panaseer

Optimizing cybersecurity:

Striking the balance between people and technology

ABOUT THE EXPERTS

Andreas Wuchner

Advisory Board Member and Field CISO at Panaseer

Andreas is a recognized cybersecurity and risk expert, with more than 25 years' experience as a business owner, board advisor and investor in complex global business environments. He advises cybersecurity startups in the US and Europe.

Marie Wilcox

VP of Marketing at Panaseer and Board Director at the Chartered Institute of Information Security

Marie has more than 20 years' experience in IT and Information Security. Prior to working at Panaseer she held senior leadership roles in both large corporates and startups including McLaren Applied, Digital Barriers, BAE Systems and Siemens.

Contents

Key findings

Security budgets need to rise 40% more to maintain confidence

Three-quarters (**75%**) of respondents said their lack of resources was impacting cyber risk mitigation. A total of **24%** qualified the impact as “significant”. Current budgets – which on average rose **29%** this year – would need to rise **40%** more to restore confidence. But **35%** of budgets today go on security tools that don’t measurably improve security posture.

Cyber teams are considered too small with too few skills

The biggest factors negatively influencing security posture were ranked 1) lack of security skills, 2) lack of budget for security training, and 3) low security team headcount. Given an extra increase in cyber budgets, **52%** said they’d invest it in a hiring spree.

Security automation has proven benefits, but still mostly limited to downstream tasks

Nearly all **(96%)** of our sample are actively engaged in security automation and enjoying the benefits. The most commonly automated functions are monitoring (**53%**) and reporting (**42%**), but around one-third of respondents are giving automated tools a more active role in upstream processes like incident response (**38%**), risk prioritization (**36%**) and threat hunting (**29%**).

Four out of five security leaders worry that consolidation of tools and vendors compromises security posture

While **86%** of organizations are consolidating cyber tools and vendors, **78%** are "very" or "somewhat" concerned that this reduces their ability to mitigate cyber risk. Just **19%** of those yet to consolidate think it will improve their security posture, whereas more than double the number (**42%**) of those who have reported an improved security posture as a real benefit.

The impact of new security regulations will be positive and far-reaching

Over one-third (**35%**) of respondents are bracing themselves for the "significant" impact of cyber legislation (like proposed SEC regulations, DORA, etc.) in the next two years. Security teams expect it will be worth it, with **74%** believing there’ll be a positive effect on their ability to manage cybersecurity posture. But they’ll need to do more in areas like controls monitoring and particularly compliance audits where around half (**49%**) currently rely on a manual, point-in-time approach.

Introduction

Cybersecurity is a fascinating discipline because it's constantly evolving. New tech, new adversaries, new TTPs. But the more things change, the more things stay the same, with security teams under constant pressure from all sides.

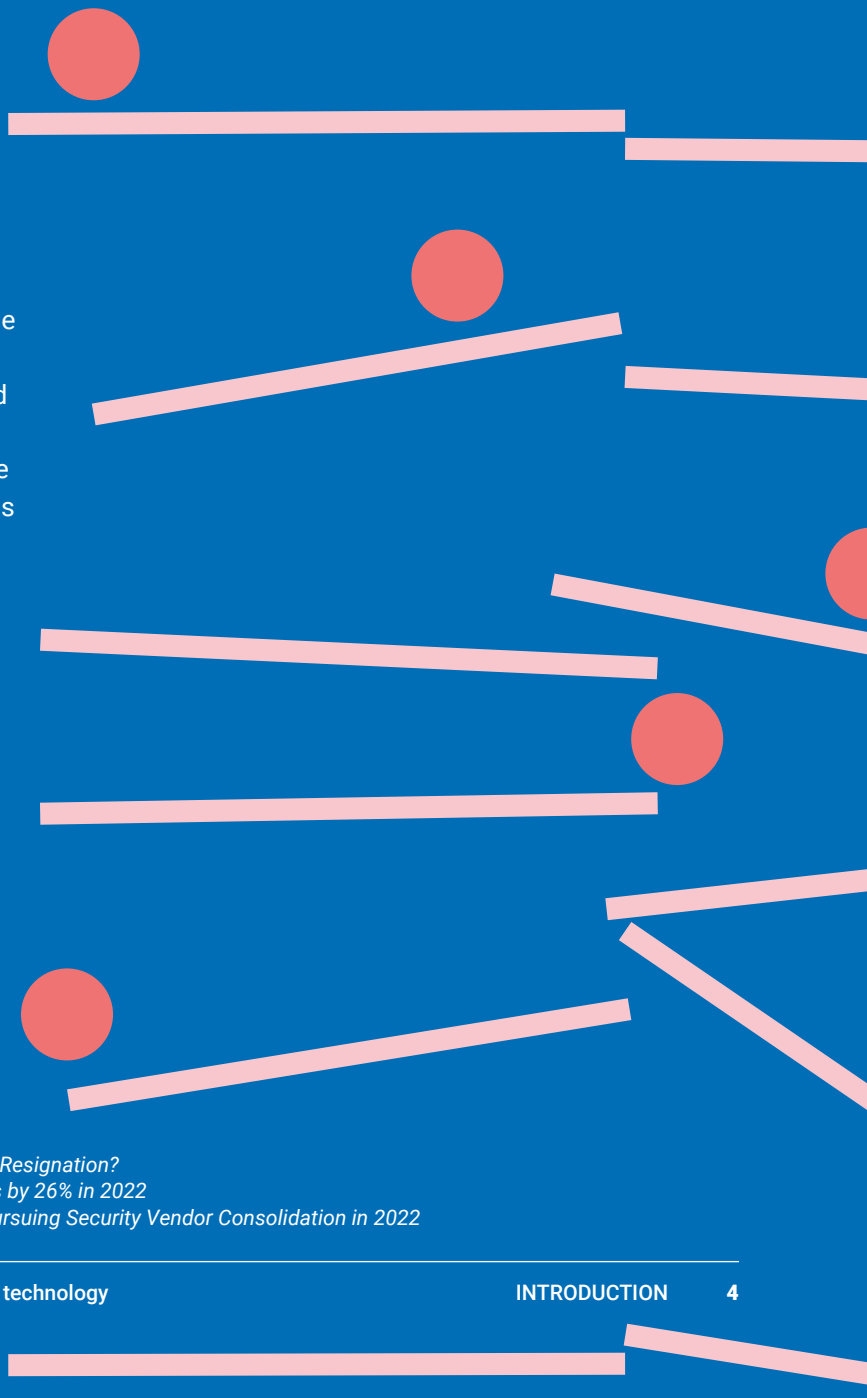
There are always more tools and larger attack surfaces to deal with; more scrutiny from regulators and senior leadership; more security risks to understand and mitigate.

Keeping pace is almost impossible in the face of a perpetual stream of urgent security events, particularly when competition for skilled security professionals is so fierce. There are numerous reports finding that CISOs and security teams are deciding they've had enough and would prefer a career that doesn't threaten to burn them out[1].

This way of operating needs to end. Hiring more people will never be the solution for an industry faced with a chronic skills shortage[2], so security teams need to find efficiencies through consolidation of their tech stack and process automation. Gartner's research shows the industry is embracing vendor consolidation as a means of simplification[3], but security teams are feeling the pain while transformation plans are slowly rolled out.

This report draws on new primary research among cyber professionals to explore how security leaders are confronting these challenges and driving more value from their security resources. We scrutinize how well they're funded, how they're coping with evolving pressures, and how they're using technology to become more efficient. With stiffer regulatory compliance mandates on the horizon, how might this drive changes in their own approach to managing risk and finding the optimum balance of people and technology in their teams?

Expert commentary is also provided throughout our analysis by two experienced professionals in this field, Marie Wilcox and Andreas Wuchner.



1 Security Intelligence (2023), *Is Cybersecurity Facing its Own Great Resignation?*
2 Infosecurity Magazine (2022), *Cybersecurity Workforce Gap Grows by 26% in 2022*
3 Gartner (2022), *Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022*

SECTION 1:

Are more security people needed or can teams evolve?

It's well understood that security teams are stretched, with not enough people, skills or budget to cope with all their priorities. Our research emphasizes this point, with around **74%** of respondents stating that their ability to manage organizational cybersecurity posture was being negatively impacted by lack of security resources. A quarter (**24%**) said the lack of resources was having a significant impact on their ability to mitigate cybersecurity risk.

Seeing security as a people problem

Drilling deeper, the greatest concerns were around lack of security skills (**30%**), lack of security training budget (**30%**), low security team headcount (**28%**) and low overall security budget (**26%**). It's clear from this that the security challenge is fundamentally a people problem. Why is that, and what are the potential solutions?

It's true that cybersecurity is experiencing a prolonged crisis in supply and demand for skills. Cyberseek[4] puts the current ratio in the US at **69%,** meaning fewer than 7 out of 10 cybersecurity jobs can be filled by the available workforce. Worldwide, Cybersecurity Ventures[5] estimates there will be 3.5 million unfilled positions by 2025.

4 Cyberseek (2023), Cybersecurity Supply & Demand Heatmap
5 Cybersecurity Ventures (2023), *Cybersecurity Jobs Report: 3.5 Million Unfilled Positions In 2025*

This creates a vicious circle, the effects of which include:

> **Skilled people are so scarce that even organizations with the money to attract trained cyber professionals can't fill the positions.**
>
> Marie Wilcox, VP of Marketing at Panaseer and Board Director at CIISEC

Marie Wilcox is VP of Marketing at Panaseer and Board Member at The Chartered Institute of Information Security **(CIISEC)**. She's witnessed first-hand how difficult it is to attract, motivate and retain highly-skilled security professionals.

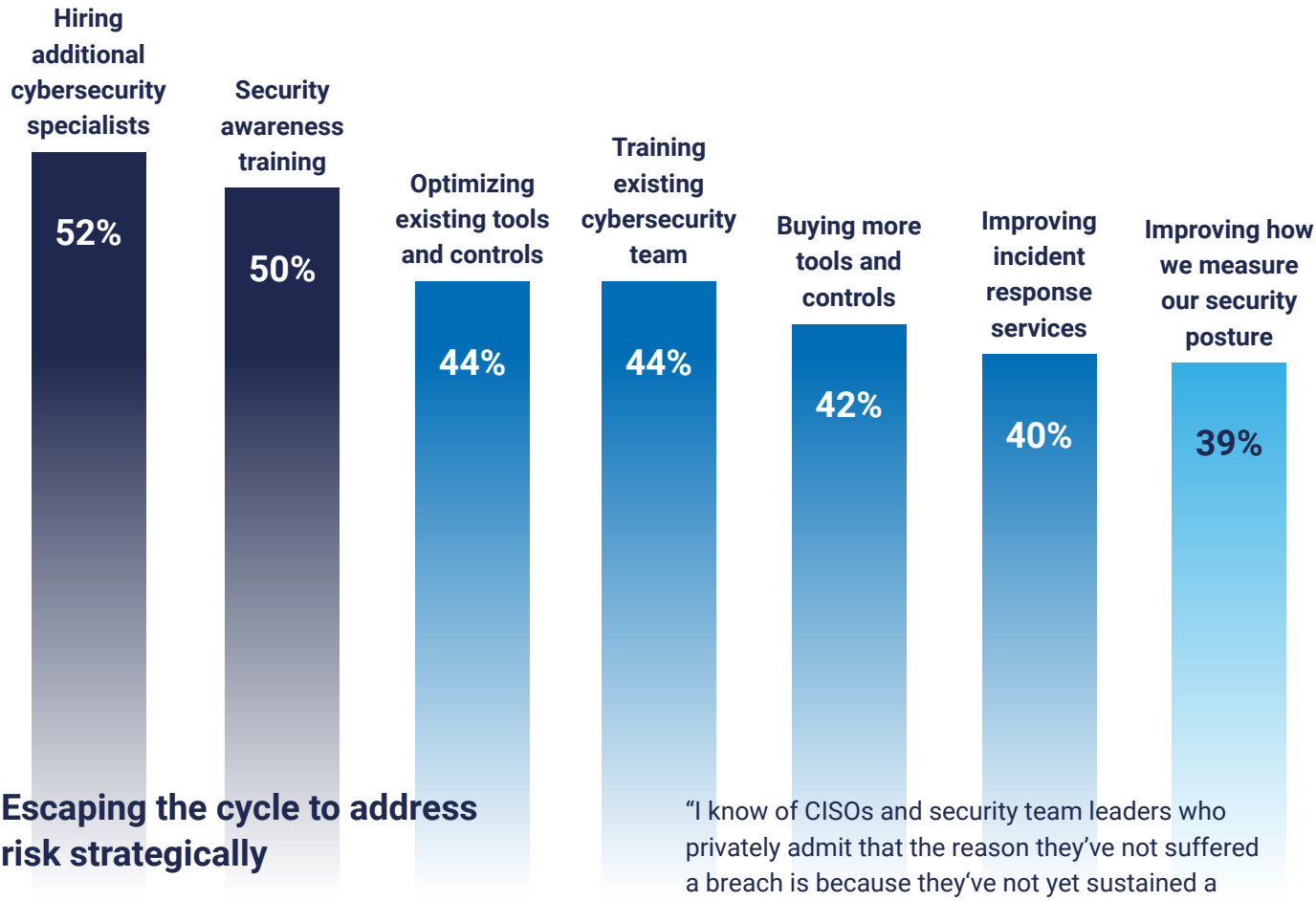
"Skilled people are so scarce that even organizations with the money to attract trained cyber professionals can't fill the positions. At the same time, individuals who are employed into cyber roles are frequently given onerous and demoralizing admin and reporting tasks that don't use their skills, and they soon want to leave," says Wilcox.

Another striking finding from the research is that the same security teams that lament deficiencies in resources and budget have been receiving sizable increases. Respondents reported average budget increases of **29%** in 2023, but say this would need to rise a further **40%** to instill sufficient confidence in their ability to mitigate security risks.

Given a hypothetical increase in budget, more than half (**52%**) would spend the money hiring more security specialists. Other key priorities would be security awareness training (**50%**) and upskilling the security team (**44%**).

People-related spending priorities ranked slightly higher among our UK respondents than US-based respondents who tended to choose more technology-led priorities. This may reflect the relative maturities of each market, with the US ahead with technology adoption and their cultural acceptance that efficiencies can be found by automating menial tasks.

If you were given a budget increase, where would you prioritize spending to improve your security posture?



Escaping the cycle to address risk strategically

Field CISO at Panaseer, Andreas Wuchner, acknowledges the day-to-day constraints facing security teams but believes the solution has to be more strategic.

"Security teams are getting pressure from all sides, but it doesn't make sense in the long term to address a lack of people with more people. Especially when these skilled professionals simply don't exist. Something has to change, but change is difficult. And that change should start as soon as possible because 'lack of resources' is becoming just an excuse."

Marie Wilcox routinely comes across security professionals referring to the 'whack-a-mole' challenge. This speaks to the circular mission of endlessly solving urgent problems and having no time left to make systemic change happen.

"I know of CISOs and security team leaders who privately admit that the reason they've not suffered a breach is because they've not yet sustained a serious attack. They're doing everything they can but can't get ahead of the curve," says Wilcox.

"My concern is this cycle will continue until organizations bring in the right technology, embrace automation and give skilled cyber people more valuable and rewarding responsibilities. But it feels like everything has to stop for that to happen, and unfortunately cybersecurity doesn't work like that"

Security teams don't have the time to think strategically and find ways of being less people-oriented in addressing their workloads, and so the cycle continues. They need to simplify things and become more efficient, and the way to do that is by accelerating a shift to security automation and vendor consolidation.

SECTION 2:

Do security teams fear the change that automation and consolidation brings?

It's clear that security teams need to regain control and address the resource issue by being more strategic than just adding people. Two responses trending in the market are consolidation and automation of security tools and processes. A Gartner survey[6] found almost three times as many organizations pursuing consolidation in 2022 (**75%**) as in 2020 (**29%**). The strong market growth of technologies like SOAR and EDR is testament to the significant adoption of security automation products among large enterprises.

Both automation and consolidation promise significant advantages in efficiency and security performance. Yet both represent change that may be uncomfortable to absorb, particularly with so little time and resource available to do more than simply "keeping the lights on".

Our research examined the drivers for both trends, and how security professionals comprehend the associated risks and benefits. Is there a fear factor and how can it be overcome?

35%

of security budgets is spent on tools that don't give a measurable improvement in cybersecurity posture.

The reality of consolidation is better than the perception

According to our respondents, an average of **35%** of security budgets is spent on tools that don't give a measurable improvement in cybersecurity posture. Such a high figure should be alarming for business leaders who understandably expect maximum ROI from cyber tools. But it's perhaps unsurprising in situations where cybersecurity teams are driven to implement new tools first, and then work out how to measure their effectiveness later.

"There are so many systems and overlapping controls, and often no single source of truth to tell organizations what they have, which increases risk and operational inefficiency. The true figure could be even higher than the **35%** indicated in this survey," says Wuchner. "I'm doubtful that the remaining **65%** is being spent on strategic risk reduction, even in large financial sector organizations."

He identifies security tool proliferation as an opposing force in efforts to become more efficient. Businesses are continually drawn to address emerging threats by adding best-of-breed point solutions.

"Wanting to fill these gaps often comes from the latest headline threats or the onset of greater digitalization opening up new security vectors. What results is an unwieldy accumulation of disconnected tools and functionalities with conflicting or unmanaged security controls, often producing 'alert fatigue'. Consolidation of tools is a logical response to that, but it relies on knowing what the effect of switching tools off will be, before you pull the plug."

6 Gartner (2022), *Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022*

This uncertainty is evident in the anxiety felt among respondents about the unintended consequences of rationalizing existing cyber toolsets. More than three-quarters (**78%**) admitted being concerned that consolidation will reduce their ability to mitigate cyber risk. Those who are "very concerned" number twice as high among our US respondents (**35%**) as their UK-based peers (**18%**).

There is good reason to suspect that this skepticism is unfounded. The experiences of our respondents indicate that the actual outcomes of consolidation are more positive than those perceived prior to committing.

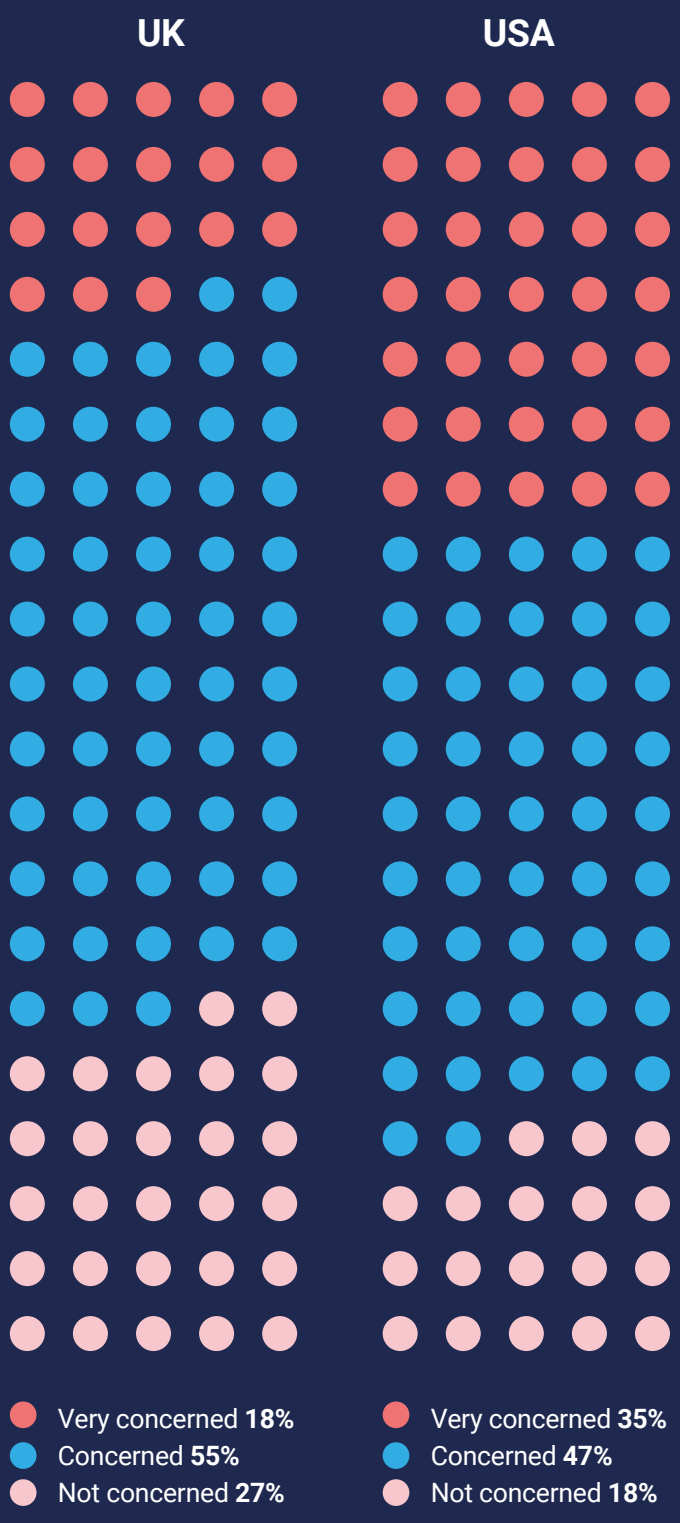
Among respondents who aren't yet consolidating security vendors, just **19%** felt that the process would improve their security posture. In contrast, **42%** of those who have begun a process of consolidation said they had seen an improvement in security posture as a result.

Wuchner believes this insight speaks to the challenge of change management for security professionals.

"They're typically being told to consolidate to save money and many fear what change will bring. The reality is different, but that doesn't necessarily make change any easier. When people are under enormous stress they can push back hard."

Effective change methodologies that address individual and cultural change have a part to play here, such as Prosci's ADKAR model[7].

To what extent are you concerned that security consolidation reduces your ability to mitigate cyber risk?



7 Prosci (2023), The Prosci ADKAR Model

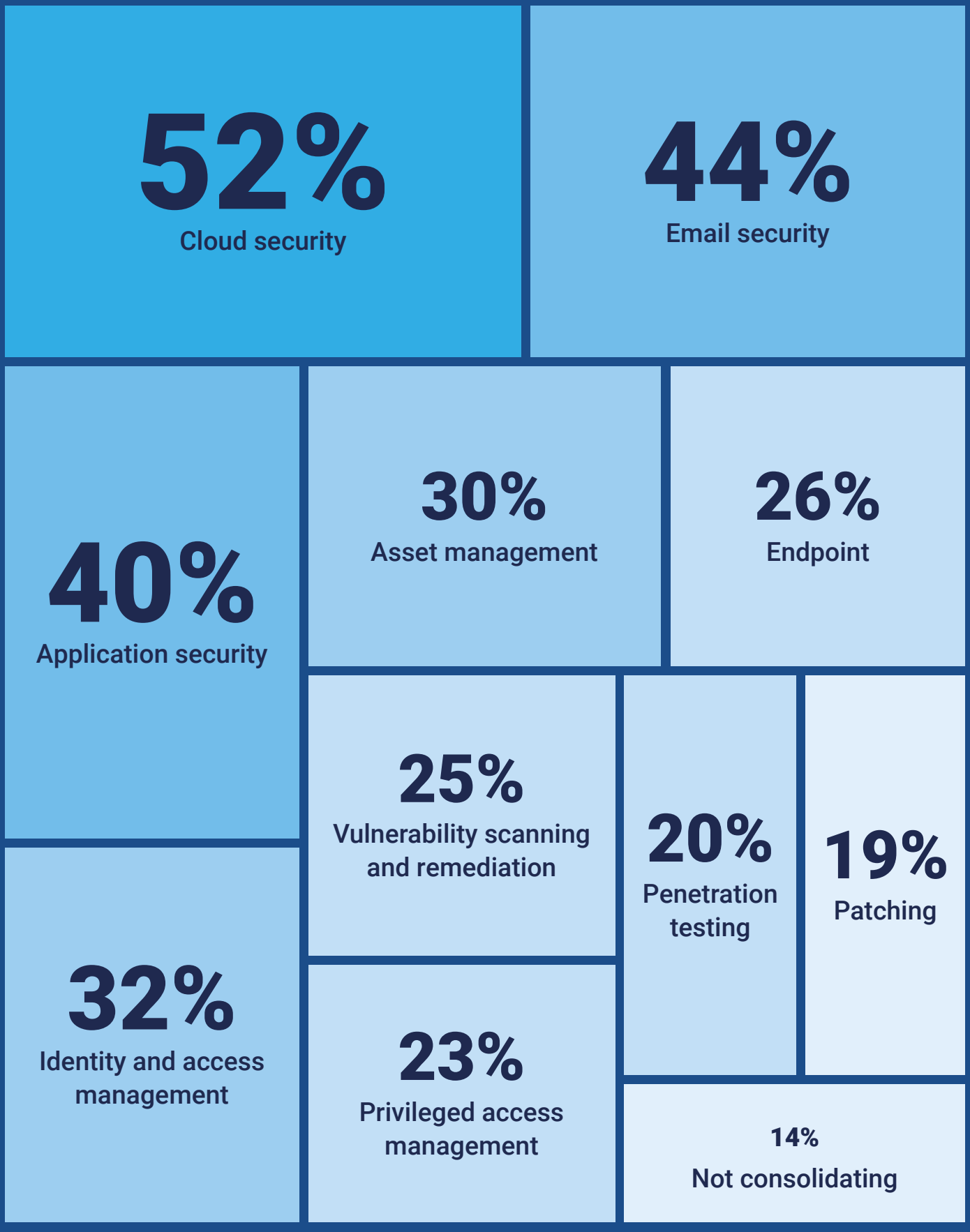
> **They're typically being told to consolidate to save money and many fear what change will bring. The reality is different, but that doesn't necessarily make change any easier. When people are under enormous stress they can push back hard.**
>
> Andreas Wuchner, Field CISO at Panaseer

With consolidation, much unease is caused by the unknown extent of what security controls may be lost. According to Wilcox, there should be no such unknowns if visibility of controls is sufficient.

"Professionals must ensure they have mapped the risks that exist, both with and without controls, and ensure appropriate controls coverage in the final state and during migration to that state. That's one of the capabilities of a Continuous Controls Monitoring solution. When we deploy the Panaseer CCM platform, we encourage the security team to declare a 'blame amnesty' – a period where everyone comes to terms with gaining full visibility of everything, including things that were hidden or unprotected, and no one has to fear that."

Our study found **86%** of organizations are currently consolidating security tools, the most common being in cloud security (**52%**), email security (**44%**) and application security (**40%**).

Which areas are you currently consolidating your security vendors and tools?



Teams know automation helps them apply finite resources better

Automation is even more widespread than consolidation, with **96%** of respondents automating at least one aspect of their cybersecurity. And while it's mostly monitoring (**53%**) and reporting (**42%**), there are signs that organizations are giving automated tools a more proactive role in upstream cybersecurity functions like incident response (**38%**) and threat hunting (**29%**), in line with cyber technology evolutions such as SIEM to SOAR and AV to EDR.

Automating processes naturally relates to the resource issue that security teams say they're suffering from. Or at least it should, says Wilcox.

> **"There's also the sense that the more you automate, the easier it becomes to draw away from the cycle of whack-a-mole. And going up the value chain with automation is important to reducing workloads and making a bigger difference to the organization."**
>
> Marie Wilcox, VP of Marketing at Panaseer and Board Director at CIISEC

"Organizations deal with lack of in-house resources by supplementing cyber teams with external people. A better option would be to automate what existing teams shouldn't be doing, such as manual reporting, and have them focus on the skilled roles they are trained for instead of having to bring in external resource," she explains.

"This can be a catalyst to getting on the front foot, leveraging automation to set priorities and enable proactive security measures."

Those who have embarked on security automation cite more efficient use of resources as the top benefit achieved from it (**57%** agree). Other leading benefits were improved decision making (**46%**), more accurate prioritization and freeing up employees to focus on different tasks (both **43%**) – all markedly higher than a reduced need for headcount (**30%**).

This is an encouraging picture that indicates an understanding of the strategic value at stake with automation; reflecting the central role it has in alleviating manual processes so that scarce human resources can be dedicated to the most meaningful security priorities.

"There's also the sense that the more you automate, the easier it becomes to draw away from the cycle of whack-a-mole. And going up the value chain with automation is important to reducing workloads and making a bigger difference to the organization," says Wilcox.

SECTION 3:

Regulation is coming – is it a tipping point?

A new wave of cybersecurity regulations are on their way, adding to the long list of requirements that security teams already contend with.

Recent US cybersecurity legislation such as the National Cybersecurity Strategy[8] mandate certain technologies like MFA and EDR, and assign greater responsibility and accountability for protecting "the digital ecosystem". Meanwhile, the Securities and Exchange Commission (SEC) has proposed new rules on cyber risk management, strategy, governance and incident disclosure[9] so investors can more accurately evaluate exposure to cyber risk.

The New York State Department of Financial Services has also strengthened existing regulations[10] to require more regular risk assessments, and assigns specific accountability to CISOs.

In Europe, the new EU Digital Operational Resilience Act (DORA)[11] will apply from January 2025 onwards and – like GDPR – affects more than just those businesses working within the EU. It directly affects financial institutions as well as ICT third-party service providers and sets a new bar for how these organizations must address ICT risk.

DORA explicitly states that security and ICT tools must be continuously monitored and controlled to minimize risk. It also holds the boards of financial services organizations legally accountable for ICT risk.

8 The White House (2023), *FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy*
9 Panaseer (2023), *SEC cybersecurity disclosure proposals: Get ready for public inspection of your cyber strategy*
10 US Department of Financial Services (2022), *Proposed Second Amendment to 23 NYCRR Part 500*
11 Panaseer (2023), *DORA: What security leaders need to know about the Digital Operational Resilience Act*

A warm welcome for regulations

It's clear from our research that incoming regulations promise to bring disruption, although a significant majority of respondents agree that adapting to them will be worth the effort – over and above simply meeting compliance. Among our respondents, **87%** forecast that new regulatory requirements will create a material impact over the next two years. Over one-third (**35%**) of these believe the impact will be "significant".

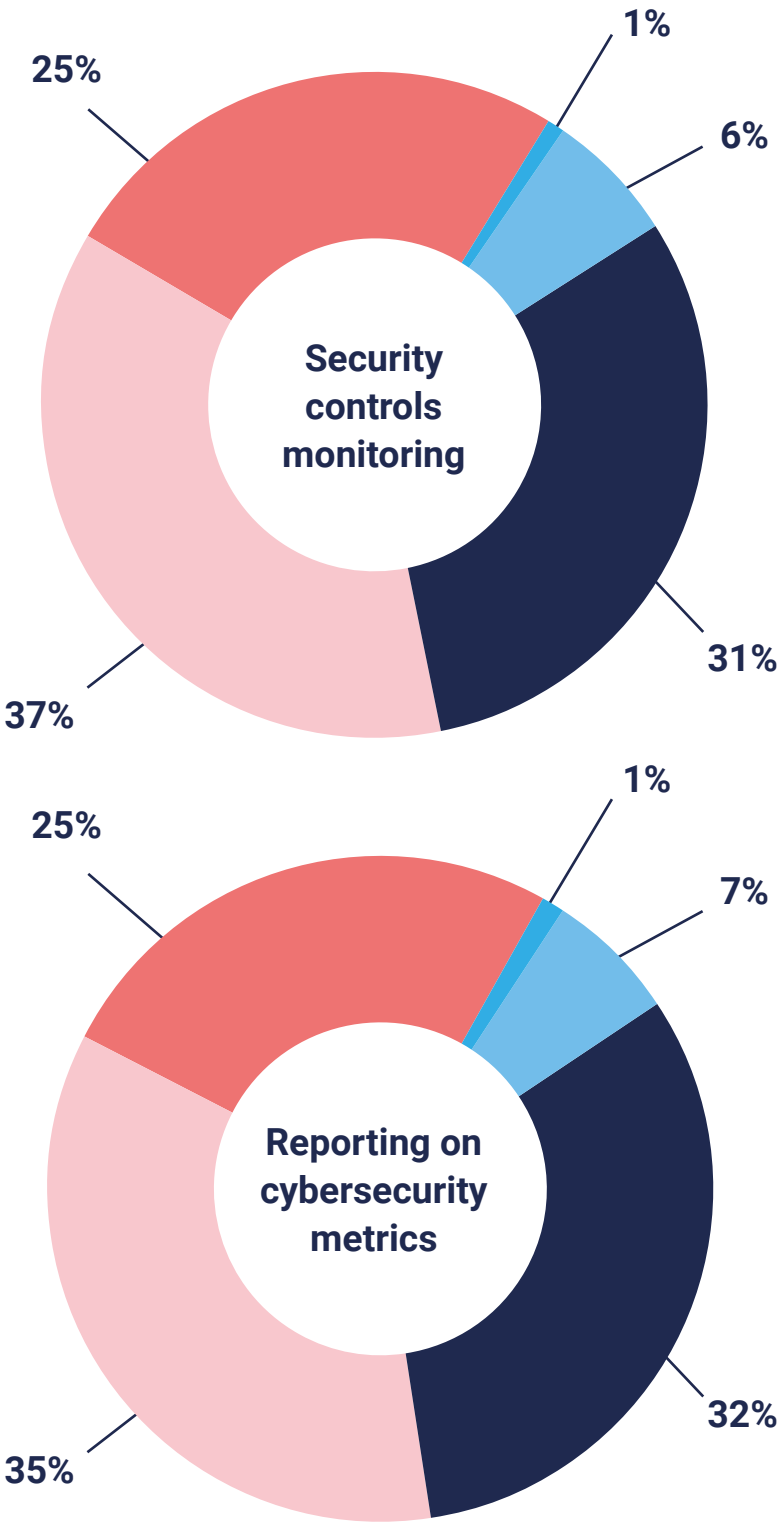
Despite the impact, three quarters (**74%**) believe there'll be a positive effect on their ability to manage cybersecurity posture, compared to just **3%** who are negative. The outlook is brightest in the US where **35%** of respondents anticipate an "extremely positive" effect compared to **12%** in the UK.

So why such a warm welcome for a potentially disruptive change? Wilcox puts it down to how security professionals feel about the specific regulatory details that ultimately result in better protected organizations.

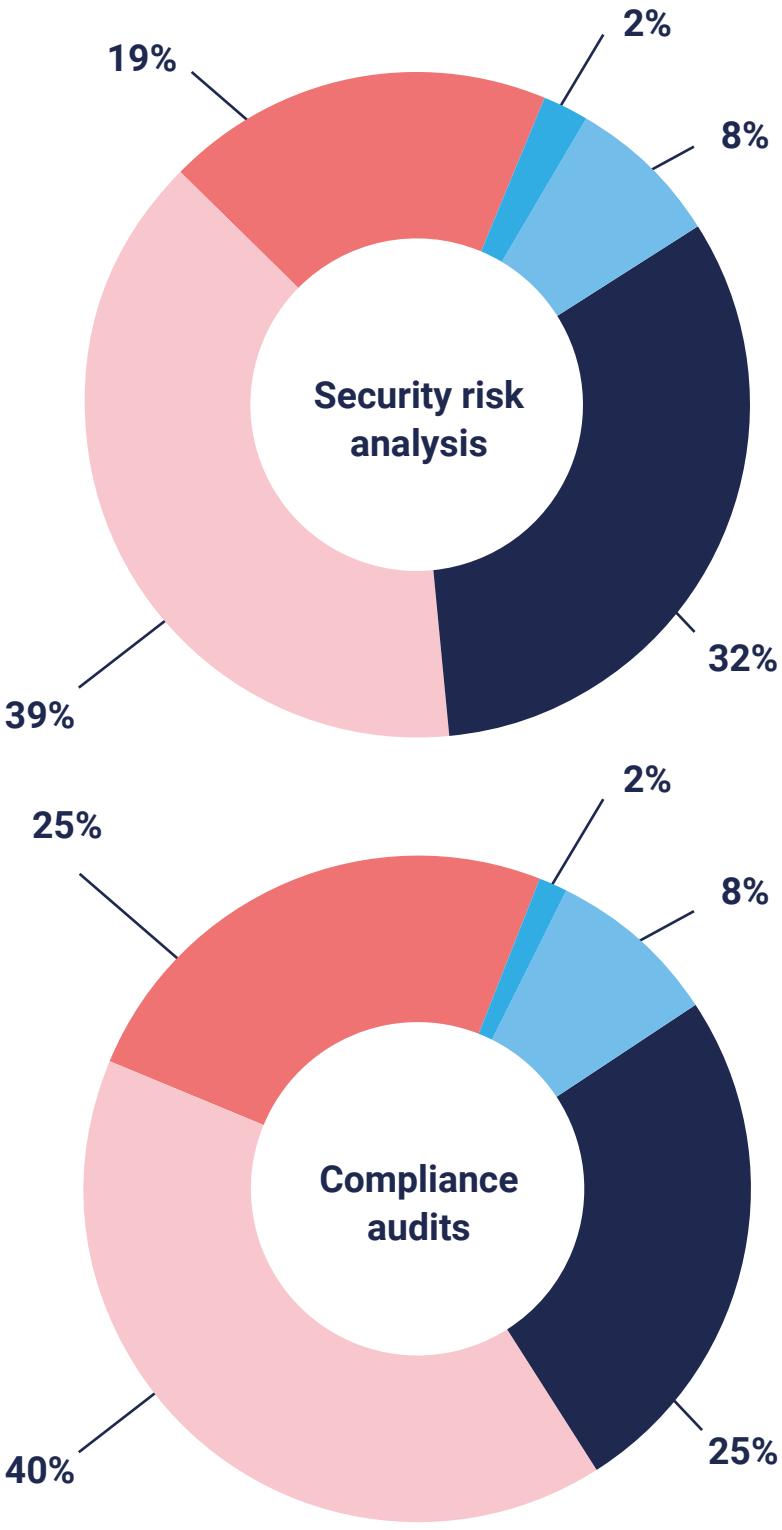
Key

- 1 - Significant decrease
- 2 - Decrease
- 3 - Neutral
- 4 - Increase
- 5 - Significant increase

How much will new cybersecurity legislation increase the burden on your security team in the following areas?



How much will new cybersecurity legislation increase the burden on your security team in the following areas?



"Regulation is inescapable and security teams can use this to make a strong case internally for the solutions they need to meet compliance," she explains.

"I think they also anticipate an impact from increased board accountability which will focus board members on the importance of cybersecurity and unlock more budget. This increased pressure on governance will benefit them individually as well as their employers."

Amid all this positivity, the process of achieving the new regulatory requirements will be tough. Our research found many expect it will add a substantial burden to their already overstretched security teams. Specifically, in terms of compliance audits and security controls monitoring, but also security risk analysis and reporting on cybersecurity metrics.

Even this won't stand in their way, however, as **82%** say they are confident in being able to meet deadlines for having everything in place.

Key

- 1 - Significant decrease
- 2 - Decrease
- 3 - Neutral
- 4 - Increase
- 5 - Significant increase

Evolving audit and compliance from manual point-in-time to automated and continuous

Automation will play a crucial role in dealing with compliance requirements. One specific area of DORA (article 9.1) mandates "continuously monitor(ing) and control(ling) the security and functioning of ICT systems and tools." More generally, automation will also alleviate the resource pressure of repetitive manual tasks and create the single source of objective truth that's needed for accurate cybersecurity decision making.

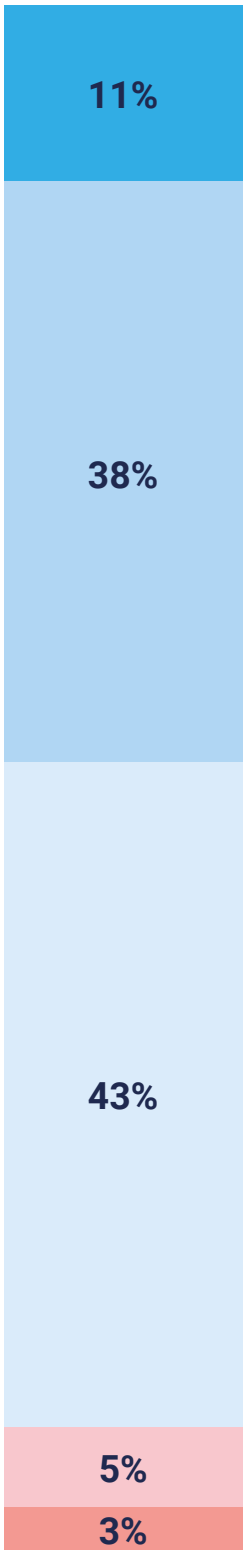
The work to achieve compliance will include an automation 'to-do' list for many organizations. Our research found that only **5%** of security leaders solely rely upon continuous audit using automation to demonstrate compliance, which indicates the scale of change that needs to occur. A much larger proportion (**43%**) who said they relied 'mostly' on this approach at present at least have a starting point to build from. This was smaller than the cohort (**49%**) who 'mostly' or 'solely' rely on manual, point-in-time audits.

Something needs to change, says Wuchner, and new regulations could be the impetus they need.

"For these organizations that lag behind on automation we are seeing the legacy of always putting people on problems rather than being truly data driven. It's only a matter of time until that whole mindset and culture changes," he says.

"The good news is that continuous, automated solutions can be implemented comparatively quickly and easily. The new regulations aren't super-urgent right now but it's imperative that the requirements are met."

Are your security audits automated or manual?



- **We solely rely on manual point-in-time audits**
- **We mostly rely on manual point-in-time audits**
- **We mostly rely on continuous audit using automation**
- **We solely rely on continuous audit using automation**
- **I don't know**

Clarity of accountability will focus minds on solutions

While the SEC and other US regulations don't go quite as far as the EU's DORA framework, the direction of travel is undoubtedly toward mandating greater board-level responsibility for managing cyber risk. This subtle shift could have seismic effects on how organizations prioritize ICT risk. At the very least, board members will want to better educate themselves about the threats and risks of their digital estate, and for that they will demand a streamlined mechanism for establishing the facts.

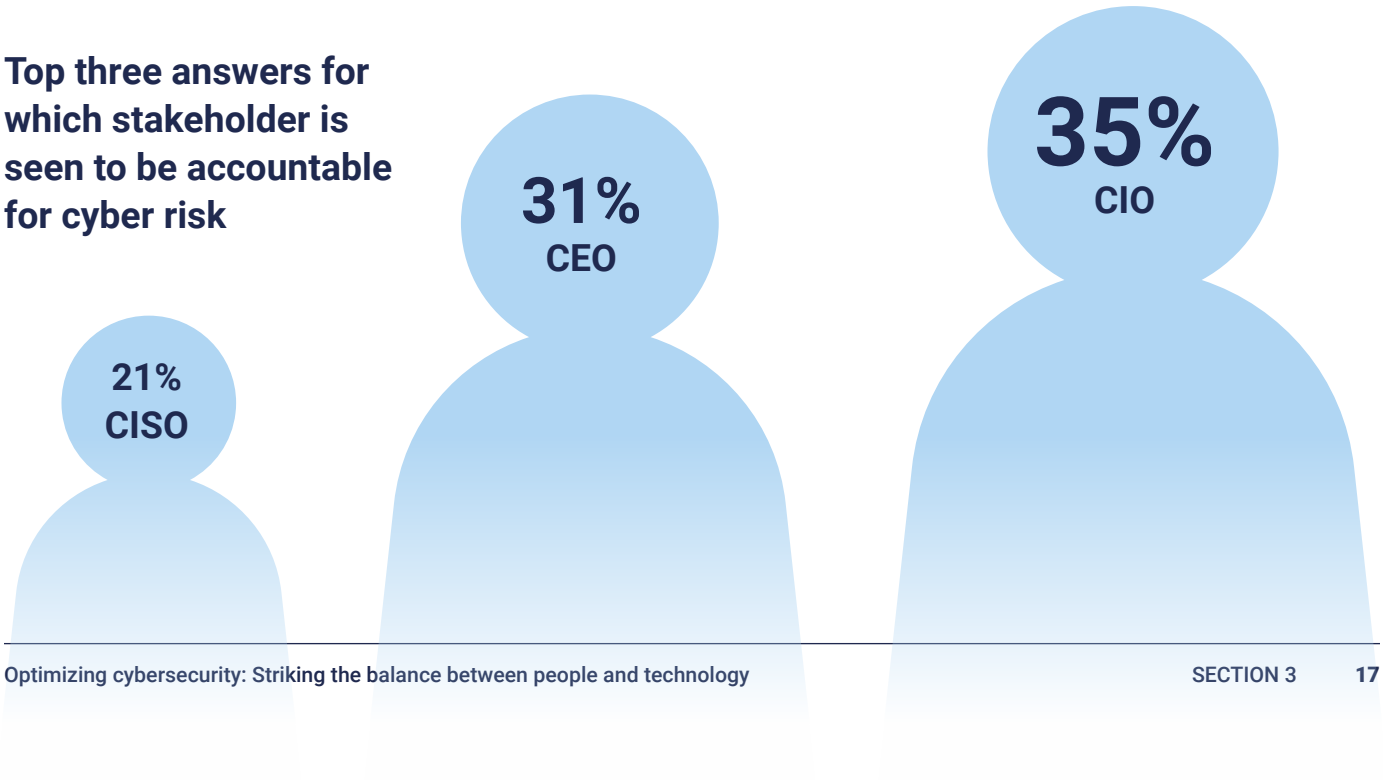
These stakeholders should be encouraged to learn that **80%** of security budgets have an explicit line item for monitoring the effectiveness of security tools; potentially a continuous controls monitoring (CCM) solution. This shows there is momentum towards automated solutions, and that organizations are already taking action that will help them comply with incoming regulations. These automated solutions bring certainty that's been lacking for too long, says Wilcox.

"Boards will want to be informed by the data, good or bad. They'll want certainty but that's very difficult unless you've achieved a single source of objective truth that no one can dispute. Getting at the truth of your security posture may be uncomfortable for some stakeholders but it's ultimately going to have to happen because of these compliance pressures and it will certainly be beneficial to security posture."

Our respondents reported a wide variety of roles as having overall accountability for cybersecurity risk at their organizations, with most identifying the CIO (**35%**), CEO (**31%**) or CISO (**21%**). Choosing who is responsible is the privilege of every organization, but the law will take over that choice in less than two years' time. By then, 100% of financial sector company boards (in the EU at least) will be held accountable, five times as many as the 18% in our research who named "the board" as being chiefly responsible for cybersecurity.

> **Getting at the truth of your security posture may be uncomfortable for some stakeholders but it's ultimately going to have to happen because of these compliance pressures and it will certainly be beneficial to security posture.**
>
> Marie Wilcox, VP of Marketing at Panaseer and Board Director at CIISEC

Top three answers for which stakeholder is seen to be accountable for cyber risk



Conclusion

Security teams have never been busier, though – as we've established in this report – many suffer from the 'whack-a-mole' tendency to focus on hitting what's in front of them; doing whatever it takes to get from one day to the next. This isn't sustainable even for organizations with immense resources.

However, change can be difficult and uncertain for cybersecurity teams – moving to greater automation and slimming down security toolsets comes with friction. The result is a fear to change mixed with an acceptance that these are the right changes to make. But that's what true risk management is for: to understand the likely impact of change so that risks can be understood and dealt with accordingly. Security professionals need to grasp this to help their organizations be successful.

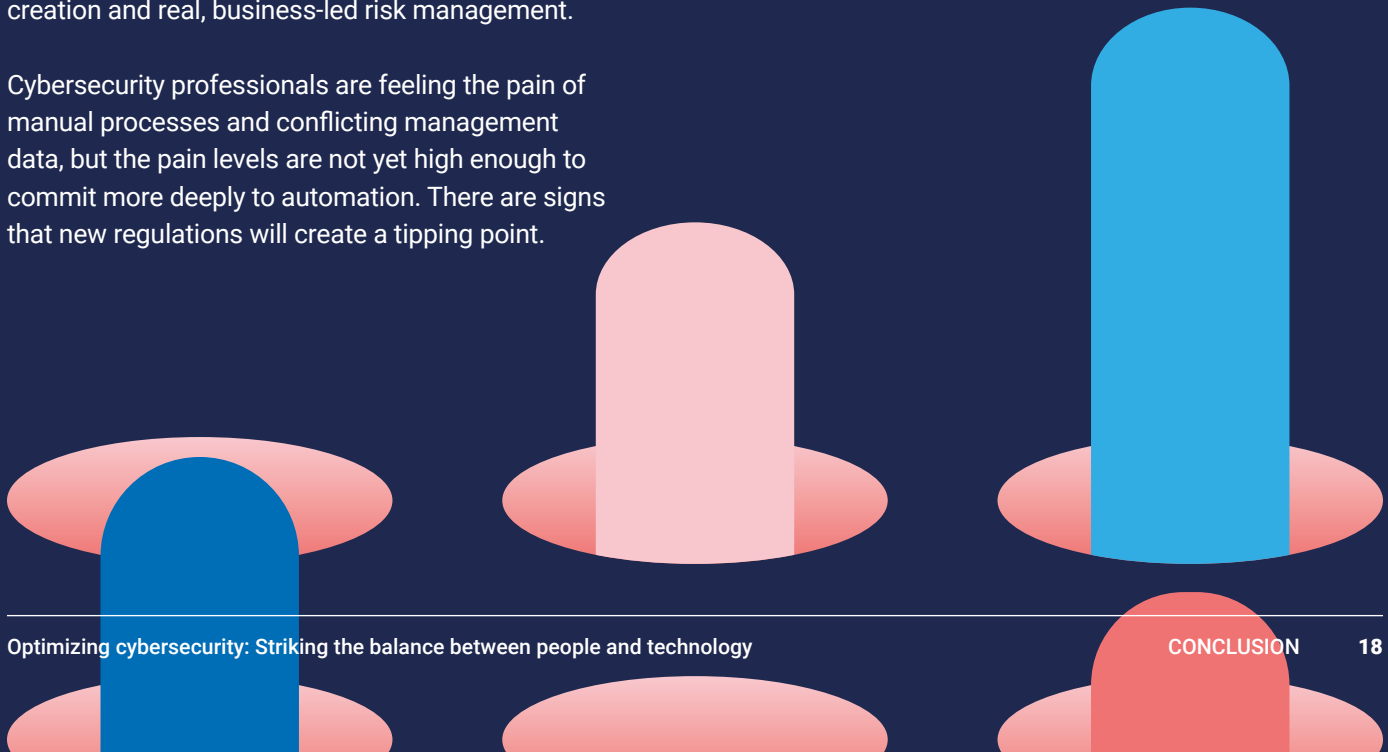
Much of our research underlines that automation holds the key. And while organizations are automating more security functions, there is some distance left to travel on creating trusted visibility into security controls, the risks they control and the value they both create and protect. This requires automated solutions like Continuous Controls Monitoring (CCM). Without it the major driver for security automation continues to be operational resilience – efficiency, cost control, simplification – rather than value creation and real, business-led risk management.

Cybersecurity professionals are feeling the pain of manual processes and conflicting management data, but the pain levels are not yet high enough to commit more deeply to automation. There are signs that new regulations will create a tipping point.

Regulation represents the most important opportunity of all; the impetus security teams need to break the old cycle. Why? Because it will shift the responsibility for resilience and security onto those with the most power to bring about change. It will mean the board learning what it takes to automate and consolidate; finding solutions that create a superior security posture with the most efficient use of resources.

Automation of the kind exemplified by CCM is increasingly recognized for its strategic value. CCM strengthens an organization's security posture by automating monitoring, reporting and audit processes, providing real-time insights and facilitating proactive risk management. It does this by evaluating the effectiveness of an organization's security tools and processes on an ongoing basis to identify potential control gaps and weaknesses.

To capitalize on the potential benefits that automation can bring, security leaders need the space to stop fighting fires so they can focus on strategic changes. This will help them find the right blend of people and technology, and ease the pressure on their overworked security teams.



Methodology

The primary research findings in this report are taken from a Dynata survey conducted in May 2023 and published here for the first time. The survey, commissioned by Panaseer, was carried out among 402 cybersecurity decision makers and practitioners. Respondents were segmented equally across the US and UK with approximately 50% at organizations between 1,000 and 5,000 employees, and 50% at 5,000+ employee organizations.

About Panaseer

Panaseer is an enterprise cybersecurity automation and data analytics company that helps organizations adopt proactive security posture management by ensuring security controls are fully deployed and working effectively – maximizing their security investments and resources through better prioritization. It gives CISOs a continuous measure of their security posture, enabling them to provide trusted updates to senior leaders, board members and regulators.

Panaseer's Continuous Controls Monitoring platform gives a complete, trusted view of security controls, with metrics and measures guidance aligned to best practice frameworks. With $262 billion spent on cybersecurity tools in 2021, CCM means organizations can do more for less by getting the most out of their existing security investments.

Automated security posture management

Continuous Controls Monitoring for enterprise security