mimecast

Human Risk & AI

FRAMING THE FUTURE

The State of Email & Collaboration Security Report 2024

Part 1:

Growing Cyber Preparedness.

The world was a fraught, risk-filled place in 2023, and cybersecurity threats continued to intensify. How could they not? With state actors menacing any number of countries and widespread economic and political dislocations unleashing torrents of criminal activity, it was inevitable that cybercrime would rise as well.

Most notably, per the Mimecast's State of Email and Collaboration Security (SOECS) 2024 Report findings, 9 out of 10 companies now have a formal cybersecurity strategy in place. This includes the 48% of respondents who have a formal cybersecurity strategy that spans all key business functions, as well as 43% who have a formal strategy but make it the sole responsibility of their IT department.

Yet another 3% are currently implementing a formal strategy and 6% have adopted cybersecurity guidelines and best practices, although no formal strategy.

100%

are now strongly engaged in cyber preparedness.

This degree of preparation extends across all industry sectors and companies of all sizes.

The financial services sector, for instance, has the highest percentage of SOECS 2024 participants with a formal cybersecurity strategy that spans the entire business (60%). This compares with just 33% for the media and entertainment sector — the lowest among the industries included in the survey. Even so, all the companies surveyed within both sectors have incorporated either a formal cybersecurity strategy or a set of best practices.

Consistent preparation across the corporate spectrum

Likewise, among companies of different sizes, the difference in preparedness is small. The largest companies, with more than 10,000 employees, led the way with 60% having adopted a formal strategy across the business. This is compared with only 43% of companies in the 500 to 1,000 employee range. But the smaller companies made up for this with higher percentages of participants that have either taken up an IT-led strategy or best practices instead.

To be sure, none of this says that corporate cyber preparedness is fully mature or as robust as it should be. As the rest of this SOECS 2024 report explains, there are still significant and dangerous gaps in many businesses' defensive measures. Many cybersecurity professionals remain frustrated over insufficient funding, lack of organizational support and pressure from upper management to confine spending on security tools to those provided by Microsoft 365. Many human risk factors in particular — which represent today's biggest cybersecurity gap — remain unaddressed and outside of cybersecurity professionals' control.

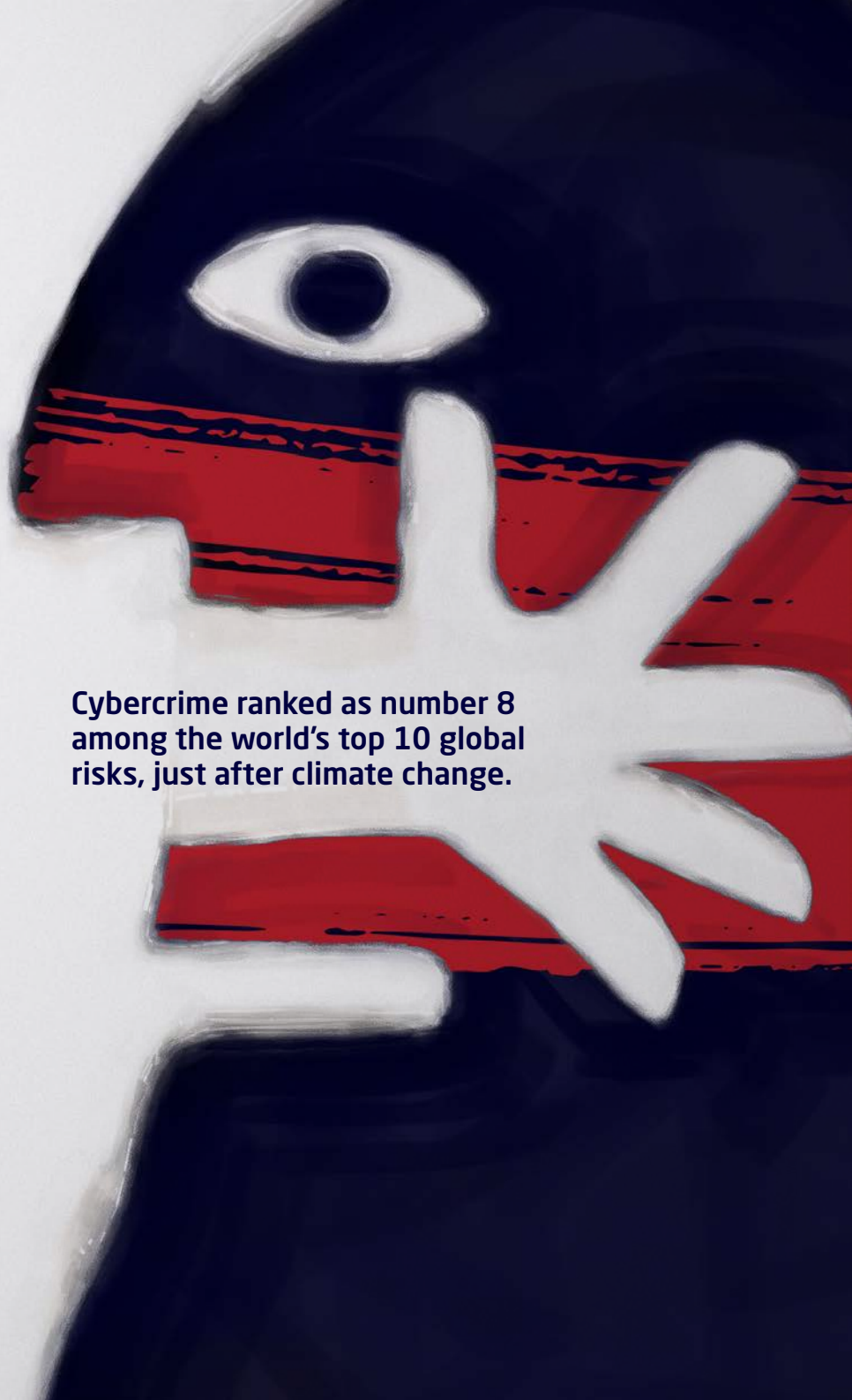
But despite these limitations, there is reason for considerable optimism as company after company takes steps to integrate cybersecurity into its day-to-day operations.

Part 2:

Cyber Risk at the Intersection of People, Communication and Data.

The World Economic Forum (WEF) now ranks cybercrime no.8 among the world's top 10 global risks, just after climate change and ahead of large-scale human migration. As stated by the WEF, "a global risk is defined as the possibility of the occurrence of an event or condition which, if it occurs, would negatively impact a significant proportion of global GDP, population or natural resources."[1]

In today's digital, networked economy, every company faces this cyber threat. The operations, reputation and revenue of every business, large or small, are at risk of a data breach or system incursion — and this has become widely recognized. According to a Deloitte Center for Controllership poll, "nearly half (48.8%) of C-suite and other executives expect the number and size of cyber events targeting their organizations' accounting and financial data to increase in the year ahead."[2]



Cybercrime ranked as number 8 among the world's top 10 global risks, just after climate change.

email

remains

the number 1

attack vector

for cybercriminals

The magnitude of the cyber threat is appalling:

+15%

Cybercrime is expected to grow by 15% per year over the next two years, from $8 trillion globally in 2023 to $10.5 trillion by 2025.[3] This is up from $3 trillion in 2015 and represents the greatest transfer of wealth in human history.[4]

1 BILLION

Nearly one billion emails were exposed in 2023, affecting one in five internet users.[5]

$4.45 MILLION

Worldwide, the average cost of a data breach is now $4.45 million, up 15% over three years. For U.S. companies, the average is more than twice that at $9.48 million per breach.[6] Globally, in 2023, the number of stolen electronic records was just shy of six billion.[7]

Email remains the number one attack vector for cybercriminals[8], and phishing attacks remain the top threat to email users.[9]

This is confirmed by the SOECS 2024 survey, which found that the volume of email-based phishing, spoofing and ransomware attacks continues to increase.

PHISHING ATTACKS

remains the top threat to email users.

Phishing

In 2023, business email compromise (BEC), a particularly dangerous form of phishing, nearly doubled. Phishing, together with stolen credentials and the exploitation of network vulnerabilities, remain the three primary ways in which companies are hacked.[10]

This affects some types of businesses much more than others. While 39% of SOECS 2024 respondents reported a rise in phishing activity, the percentage was higher for 6 of the 12 industries represented in the survey. This included more than half (54%) of organizations in the public sector and nearly half (49%) in the business and professional services sector, which includes law and accounting firms, among others.

Overall, 41% of the SOECS 2024 participants experienced more email-based threats in the past 12 months, and 38% see the growing sophistication of these attacks as their biggest email security challenge.

Spoofing

Email spoofing, where an imposter tries to make it seem as though an email comes from a trusted source, also continues to spread, with more than a third (35%) of the SOECS 2024 respondents noting that the number of these attacks grew again in the past year. But as with phishing, some industries were hit much harder than others: The business and professional services sector had the dubious distinction of having the most respondents (52%) reporting a jump in these types of attacks.

Likewise, web spoofing, where the perpetrator attempts to defraud companies and their customers by creating a website that impersonates the company's site, continues to run rampant. Nearly all (98%) of SOECS 2024 participants discovered a counterfeit web domain in the past year, with more than 60% unearthing this type of fraud on multiple occasions.

Ransomware

By far though, the type of email-delivered threat that is spreading the fastest — and at greatest cost to its victims — is ransomware.

In 2023, ransomware attacks increased 95% year-over-year.[11] At the same time, the average ransom payment soared from $212,000 in 2022 to $740,000 in 2023 — an increase of 250%.[12]

Eight out of 10 SOECS 2024 respondents have fallen victim to ransomware in the past year, and 3 out of 4 of the victims felt compelled to pay the ransom. And while two-thirds of these ransom payers successfully recovered their data, the remaining third did not.

Significantly though, among the ransomware victims, 23% did not pay the ransom, yet still managed to retrieve their data.

Key Findings.

employees

3 OF 4
respondents say their company is at risk of inadvertent data leaks by careless or negligent employees...

Yet only

15%
of companies provide cyber awareness training to their employees on an ongoing basis

collaboration

70%
respondents say collaboration tools pose urgent new threats

7 OF 10
anticipate fallout from a collaboration tool-based attack

strategy

9 OF 10
respondents now have a formal cybersecurity strategy

96%
of them credit it with reducing their organization's cybersecurity risk

37%
say M365 fails to block malware without the use of additional security tools

75%
companies use or are in the process of rolling out DMARC to ward off spoofing attacks

email

4 OF 10
continue to see a rise in email-based threats

AI

80%
respondents are concerned about new threats posed by AI

support

97%
of respondents say their boards and senior managers support their cybersecurity efforts

ransom

8 OF 10
have been the victims of ransomware

3 OF 4
paid the ransom

67%
respondents no longer view cyber insurance as a comprehensive safety net

80%

are concerned about the use of AI to carry out attacks against their organizations.

67%

of organzations say that AI-spawned attacks will become inevitable over the next few months.

86%

believe they will be able to respond to an AI-spawned attack.

AI-based threats

One key reason for the accelerated spread of phishing and ransomware is the emergence of generative AI, which is making it easier for malefactors to perpetrate successful attacks. A tool like ChatGPT, for instance, can be used to generate emails to individual employees that appear to come from their boss and reference company events or personal information.

This has 8 out of 10 SOECS 2024 respondents concerned about the use of AI to carry out attacks against their organization, with nearly 7 out of 10 (67%) conceding that AI-spawned attacks will become inevitable over the next few months. Counterintuitively, the large majority (86%) believe they will be able to respond to an AI-spawned attack as readily as any other incursion.

Factors outside of cybersecurity's control

However, there are other issues threatening companies' cyber preparedness and SOECS 2024 repondents are less confident that they will be able to manage

Human risk

Factors outside of companies' control and often related to human risk include employees' ability to recognize and respond to cyberthreats (cited by 36% of respondents), and whether security protocols for remote workers are strictly enforced (also cited by 36% of respondents).

Collaboration tools

One critical concern, highlighted by 69% of the respondents, is the broad array of collaboration tools that are used by their companies. These tools and their widespread use have become a major bone of contention for those responsible for their organization's cybersecurity.

Part 3:

Collaboration and the Expanding Attack Surface.

While email remains their primary route of attack, bad actors are also taking advantage of how collaboration tools expand an organization's attack surface.

Few contemporary businesses can function without collaboration tools, which integrate communications and messaging with project management functions. Designed to provide a central platform for sharing data and documents, collaborative software has become the sine qua non of today's remote and hybrid work environments.

These tools, which include virtual communication platforms such as Zoom and teamwork-enabling apps like Google Workspace, Slack and Microsoft Teams, continue to soar in popularity. Among SOECS 2024 respondents, 84% have seen such tools continue to proliferate during the past 12 months, and an even higher percentage (90%) agree that they have become essential to their organization and its day-to-day operations.

Inadequate safeguards

But these IT and cybersecurity professionals are also extremely concerned that the rapid spread and growing reliance on collaborative software makes it an increasingly attractive target for the criminal set. Seven out of 10 (70%) say they pose urgent new threats, while a nearly identical number (69%) think it is likely, extremely likely or even inevitable that their company will be harmed by a collaboration tool-based attack.

The respondents point to a number of factors that are inflaming the situation:

59%

of employees routinely download and make use of new collaboration tools that have not been vetted by the IT department.

61%

say that most of the native security provided by these tools is inadequate.

69%

of respondents say they are overwhelmed trying to keep up with the number of collaboration tools used by their company.

56%

worry that their organizations' cyber defenses cannot keep pace with these new threats.

In response, these cybersecurity professionals are prodding their organization to take more robust defensive measures.

48%

say their companies have already deployed additional layers of protective software to guard against collaboration tool-based attacks.

47%

are taking steps to gain more visibility and control over which tools employees are using and how they are being used.

47%

are providing collaboration tool-specific security awareness training to help employees recognize and respond appropriately to potential threats.

37%

say their companies are only relying on the native security protections included in their collaborative software.

1%

admit they aren't doing anything to prevent a collaboration toll-based attack.

The anxiety over collaboration tools reflects the current yin and yang of corporate cybersecurity. While companies' defensive postures have significantly improved over the past few years, new cyber risks continue to proliferate and significant gaps in cyber preparedness continue to persist.

Part 4:

Protecting Work and Managing Cyber Risk.

Most companies now have a formal cybersecurity strategy in place, and almost all of them (96%) agree that it has reduced their cyber risk. Viewed through the lens of people, process and technology, taking a more strategic approach has been a rousing success.

People:

99%

Virtually all the SOECS 2024 respondents (99%) say their company's cybersecurity practices are effectively protecting the organization's customers, employees and business partners.

Process:

99%

The respondents are nearly unanimous (99%) that their cybersecurity measures are safeguarding their organizations' business and operational processes.

Technology:

100%

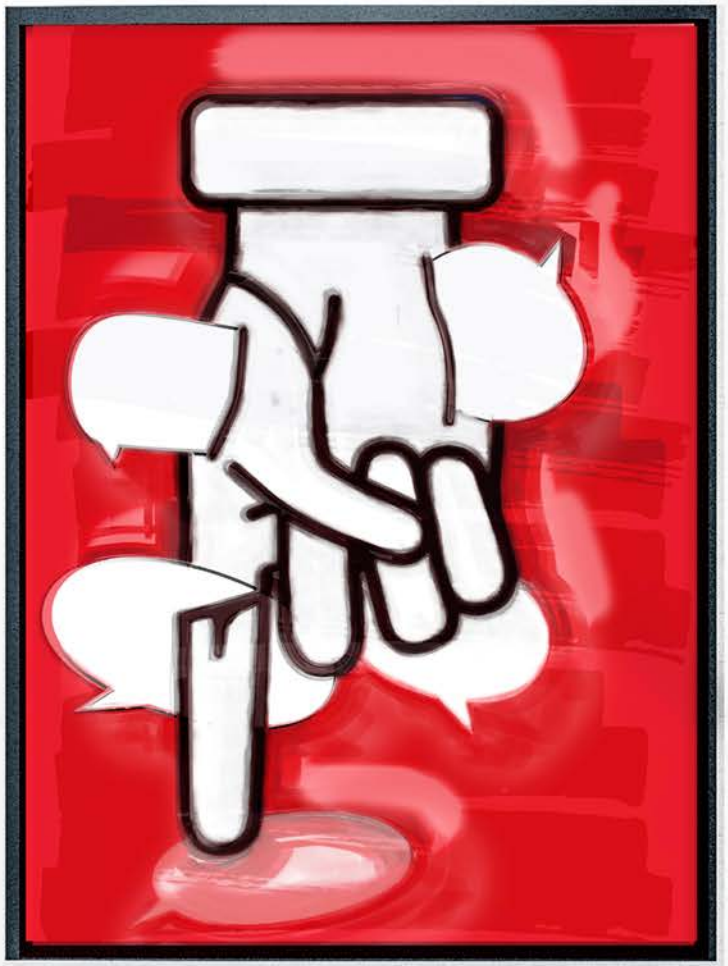
And 100% unanimously agree that those same policies are working to secure their email, collaboration tools and other technology-based assets.

Although welcome, these outcomes also beg the question that if the cybersecurity strategies at these organizations are proving so successful, then why were there over 500 million phishing attacks reported in the U.S. alone in 2022?[13] And why did businesses worldwide shell out $449 million to ransom their data during the first half of 2023?[14]

The answer, of course, is that while adopting a comprehensive set of security measures has mitigated cyber risk at many companies, it has not come close to eliminating it. When asked to qualify the degree of protection afforded by their organizations' cybersecurity practices, only 7% of respondents claimed they provided complete protection, while 92% allowed that the protection was incomplete.

500 M

phishing attacks reported in U.S. alone in 2022.



More resources needed

A lack of resources is part of the problem. In a positive development, most respondents (97%) say their boards and senior managers support their cybersecurity efforts, and the majority (57%) characterize the level of that support as high. Yet at the same time, many respondents feel their efforts are undercut by inadequate budgets and limitations on how those monies can be spent.

The respondents report that, on average, 9% of their organization's IT budget is allocated to cybersecurity. This is much lower for certain industries, such as the energy sector, which only earmarks 3% of IT spending for security. The respondents, on the other hand, believe the 9% average is a third less than it should be. They would like to see an average of 12% of their corporate IT budgets designated for cyber preparedness.

Among the consequences of this underspending:

40%

respondents say they have had to compromise on which cybersecurity tools they use to monitor email and collaboration tool-based threats.

37%

say they are unable to detect and respond to threats as quickly and efficiently as needed.

36%

say the underspending has led to significant holes in their organizations' defenses.

Forced to rely on Microsoft 365

These spending constraints are having another serious impact. To contain spending, more than a third of the respondents (35%) say they have been blocked from investing in cybersecurity solutions apart from those provided by M365. The protections provided by the Microsoft software suite, however, have significant limitations, and this has undermined their cyber preparedness.

The respondents point to a variety of shortcomings in M365's security measures. Chief among them:

32%

Limited ability to see beyond specific incidents (the trees) and view the full threat picture (the forest).

30%

Failing to prevent "too many attacks from reaching the user's inbox" .

30%

Making it too difficult to implement a zero-trust policy.

Most significantly, on their own, without the use of additional, non-native security tools, a third of the respondents said M365's native security protections were unable to prevent malware (37%), spam (33%) or phishing (33%) attacks. Almost as many (32%), said that by themselves the M365 security apps could not block BEC and spoofing attacks against their company.

Line of DMARCation

To prevent phishers and other fraudsters from spoofing their email domains, companies are making DMARC part of their cybersecurity strategy.

Domain Message Authentication Reporting and Conformance is a protocol that helps determine whether an email was sent from the domain with which it is associated. This makes it much easier to identify and block emails that purport to come from one party but were sent by another. Implementing DMARC, however, can be painstaking and time consuming, which is why some businesses have been slow to adopt it.

But that was then. Now, companies across the board appear to have decided that the greater protection it affords is worth the effort. To wit, 94% of this year's SOECS participants are either already using DMARC, in the process of deploying it, or planning to do so over the next 12 months — the highest percentage since Mimecast first launched the survey in 2016.

The top reasons given for implementing DMARC:

56%

making email more trustworthy.

54%

ensuring compliance with industry regulations.

48%

protecting the company's brand.

94%

of participants are either already using DMARC, in the process of deploying it, or planning to do so over the next 12 months.

The top difficulties cited are:

46%

time it takes to manage and maintain the protocol.

45%

extent to which it can interfere with business operations.

39%

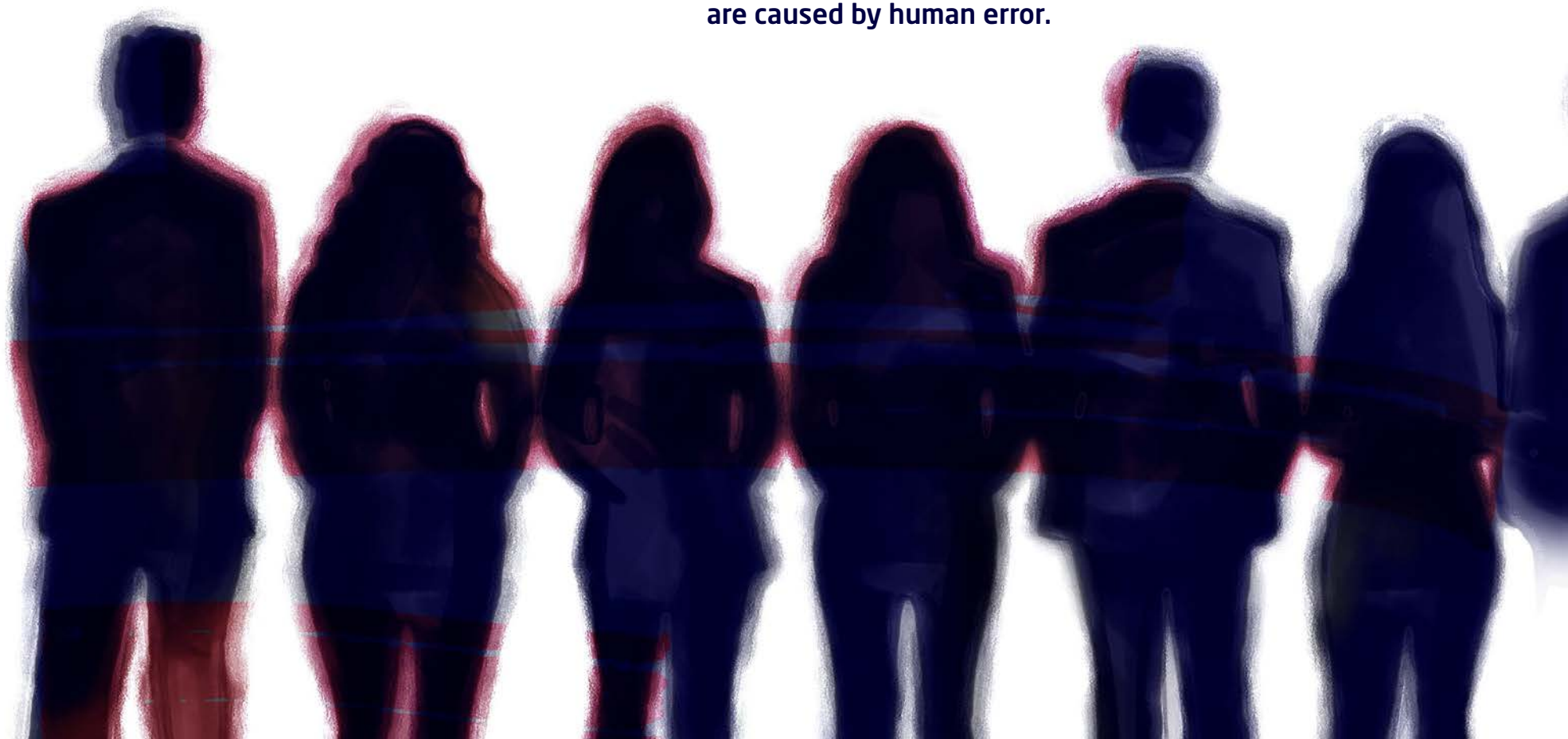
resistance to using it on the part of the organization's stakeholders.

Human risk is today's biggest cybersecurity gap, and this comes through strongly in the SOECS 2024 report: More than two-thirds of respondents believe that employees are putting the organization at risk through the misuse of email, oversharing company information on social media and careless web browsing.

The concern is even greater for certain sectors, such as the public sector, where almost 9 out of 10 respondents (87%) worry that employee email and social media lapses will damage their institution.

74%

of cybersecurity breaches are caused by human error.



Despite these fears, only slightly more than half of respondents say their organization provides monthly or ongoing cybersecurity awareness training, and this is down slightly from 2023 (52% versus 54%).

Professional educators have long held that to be effective, security awareness training must be consistent, delivered regularly in small doses and tailored to fit individual employees. But beyond this, to close the gap and significantly reduce the risk factors represented by their workforce, there is growing acknowledgement that companies need to move beyond one-size-fits-all training that checks the compliance box, but does little to reduce employee risk.

More effective types of adaptive training are emerging, based on the recognition that 8% of a company's users are responsible for 80% of its security incidents.[16] These training programs begin by determining the risk level represented by different employees, and then concentrating on those employees with the riskiest behavior to provide individualized training to correct those behaviors.

The SOECS 2024 respondents are not there yet. But their keen awareness of human risk and how it translates into cyber risk suggests that, going forward, they will increasingly push for their organizations to embrace adaptive training methods.

54%

say their organization provides monthly or ongoing cybersecurity awareness training.

Part 5:

Cyber Insurance versus Cyber Preparedness.

As they have stepped up their cyber preparedness efforts, businesses have become less dependent on their cyber insurance policies.

By no means are companies dropping their insurance: 95% of SOECS 2024 participants have at least one policy and 45% have more than one. They are becoming much less likely to treat these policies as a subsitute for a culture of cyber resilience.

2/3

Cyber insurance is no longer viewed as a comprehensive safety net.

For example, when asked whether their organization views cyber insurance as a comprehensive safety net for coping with cyber threats, just under two-thirds of the respondents (65%) emphatically stated they did not. That is compared to only 50% who held that view last year.

Likewise, when asked if their organization is less likely to rely on cyber insurance due to the restrictions insurers are placing on these policies, two-thirds (66%) agreed, compared to 52% in 2023.

Because of this reduced reliance, nearly 9 out of 10 respondents (86%) said they thought their organization needs to compensate by investing more in its own cyber defenses. When asked where this investment was most likely to occur, the top three categories singled out by respondents were greater email security (45%), greater collaboration tool security (44%) and more use of AI for cybersecurity applications (41%).

While cyber insurance coverage still matters, companies of all sizes and sectors recognize that their own cyber resiliency matters more.

Part 6:

Top Takeaways

.01 Most cyber risk is due to human risk

No matter what processes and technologies are employed, strong cybersecurity depends primarily on the behavior of people. But human risk represents a huge security gap at most organizations. Companies need to embrace more adaptive forms of cyber awareness training. This allow them to identify which employees are engaged in the riskiest behaviors and provide individualized training to address those behaviors.

.02 The threat is in the email

Email remains the primary attack vector for the biggest cyber threats that most companies are facing — phishing, spoofing and ransomware. In other words, there is no cybersecurity without strong email security. Robust email security depends on multilayered protections that can cope with ever-more sophisticated attacks.

.03 Phishing catches people

Phishing attacks are ubiquitous and multiplying rapidly. But phishing only works if people fall for it. The right email protections are an important aid in mitigating the threat. Primarily, employees need to be alert to the danger and trained to avoid it.

.04 Collaboration is a double-edged sword

Email may be their main route of attack, but the burgeoning number of collaboration tools pose new and dangerous openings for cyber criminals. While few companies can operate in today's global work environment without relying on these tools, they urgently need to consider the new threats they pose.

.05 DMARC defeats spoofing

DMARC is not the easiest protocol to administer, but it is highly effective against email spoofing, which continues to proliferate. The minority of companies that have yet to embrace DMARC are leaving a gap in their cyber preparedness. Getting spoofed repeatedly because they fail to implement DMARC can be a costly reminder.

.06

Microsoft 365 consolidation is penny-wise and pound-foolish

Trying to save a few bucks by restricting cybersecurity spending to those tools included in M365 is a self-defeating proposition. Microsoft's safeguards are simply not effective enough on their own; they need to be complemented with other security tools to achieve a reasonable degree of cyber preparedness.

.07

The AI threat is coming! The AI threat is coming!

The SOECS 2024 respondents already consider the increasing sophistication of today's email-based attacks as their primary cybersecurity challenge. But soon the widely expected proliferation of AI-generated threats will amplify the danger. Businesses across-the-board need to fight fire with fire by stepping up their investment in AI-driven threat detection and prevention tools.

.08

Cyber preparedness reduces cyber risk

Nine out of 10 companies now have a formal cybersecurity strategy in place, and 96% of them agree that it has strengthened their ability to protect their people, processes and technology. This has been recognized by most senior managers and board members, who are actively advocating better cyber preparedness.

.09

Cyber insurance does not equal cyber preparedness

Most companies have recognized this basic truth: A cyber insurance policy is not a substitute for a company's own cyber preparedness plan. While it may make financial sense to insure against cyber risk, even the best cyber insurance can only compensate for damage that has already been done; it cannot prevent the damage from occurring in the first place. Only an organization's own cybersecurity can do that.

.10

There is no spending like cybersecurity spending

Where today's cyber preparedness strategies fall short is in how they are implemented. Too many boards and senior executives actively endorse these efforts and then fail to back them with sufficient resources. But cyber preparedness is like a living thing: To survive and thrive in an ever-more treacherous environment, it needs constant care and feeding.

The Bottom Line

The global storm of cyber threats continues to intensify. Companies of all sizes and from all industries are more alert than ever to the danger of this cyber siege of their employees and are taking significant steps to confront it. Nevertheless, they will need to up their game going forward. New sources of threats and AI-driven attacks are sure to further roil already troubled waters. Fortunately, new security tools and training methods, such as adaptive training, have also arrived to help keep people and their work protected.

About the survey results included in this report.

The State of Email & Collaboration Security 2024 report is based on an in-depth global survey of 1,100 information technology and cybersecurity professionals. Mimecast commissioned UK-based research firm Vanson Bourne to conduct the survey, which took place during October and November 2023. Survey participants were drawn from six countries, including the U.S. (27% of the total), the United Kingdom (18%), France (18%), Germany (9%), South Africa (9%) and Australia (18%).

Survey participants worked at organizations ranging from 250 to 500 employees (9% of the total) to more than 10,000 employees (8% of the total). These companies were spread across 12 industry sectors, including information technology and telecommunications (15%), retail (14%), manufacturing (12%), business and professional services (12%), financial services (11%), healthcare (10%), energy (6%), media and entertainment (5%), the public sector (5%), construction and real estate (3%), consumer services (2%) and other commercial businesses (4%).

Among the participants, CIOs, CTOs, CISOs, IT Directors and IT Security Directors comprised 78% of the total. The remainder included IT and SOC managers, as well as security architects and analysts.

1. "The Global Risks Report 2023," World Economic Forum
2. "A Rise in Cyber Events Targeting Accounting and Financial Data," Deloitte
3. "2023 Cybersecurity Almanac," Cybercrime Magazine
4. "Cybercrime to Cost the World $10.5 Trillion Annually by 2025," Cybercrime Magazine
5. "Cost of a Data Breach Report 2023," IBM
6. "List of Data Breaches and Cyber Attacks in 2023," IT Governance
7. "Global Threat Intelligence Report," Mimecast
8. "2023 Data Breach Investigations Report," Verizon
9. "Email remains the top attack vector for cybercriminals," Cybernews
10. "2023 Data Breach Investigations Report," Verizon
11. "Q3 Ransomware Report," Corvus Insurance
12. "Average amount of cyber ransom payments," Statista
13. "Phishing Statistics by State in 2024," Forbes
14. "Crypto Crime Mid-year Update," Chainalysis
15. "2023 Data Breach Investigations Report," Verizon
16. "8% of Your Users Cause 80% of Your Security Incidents," Elevate Security

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.