

A STRATEGIC IMPERATIVE FOR THE C-SUITE

Seven emerging trends in cyber resilience

The key cybersecurity trends the C-suite must master to achieve true cyber resilience range from AI-powered threat identification and automated mitigation to proven cyber readiness and speedy, comprehensive cyber recovery.

01

BUILDING RESILIENCE
IN 2024

02

01 REGULATORY COMPLIANCE DEMANDS
CYBERSECURITY CHANGE

03

03 SECURITY AND IT TEAMS
MUST CONVERGE

06

04

CYBER READINESS FALLS
ON EVERYONE

05

09 ADOPTING AI FOR GOOD
... AND BAD

14

06

CYBER RESILIENCE REQUIRES
TOOL CONSOLIDATION

18

07

GENERATIVE AI
WASHING COMES CLEAN

22

08

AUTOMATION SPEEDS SECURITY
RESPONSE

25

09

ACHIEVING CYBER RESILIENCE
IN 2024

30

CO

CONCLUSION

33

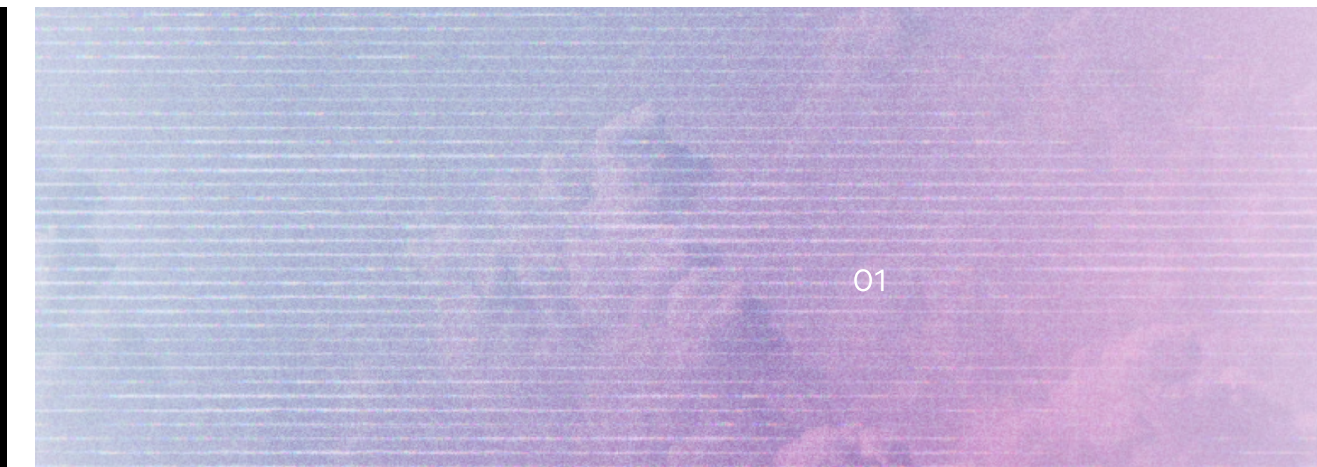
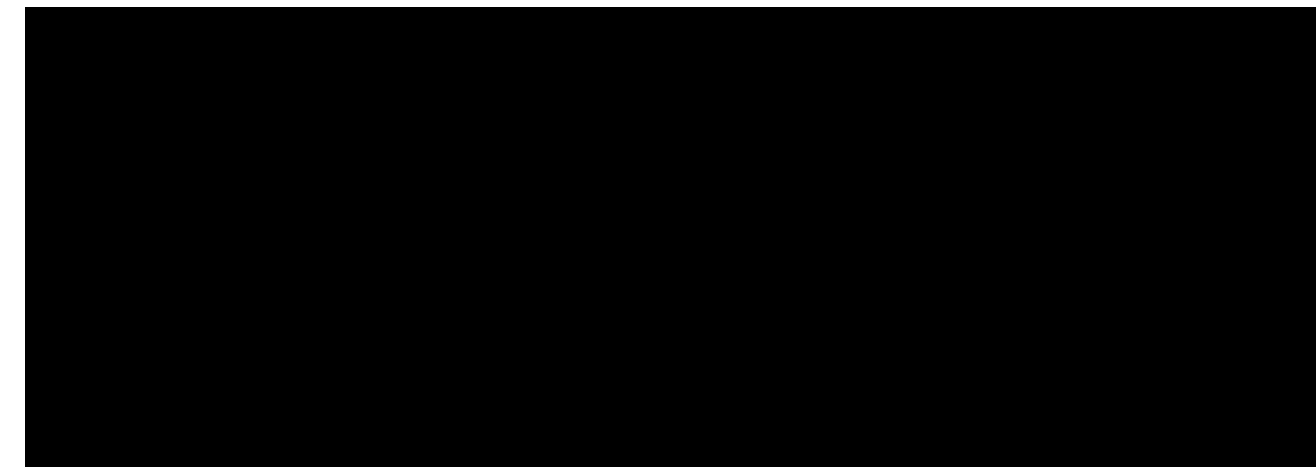
Building resilience in 2024

As digital technologies evolve and enable more innovation, cyber attacks often keep pace—becoming more sophisticated and difficult to prevent—and at times leveraging the same technology advancements to expand the threat landscape and challenge security leaders to stay ahead of the cybersecurity curve.

In 2024, C-level executives will prioritize cyber resilience as a strategic imperative to not only better identify and prevent potential threats, but to also mitigate risk and resolve incidents quickly with minimal impact to the business and its resources. The ultimate goal is a business that can successfully prevent most attacks and recover quickly from those unavoidable incidents using emerging technologies such as generative AI and leveraging savvy approaches to thwart malicious efforts.

This report will provide C-suite leaders—not restricted to the CISO or CSO—the knowledge and critical understanding they need to successfully navigate the complex cybersecurity landscape. By examining key trends such as C-level scrutiny of cyber resilience plans, emphasis on cyber readiness, generative AI adoption, increased automation, and tool consolidation, this report will shine a spotlight on the need for comprehensive cyber preparedness across the organization—and why cyber resilience will become a mandate for every domain across the business.

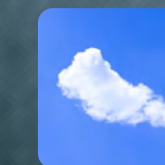
Cyber resilience is a responsibility that encompasses a comprehensive understanding of regulatory requirements, such as the [recent Securities and Exchange Commission \(SEC\) rule](#) that requires registrants to disclose material cybersecurity incidents they experience. This mandate and others like the European Union's Digital Operational Resilience Act (DORA) highlight the growing need for boards to have cybersecurity expertise and knowledge on hand when conducting business. Companies must adopt a culture of transparency to comply with regulations and embrace a holistic approach to cybersecurity that brings IT and security domains closer together, working toward a common goal of cyber resilience.



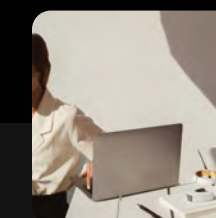
“Cyber attackers never rest and are constantly discovering ways to exploit vulnerabilities. A truly effective cyber resilience strategy must go beyond just backup and recovery. It’s crucial that organizations adopt a new approach that spans prevention, mitigation, and recovery,” said Phil Goodwin, Research Vice President, Infrastructure Systems, Platforms and Technologies Group, IDC in a recent statement. “Whether on-premises, in the cloud, or in a hybrid environment, they must integrate multiple layers of defense. With AI now a tool for both defense and offense, the urgency for comprehensive cyber resilience has never been more evident.”

Here we detail **seven key trends** empowering C-level executives to drive a necessary transformation across businesses that must evolve their approach to cybersecurity into a cyber resilience strategy. With this report, the C-suite can stay ahead of emerging trends, deploy a holistic approach to cybersecurity, protect their organization, maintain stakeholder trust, and position themselves as leaders in the face of an ever-evolving and growing landscape of cyber threats.

Regulatory compliance demands cybersecurity change



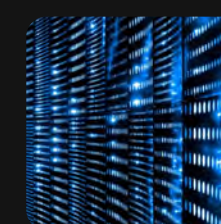
Sort code	97-22-365
Account number	256541



Amount	\$99.67
Sort code	97-22-365
Account number	256541
<input type="button" value="Confirm"/>	

Both business and security leaders understand the need to comply with regulatory requirements that aim to protect customers and investors.

Yet with the SEC's new Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure rule, effective December 2023, CSOs and CISOs could be challenged to accurately report on incidents when board members are on the hook for overseeing compliance. Why such an imperative?



The rule demands security leaders and other C-level executives remain in lockstep when it comes to cybersecurity incidents and the reporting of such incidents. The SEC wants companies to articulate how cybersecurity fits into their overall risk management program. Furthermore, it requires the Board of Directors to oversee and assess the effectiveness of risk reduction activities in an enterprise risk management framework and process.

“They want corporate executives to articulate whether and how cybersecurity is part of the company’s business strategy, governance processes, financial planning, and capital allocation,” said Melissa Hathaway, president of Hathaway Global Strategies and chair of Commvault’s Cyber Resilience Council.

This means in 2024 security leaders must work with other C-level executives and the board to document and operationalize the policies and procedures for the identification and management of cybersecurity risks. Good governance mechanisms delineate the accountability and responsibility for ensuring successful execution, while actionable, repeatable, meaningful, and time-dependent key performance indicators (KPI) should be used to reinforce realistic objectives and timelines.

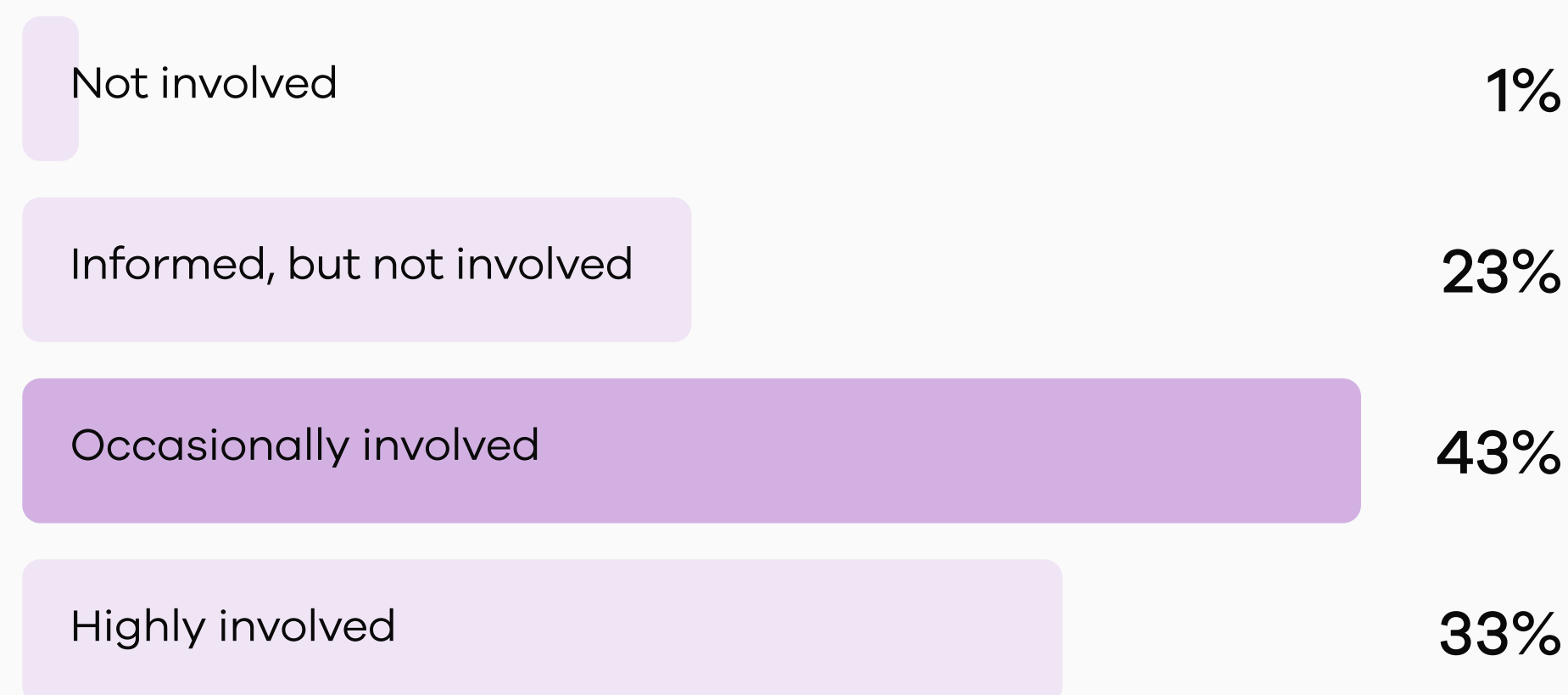
Management should assess the competency of the personnel responsible for implementing these policies and be ready to identify these people—by name—in their annual filing. Finally, the SEC wants companies to report the nature, scope, and timing of a material cyber incident via an 8K or 6k filing within four days after determining it will have material consequence

This level of transparency amongst C-Level executives will require a cultural shift that might challenge some organizations. IDC stated in a [Commvault-sponsored report](#) (see Figure 1) that just one-third of CEOs and Managing Directors are involved in a company’s cyber-preparedness efforts.

Forty-three percent of more than 500 respondents reported that they were “occasionally involved” in cyber-preparedness, and 23% of those surveyed said they were “informed, but not involved” in cyber-preparedness. Just 1% reporting being not involved at all.

FIGURE 1

CEO and Managing Director in Cyber-Preparedness (Percentage of respondents)



n = 513, Base = all respondents; source: IDC Custom Survey sponsored by Commvault, August 2023

“Companies do not always consider their infrastructure planning and IT investments with commensurate information security risk reduction activities as part of their corporate planning and business strategy development.”

MELISSA HATHAWAY
PRESIDENT
HATHAWAY GLOBAL STRATEGIES

The risk to their businesses is real. The average company takes approximately 204¹ days to detect and contain a breach. The longer it takes to detect and contain a breach of corporate networks and data sets, the more costly it becomes to resolve.

The recent SEC cybersecurity rule along with the [Caremark Act](#) in the U.S., Information Security Registered Assessors Program (IRAP) in Australia, [DORA](#) in the EU, and even state-level rules like New York’s Codes, Rules, and Regulations ([23 NYCRR Part 500](#)) are forcing companies to change their culture of transparency to comply with regulations. In 2024, many boards will seek to fill director seats with cybersecurity experts and bring in third-party help.

“The main challenge that many corporations face, though, is that the resources available to increase the resilience of business operations and decrease the exposure to malicious activity are finite,” said Hathaway. “As decisions are made to increase efficiency, productivity, and implement cost-cutting initiatives, it’s essential that these decisions fall within a risk management framework that is informed by modern day threats to networked systems, interconnected devices, and automated business operations.”

Security and IT teams must converge

Companies must invest in cyber resilience and be adequately prepared for an adverse event. This requires bringing security and IT, as well as line-of-business owners, closer together to ensure their cyber resilience framework is documented, tested, and meets regulatory compliance.

To drive cyber resilience across an organization, the intelligence and efforts across teams must converge, concentrating efforts to maintain reliable, secure operations across stakeholders. Bringing these teams closer together will not only result in superior cyberattack preparation, but it will also enable organizations to recover more quickly and emerge from the attack with mitigated damage.

In 2024, the convergence of IT operations (ITOps) and security operations (SecOps) will accelerate to align with best practices and better enable organizations to detect, identify, and thwart threats across domains. For instance, ITOps teams are often responsible for the availability and reliability of enterprise resources, ensuring systems and applications are running smoothly. **If performance degrades or components are no longer available to end users and customers, it typically falls on IT operations to recover data and restore systems.**

Separately, SecOps groups tend to be primarily responsible for intrusion detection and prevention.

As security teams work to identify the anomalous activity that might be a potential threat, ITOps teams could also encounter similar events impacting performance. Collaboration between these domains could more quickly reveal that the alerts seemingly related to performance are actually an attack that the security team must identify and resolve (see Figure 2). While deploying patches often falls to ITOps teams, for instance, an unpatched system could be the source of a security vulnerability. When these teams share information and insights, the impact of potential threats lessens.

Still, survey data from IDC found that these two groups remain disconnected. According to the IDC report, [The Cyber-Resilient Organization](#), just 30% of security operations teams fully understand ITOps roles and responsibilities for cyber preparedness and response. Similarly, only 29% of ITOps teams fully understand what falls to SecOps.

Collaboration between ITOps and SecOps teams will evolve in 2024 or companies will find themselves at a disadvantage. Businesses must think about cyber preparedness across the entire NIST Cybersecurity Framework, which includes detecting, identifying, protecting, responding, and recovering from attacks. As the threat landscape becomes more sophisticated, these two teams must work together on a regular cadence to create common approaches to incident response and common goals for cyber resilience.

FIGURE 2

Responsible for...

IT Ops

- Job scheduling
- Monitoring
- Machine development
- Training
- Help desk calls
- Workers' compensation
- Backups
- Point-of-sale systems
- Application support
- Patch management
- Software deployment

Security Ops

- Monitoring security events
- Monitoring tools
- Compliance and regulatory governance
- Vulnerability scanning
- Identity and access management
- Technical policy changes
- Configuring networks
- Detection and response forensics
- Validation and controls of endpoints

The Futurum Group “also notes opportunity for IT operations teams to provide security teams with more insight into the IT environment, so that security teams can better understand the organization's risk posture. Similarly, security teams can provide IT operations teams with more threat intelligence data, as well as guidance on how to mitigate vulnerabilities, in order to position the organization to respond more quickly to attacks and to shift to a more proactive, as opposed to reactive cyber-resiliency posture.”

“The large majority of respondents indicated that, while collaborative processes and shared goals are steadily on their way to being established, only about half indicated that their organization has integrated their systems and data security.”

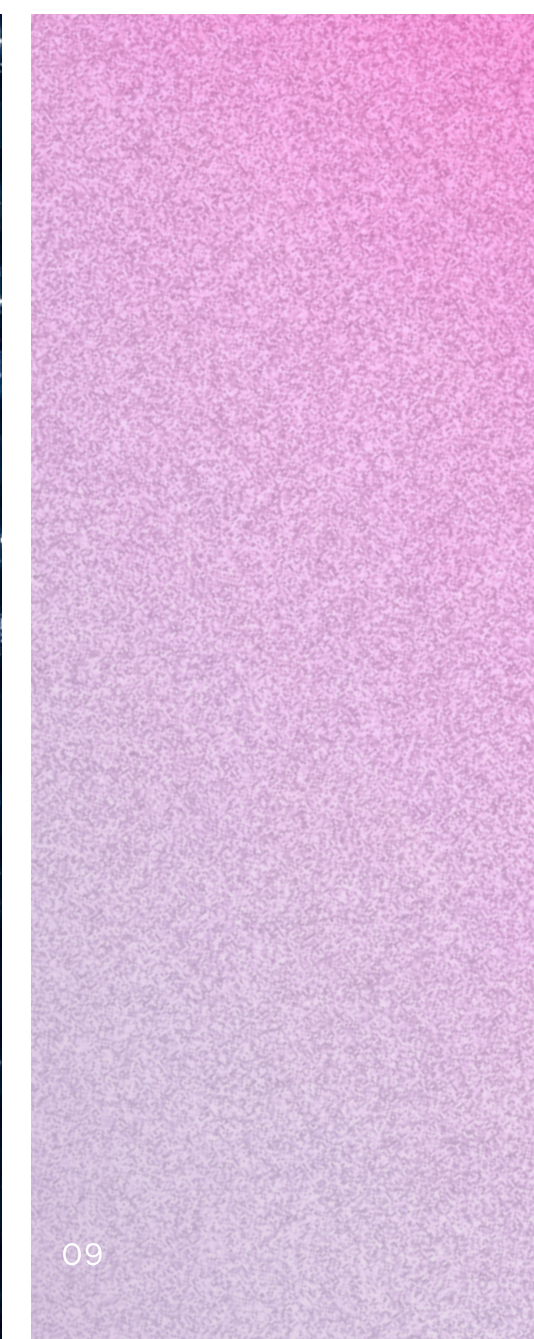
THE FUTURUM GROUP REPORT,
OVERCOMING DATA PROTECTION
FRAGMENTATION FOR CYBER
RESILIENCY

Cyber readiness falls on everyone

A critical component of cyber resilience is cyber recovery. And a key to a fast recovery is cyber readiness.

In 2024, cyber readiness can be validated, and enterprise organizations should be testing and verifying that their planned responses to attacks will result in the desired recovery and protection their business needs. Enterprises must ensure both hardware and software assets are clean following an attack as well as continually test their cyber recovery readiness prior to a breach.

Organizations must practice the most important procedures they will rely on to protect the future of their business. Often these recovery testing and validation processes are cost-prohibitive, such as maintaining an isolated data center with no connectivity to other networks to eliminate contamination leaking out of this recovery testing ground. Many organizations cannot support clean rooms to test and validate security forensic operations and often find themselves vulnerable to attack and not prepared for reliable recovery.



“While the threat and rising impacts of ransomware and other cyber-attacks has been well-established in the market, the survey uncovered that a staggering 98% of respondents indicated that data recoverability influences their ability to be resilient against ransomware attacks, with three-quarters of respondents indicating that it is very or critically influential.”

Still, enterprise organizations admit that disaster recovery and cyber-recovering testing are too often overlooked because they are time-sensitive and intrusive to the organization.

According to the IDC report,

59%

of respondents surveyed expect cyber-recovery efforts to take days or weeks to complete.

Only

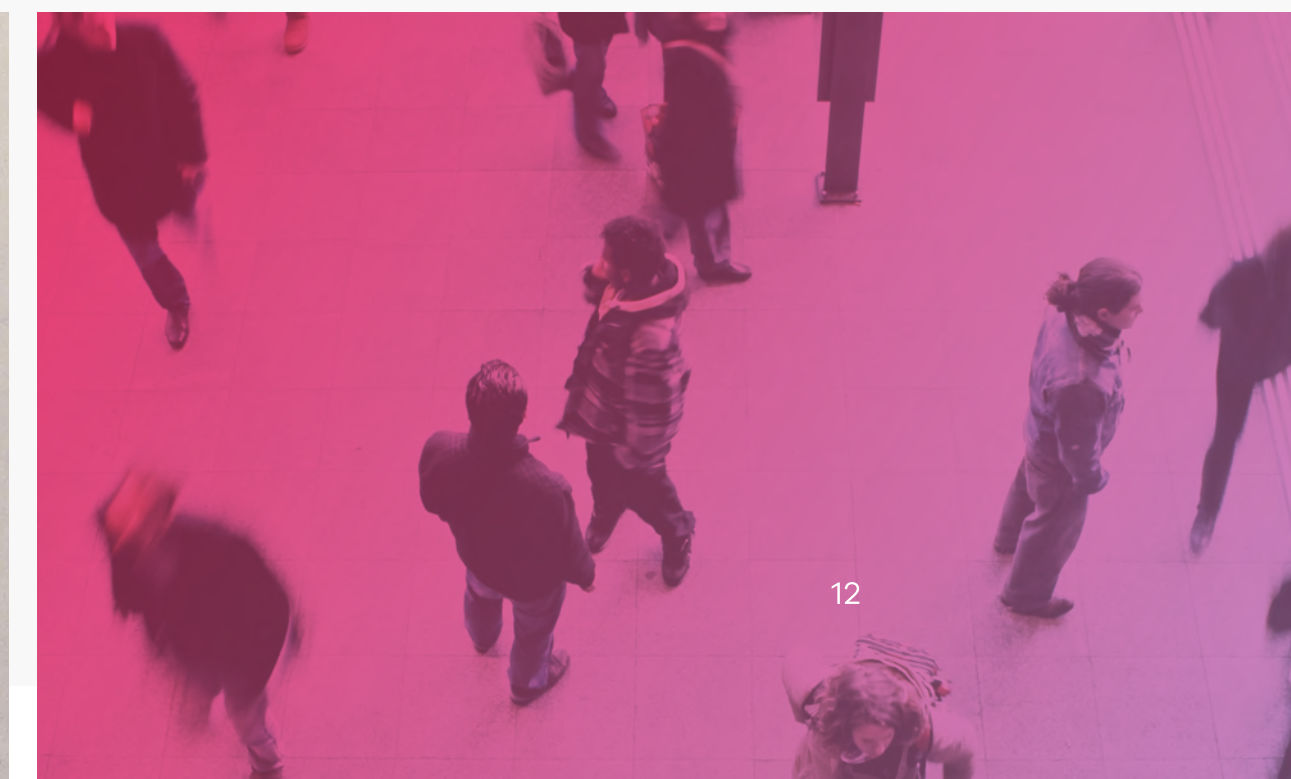
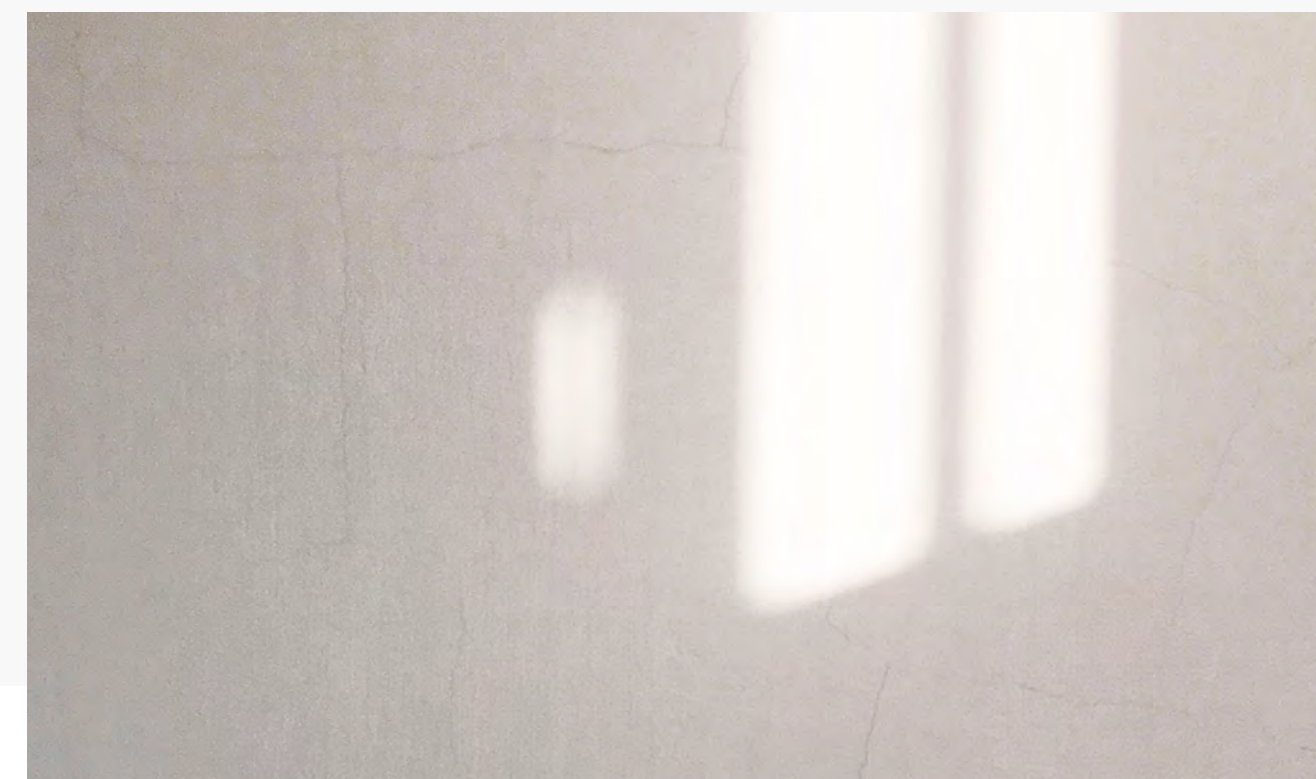
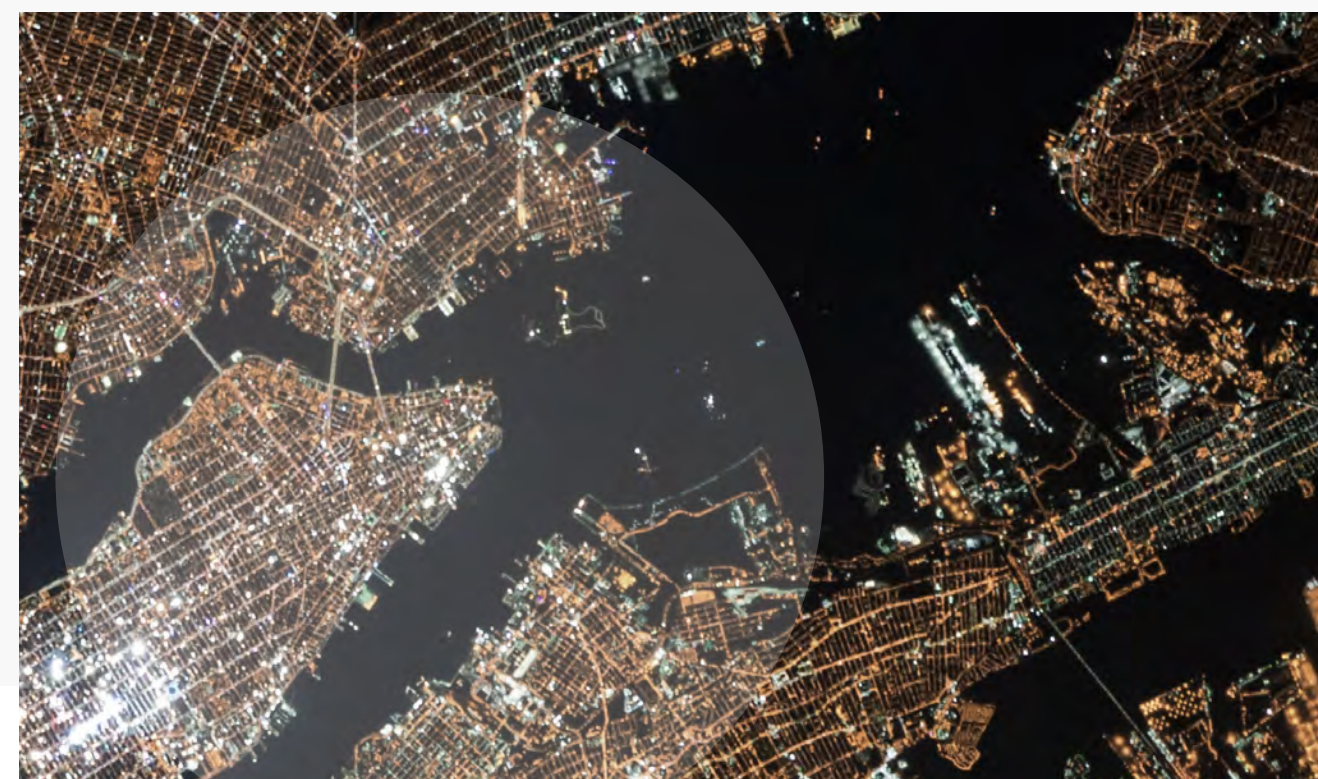
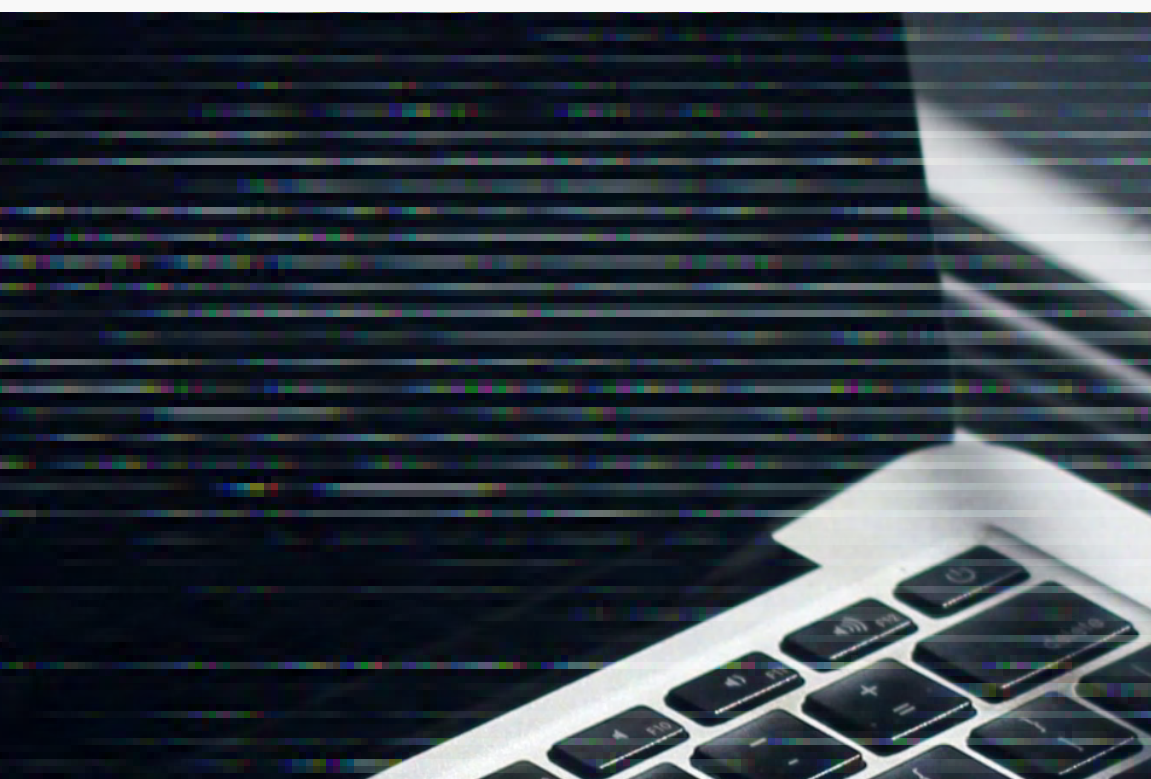
41%

believed they could recover in less than 24 hours.

Proper testing and validation can help avoid the consequences of lengthy recoveries, such as loss of revenue, loss of customers, and cost of downtime.

A company's cyber resilience relies on its capability to **remediate and recover** from a breach.

Data protection takes up a critical role in this effort that ensures the business can operate by evaluating and testing clean points, standing up safe environments, recovering backed up data sets, and continually protecting and testing data in air-gapped instances. The scope of necessary recovery efforts per incident widely varies and increases over time, **making the ability to discover threats early, react sooner, and minimize how much needs to be recovered paramount.**



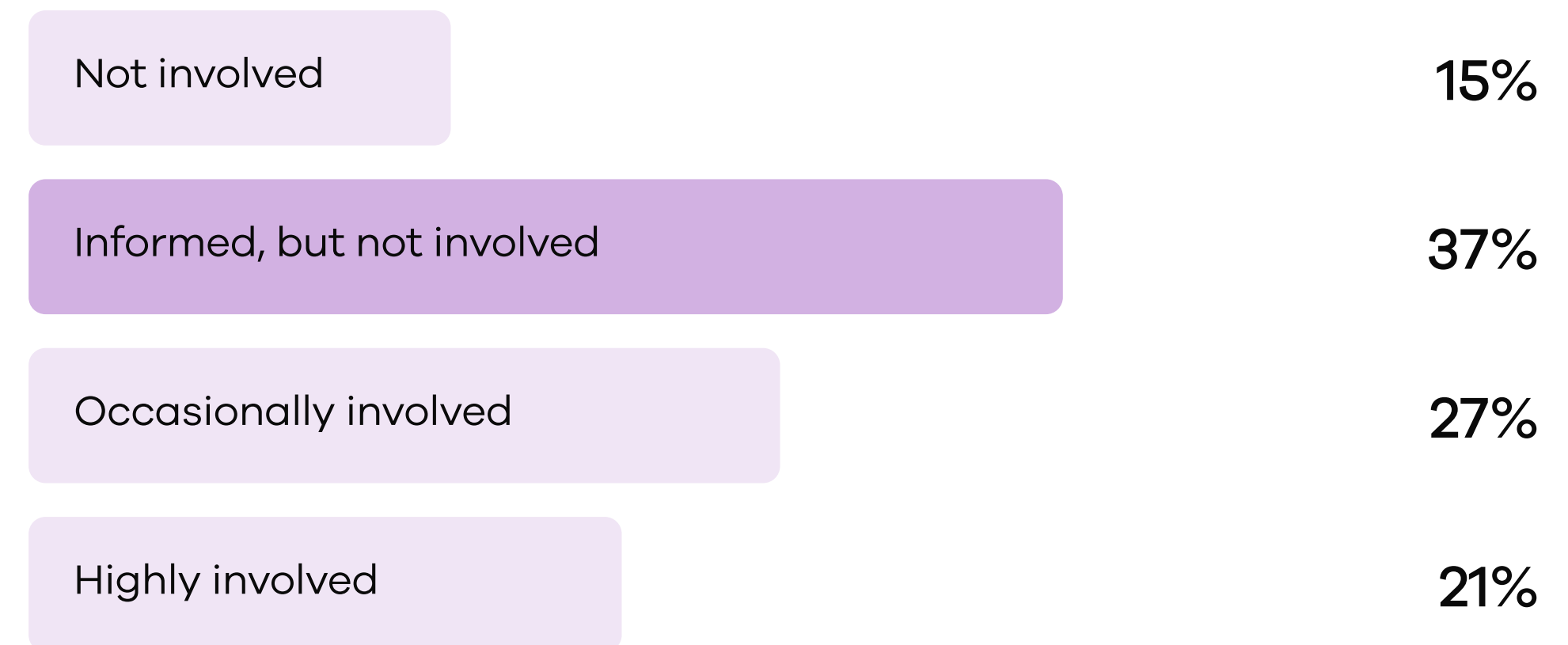
In 2024, all levels of an organization will be involved in cyber recovery, including the lines of business.

This level of involvement across the business is critical to minimizing the impact of an attack and accelerating resolution. The onus of cyber readiness falls on everyone in an organization also because lack of awareness following an attack slows recovery efforts. Cybersecurity awareness and training will go a long way toward enabling the entire organization to act appropriately in the wake of an attack.

“LOB leaders are highly involved in less than a quarter of cases and essentially not involved in 52% of cases. To amplify what we learned from our panelists, LOB leaders cannot suddenly become interested after the organization has been attacked; they must be involved in the preparation efforts so that all employees take training and awareness seriously. Without thorough training and awareness, organizations increase risk of attack and are more likely to experience longer recoveries,” the IDC report reads.

FIGURE 3

Line-of-Business Leader Involvement in Cyber-Preparedness



n = 513, Base = all respondents; source: IDC Custom Survey sponsored by Commvault, August 2023

Adopting AI for good ... and bad

A critical component of cyber resilience is cyber recovery. And a key to a fast recovery is cyber readiness.

Given the hype and attention around artificial intelligence (AI), it shouldn't come as a surprise that organizations will continue to incorporate AI into their cyber resilience and data protection efforts.

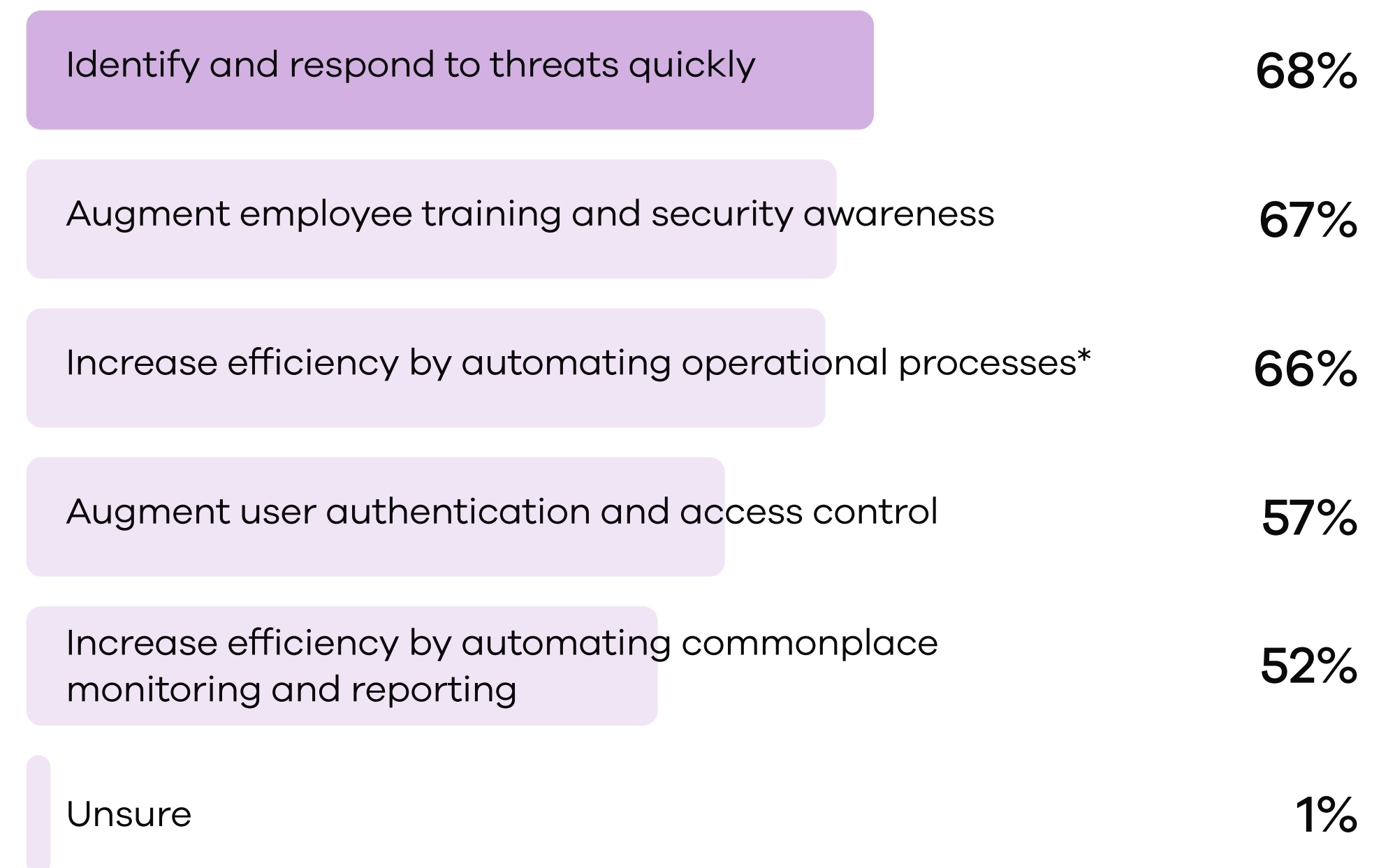
Already, nearly 70% of respondents indicated that they have integrated AI into their data protection toolset, according to The Futurum Group. While they note that figure is likely inflated due to the industry-wide AI-washing (more on that in a moment), it's still a good indicator of customers' appetite to utilize AI to augment their cyber resilience.

AI will be pivotal to cyber resilience as the threat landscape continues to expand, characterized by a diverse array of assets that may cross boundaries, encompass multiple tenants, and include a mix of hardware, virtual environments, software-defined systems, third-party control, and assets in software-as-a-service (SaaS) spaces.

The ability to collect, analyze, and interpret data from these assets and surrounding systems is critical in identifying potential security threats or anomalies.

FIGURE 4

How is AI improving, or how would you expect AI to improve your organization's security?



*e.g. vulnerability scanning, patch management, and incident response

AI will significantly impact these areas, bringing together and analyzing vast amounts of telemetry data, and pivoting from single events to correlating a series of meaningful events within a context that humans can quickly assess as a threat or attack or can trigger automated responses based on thresholds.

With AI comes quicker response times, better focused resources/reduced alert fatigue, and more time to focus on effective threat mitigation strategies – **all benefits for a cybersecurity team that needs to see the full picture.**

However, the good guys aren't the only ones that will benefit from AI. Malicious actors will use AI in ransomware to enhance attack capabilities and better evade detection. Among the ways AI could be deployed:

Generate malicious code

or phishing emails that mimic trusted entities or individuals

Automate and scale up attacks

using machine learning algorithms

Evade detection

by blending in with normal system behaviors

Use voice cloning

or native language accuracy for voice-based or email-based phishing

Change its code

and exploit channels automatically

Cybercriminals will also focus the impact of attacks by using defender tools to perform tasks like asset discovery and vulnerability analysis across a broad range of diverse assets. Unlike defenders who use this information for protection, attackers will prioritize and exploit vulnerabilities that maximize impact with minimal effort, leveraging the same advanced tools and AI-driven analysis typically used for defense. Attackers may even go so far as to run predictive modeling to understand the degree of impact or discover new parameters and techniques that lead to creating a new emerging threat.

In 2024, companies will recognize and handle their data as assets, placing emphasis on robust asset management, talent acquisition and development, and future planning—all fundamental elements to enhancing cybersecurity.

Companies will use AI to analyze, index, and classify data assets for a range of purposes, including securing their data, streamlining, and minimizing an attack surface, and ensuring data segmentation into well-governed domains through high-fidelity controls and responses from security automation and orchestration tools.

Ongoing development of IT and security teams will be essential, especially as it relates to deploying, maintaining, and administrating new AI systems.

For businesses,
human oversight will
remain crucial, requiring
them to prioritize ongoing
education and upskilling to
ensure their teams can
leverage AI technologies to
their full potential while
maintaining vigilance over
their critical systems
and data.

Cyber resilience requires tool consolidation

Most businesses have multiple cloud providers and SaaS applications. These multi-cloud environments require a closer look at data security and protection because inconsistencies in data reporting and storage could exist across the varied environments.

Enterprise organizations must be able to verify that the data housed across the cloud environments and systems is being secured —and that it is recoverable.

The sooner businesses evaluate the risk created by having multiple cyber resilience solutions deployed to protect their data, the sooner they can reduce their potential data loss.

“Reducing the silos and complexity of data protection is necessary for enterprises to maximize their cyber-resiliency, as their data grows increasingly fragmented across a heterogeneous mixture of on- and off-premises applications and infrastructures.”

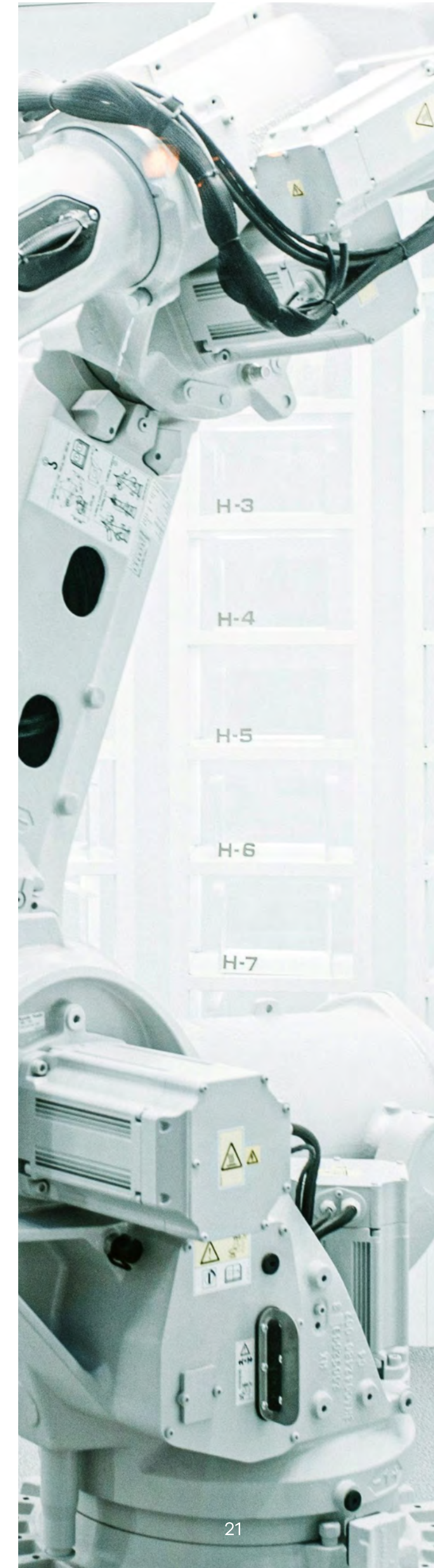
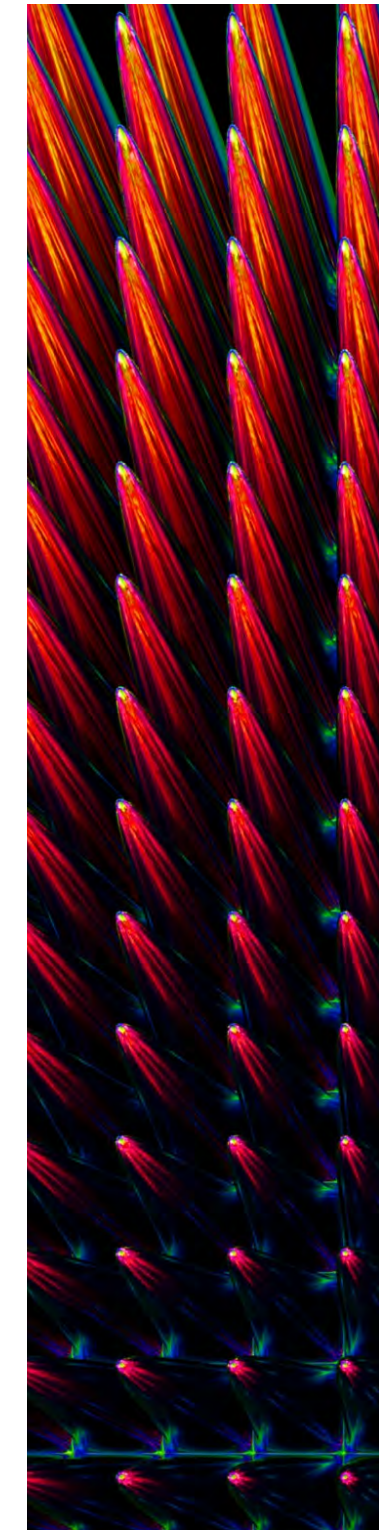
A challenge many organizations face also involves the myriad tools and technologies used across the environment to measure performance, maintain availability, and protect data and resources.

While the initial intention in acquiring the tools is positive, the proliferation of too many technologies and the fragmentation of data protection tools will ultimately lead to data sprawl—threatening an organization’s overall cyber resiliency.

“Further leaning into shared tools and processes, such as security information and event management offerings that provide a more holistic view across the IT environment in order to uncover, analyze, and respond to security threats, is a key area of opportunity to improve joint response to, and remediation of, incidents.”

THE FUTURUM GROUP REPORT
OVERCOMING DATA PROTECTION
FRAGMENTATION FOR CYBER
RESILIENCY

Not only must silos break down in 2024, organizations must also consolidate the tools they use across teams to minimize potential miscommunications and gaps in coverage. **Not only do many tools cost money, but they can also hurt an organization by creating blind spots or redundant noise.**



Part of the problem that occurs when data is scattered across multiple tools is that the context is lost. Context is critical in understanding the nature of an event and the likelihood that it is part of a greater cybersecurity threat. For instance, sometimes network metrics will reveal a bad actor on the network that the security team would recognize as a potential threat that perhaps the network team would categorize as just an anomalous event, delaying a proactive response to prevent a bigger breach.

“Everyone wants high-performing, reliable, and secure digital products, or services, whether you’re in security, DevOps, site reliability, or the network. That drive for a common outcome among IT domains is pushing teams to invest in tools that can find the theme across all these data sources and provide more collaboration across teams,” says Stephen Elliot, group vice president I&O, cloud operations, and DevOps, IDC, in a [recent Network World article](#).

Generative AI washing comes clean

“Generative AI” won the battle of the buzzwords in 2023, and in 2024, industry watchers expect generative AI will prove it deserves all the hype as more businesses apply the technology to become more efficient and effective. While the potential applications of AI could be limitless, how much of it is vaporware and what are some of the potential downsides?

A search of PR Newswire turns up nearly 2,500 news releases that mention generative AI. The question is, “How much of it is real?” This year, vendors will need to start delivering on the promise of generative AI in their product sets.

While generative AI offers numerous benefits, there are also potential downsides to consider in enterprise applications:

Ethical Concerns

Generative AI can raise ethical concerns, particularly in areas like deepfakes, where it can be used to create manipulated or misleading content. Enterprises need to be cautious about the ethical implications and potential misuse of generative AI technology.

Quality Control

Generative AI may not always produce outputs of the desired quality. There can be instances where the generated content or recommendations are inaccurate, biased, or lack the necessary context. Enterprises need to invest in robust quality control mechanisms to ensure the reliability and accuracy of generative AI outputs.

Data Privacy and Security

Generative AI relies on large amounts of data, and enterprises must ensure the privacy and security of sensitive information. The use of generative AI may increase the risk of data breaches or unauthorized access if proper security measures are not in place.

Overreliance on AI

There is a risk of over-reliance on generative AI, where enterprises may solely depend on AI-generated outputs without critical human oversight. This can lead to a loss of human judgment and decision-making, potentially resulting in errors or biased outcomes.

It is important for enterprises to carefully consider these downsides and address them through responsible implementation, robust governance frameworks, and continuous monitoring to mitigate potential risks.

Automation speeds security response

Much like GenAI, automation will become an even more important tool in 2024 for businesses looking to thwart sophisticated attacks.

Enterprise environments include many systems, devices, applications, and other resources that generate logs, events, and alerts. Automation can collect, correlate, and make sense of the meaning of the data from various sources faster than can be done manually. Automated incident response aims to identify and triage the source of potential threats, bubbling up the meaningful alerts to human operators for further investigation.



Additionally, as cyber attackers deploy more clever tactics, relying on manual detection and reporting processes are very likely to result in missed anomalies and successful attacks.

A potential solution—



Automation

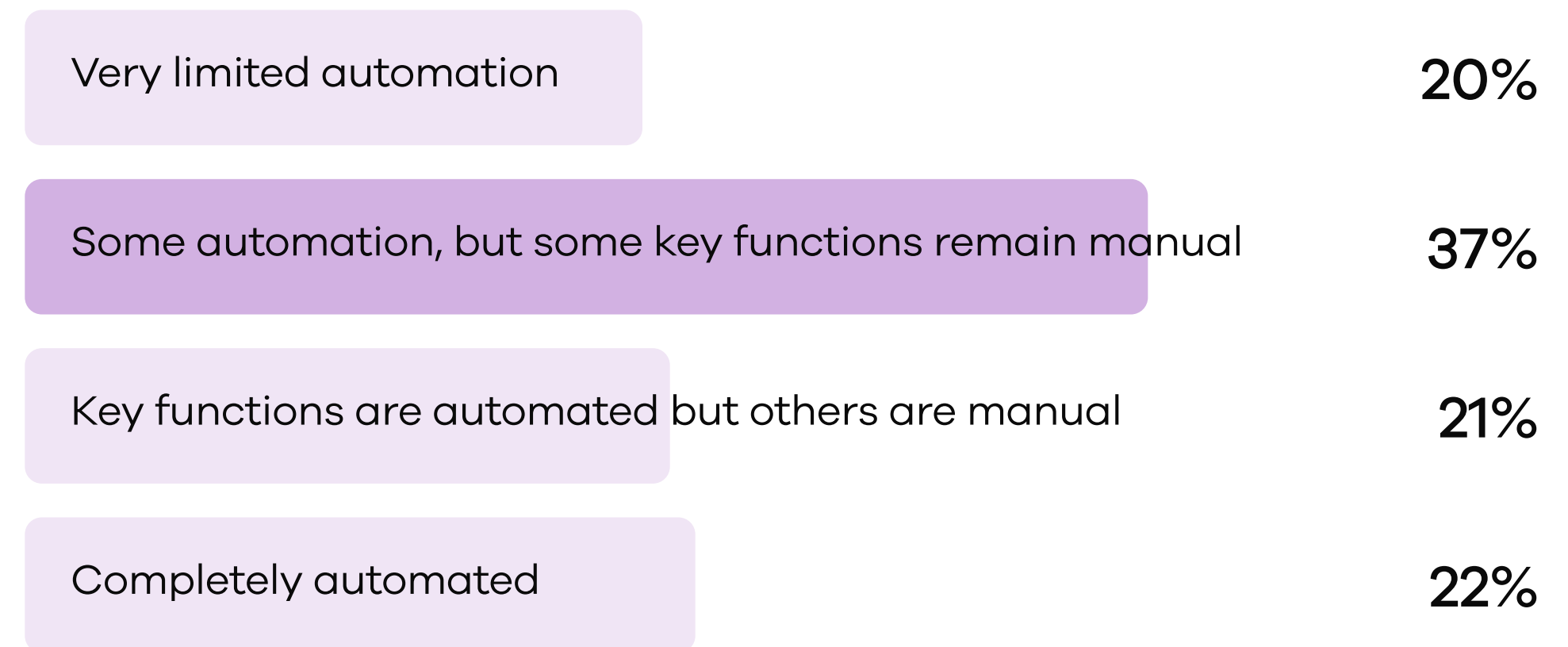
—could lead to faster detection to mitigate the intrusion impact.

However, most organizations (57%) have limited automation for key functions, increasing their chances of missing a threat before it happens; only 22% report being fully automated, according to IDC.

“Speed of detection is clearly key to mitigating intrusion impact, and detection, in particular, requires automation to be effective. However, it appears that most organizations are still on the journey to fully automated detection and reporting,” the IDC report states.

FIGURE 5

Degree of Automation in Cyber-Detection and Reporting (Percentage of respondents)



n = 513, BAse = all respondents; source: IDC Custom Survey sponsored by Commvault, August 2023

Automation will also become one of the more important tools for cyber resilience as more businesses report skills and talent shortages in security. According to [ISC2's Cybersecurity Workforce Study](#), the global cybersecurity workforce grew to 5.5 million, but the gap between supply and demand remains.

"The pressing reality is that we must double this workforce to adequately protect organizations and their critical assets," said ISC2 CEO Clar Rosso in a statement. "Our message is that organizations must invest in their teams, both in terms of new talent and existing staff, equipping them with the essential skills to navigate the constantly evolving threat landscape."

The recent ISC2 study shows that "75% of cybersecurity professionals view the current threat landscape as the most challenging it has been in the past five years."

In addition to that,

52%


believe that their organization has the tools and people needed to respond to cyber incidents over the next two to three years.

40%

believe automation in cybersecurity will have the greatest positive impact on their ability to secure an organization.

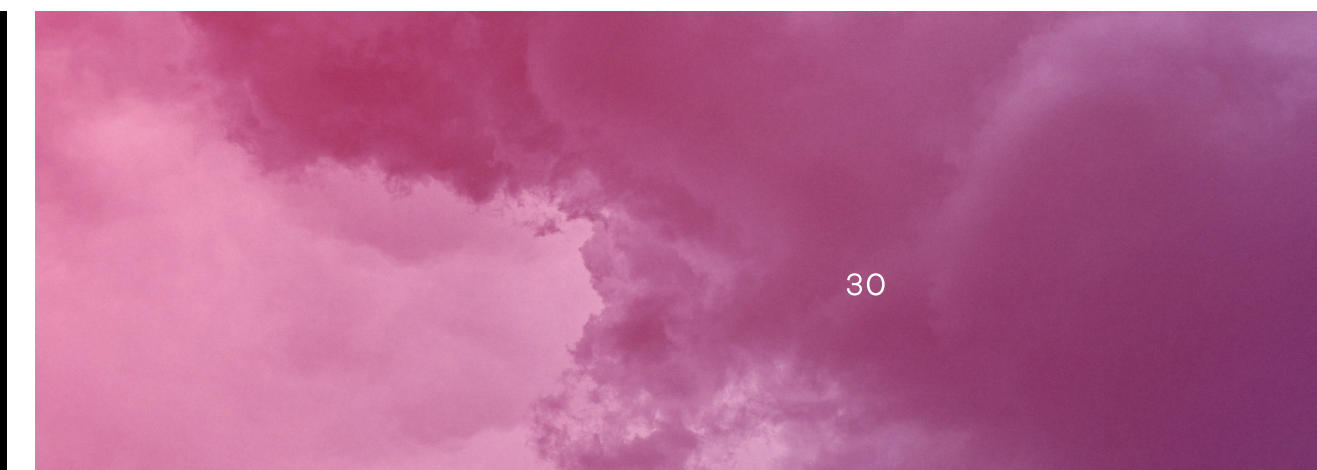
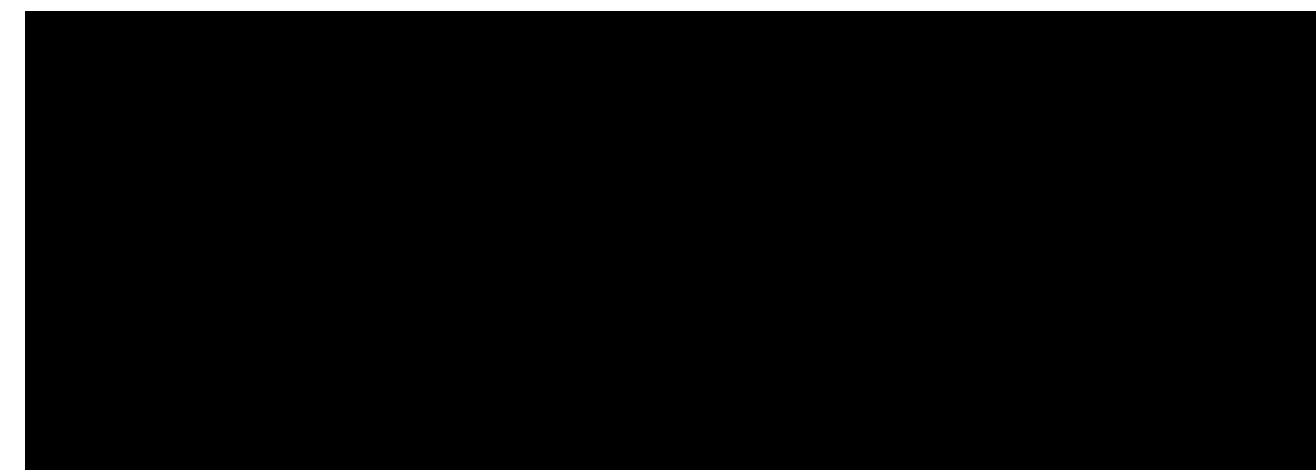
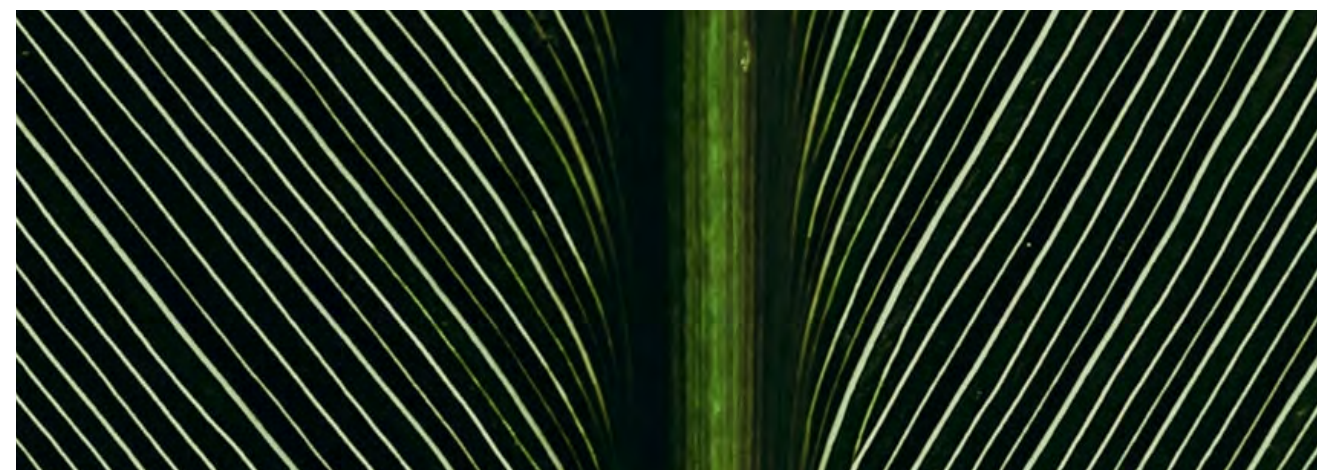
30%

point to advancements in AI as another positive resource for cyber security.

As budget constraints persist into 2024 limiting headcount,  automation will help fill the gaps as businesses hope to protect against the ever-evolving threat landscape.

Achieving cyber resilience in 2024

Cyber resilience encompasses the ability of an organization to withstand and recover from cyberattacks, and it incorporates many disciplines working in concert to protect data, detect threats, respond to attacks, and recover quickly and fully from disruptions. It is imperative that organizations focus on cyber resilience in 2024, but there is no end date for this improvement project. Cyber resilience must constantly evolve to stay ahead of bad actors and the threats they pose.



Business leaders can empower themselves with cyber readiness and continuously improve on their cyber resilience by following a few guidelines.

Know the regulatory requirements

It is paramount that business leaders protect their assets and the assets of their customers. Understanding the recent regulatory requirements will help organizations stay compliant and remain on the right side of regulators. Cybersecurity is a strategic differentiator for businesses in this digital age. Organizations will look to place cybersecurity experts on their boards to ensure proper oversight of cybersecurity risk management.

Break down silos, give teams a common goal

IT and security teams should enhance collaboration across their teams and other lines of business throughout an organization. Network, server, application, storage, cloud, and more assets generate tons of data that can have multiple meanings. Bringing these teams together can help front-line IT and security professionals more quickly identify if a network performance issue is actually an early indicator of a potential security attack. With all teams working toward cyber resilience, collaboration will increase, downtime will lessen, and the threat landscape will be minimized.

Drive cybersecurity awareness

Provide cybersecurity education and training to all employees of an organization. Empower lines of business leaders with the knowledge to protect their teams and their customers from potential vulnerabilities. The types of number of potential attacks increases every year, and communicating to employees the known threats and the methods of attacks can better safeguard them and your organization.

Adopt AI for good

AI brings with it the promise of more efficient, effective cyber readiness. With intelligent systems aggregating and correlating data, human operators will be able to more quickly find and protect vulnerabilities as well as identify when anomalous behavior is part of a malicious attack.

Minimize risk, consolidate tools

Organizations tend to buy tools to address a specific issue, and eventually, this results in too many tools, oftentimes that cannot communicate with each other. All these tools while trying to solve a problem or provide insights can actually present unknown gaps in coverage and pose potential risks to an organization. By consolidating tools, organizations can create an environment of integrated technologies and reduce the blind spots hidden within disparate tools.

Embrace GenAI with some cautions

It remains to be seen how GenAI will be best applied in many use cases, but it is worth exploring to better understand how to protect assets and recover from attacks. It is a given that bad actors are tapping into the power of GenAI to orchestrate their next malicious endeavor. Organizations should also be experimenting and testing how they can take advantage of the advances in this technology to better secure their environments.

Leverage automation

Humans will always be needed in the cybersecurity domain, but with significant advances in technology, automation can reduce the noise and lessen the tedious workloads from security pros who should be focusing on strategic efforts to thwart attacks. Let automation troll through myriad logs to find the anomalous events and correlate the data to find the true source of a threat—and free skilled staffers to help the organization become cyber resilient.

Conclusion

This report has highlighted the seven major trends in cyber resilience that the C-suite should be thinking about and acting on to achieve true cyber resilience in their organizations. From regulatory compliance and the convergence of security and IT teams to the adoption of generative AI and automation, these trends underscore the strategic imperative of cyber resilience.

By staying ahead of these trends and embracing a comprehensive approach to cybersecurity, C-level executives can effectively protect their organizations, maintain stakeholder trust, and position themselves as leaders in the face of an ever-evolving and growing landscape of cyber threats. It is crucial for C-suite leaders to prioritize cyber resilience as a strategic imperative and work toward building a resilient and secure future for their organizations.