlands, Sweden, Denmark, Saudi Arabia, the United Arab Emirates, South Africa, Singapore and Australia.

Survey participants worked at organizations ranging between 250 to 500 employees (15%) and more than 10,000 employees (9%). These companies were spread across 12 industrial sectors, including financial services (14%), technology and telecommunications (13%), retail (13%), healthcare (11%), manufacturing (9%) and the public sector (7%).

Among the participants, CIOs, CTOs, CISOs, IT Directors and IT Security Directors comprised 62% of the total. The remainder included IT and SOC managers, as well as security architects and analysts.

CCS MEDIA

**To find out more,**
**speak to your Account Manager**

**call:** 01246 200 200

**email:** letstalk@ccsmedia.com

**visit our website at** ccsmedia.com

mimecast®

Advanced Email & Collaboration Security

1. "The future of risk," Deloitte
2. "The 10 Biggest Risks and Threats for Businesses in 2022," Forbes
3. "The 3 Most Important Global Corporate Risks in 2022: Part I," Censinet
4. "Cybersecurity Breaches to Result in Over 146 Billion Records Being Stolen by 2023," Juniper Research
5. "Cybercrime to Cost the World 8 Trillion Annually in 2023," Cybercrime Magazine
6. "Cost of a data breach 2022," IBM
7. "Data Breach Investigations Report 2022," Verizon
8. "Blumira's 2022 State of Detection and Response," Blumira
9. "The State of Phishing 2022," SlashNext
10. "Phishing Statistics & How to Avoid Taking the Bait," DataProt
11. Ibid
12. "Top 21 Cybersecurity Stats You Should Know about in 2023," Simplilearn
13. "8 Cybersecurity trends to be aware of in 2022/2023," AT&T Business
14. "2019 Data Breach Investigations Report," Verizon