panaseer

2023 Security Leaders Peer Report

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.

Mark Ashworth

Information Security Lead at Panaseer

Mark has over 20 years' experience in IT and Information Security and has worked in both enterprise and startup companies.

Contents

Introduction 3

Key findings 4

SECTION 1:
The extent of security control failures and their impact on organizations 5

SECTION 2:
Control of tools, not tooling itself, demands greater priority 7

SECTION 3:
The human impact of security limitations and frustrations 9

SECTION 4:
Almost two-thirds of security teams' time now spent on manual reporting 12

SECTION 5:
Monitored security control metrics are too limited and too few 14

SECTION 6:
Heightened interest in security automation solutions 17

Conclusion 18

Methodology 19

Introduction

The Panaseer Security Leaders Peer Report has become an annual opportunity to understand the concerns and constraints facing CISOs and other senior cybersecurity leaders through the lens of current and emerging market challenges.

Now in its third and most wide-ranging edition, this 2023 report returns to key themes in security controls coverage and monitoring to chart their progress over time. Coming as it does after successive **pre-pandemic (2019)** and **mid-pandemic (2022)** editions, it also stands as a post-pandemic picture of cybersecurity sentiment across a range of priorities.

As cyber-attacks continue to impact enterprises, we look at the scale of preventable breaches and what can be done about them. Adding to their arsenals of existing security tools may not be the way forward – we examine how security leaders are instead addressing security controls coverage gaps and preventing control failures from becoming security incidents.

For the first time in a Security Leaders Peer Report, we also examine how security teams are personally impacted by working in a stressful, high-pressure environment. This reveals an intimate view of what frustrates security professionals with their roles in general and confronting the security controls challenge in particular. We also explore what, if any, influence this has on staff churn and the consequences that may arise.

> **"Security leaders want to achieve things and make progress. But there are obstacles everywhere. As well as daily threats there is a constant demand for reporting from different stakeholders, and this is driving them to get greater control of their environment; to measure more so that they can manage it."**
>
> Andreas Wuchner, Advisory Board Member and Field CISO at Panaseer

Key findings

Control failure remains a major preventable cause of breaches.

79% of enterprises have experienced cyber incidents that should have been prevented with current safeguards. Around **9 out of 10** security leaders state that failure of an expected control is the primary reason for breaches.

The tools are there. The issue is ensuring controls are deployed and properly configured.

Most enterprises own the essential security tools to protect against breaches. **82%** of respondents agree that monitoring and addressing expected controls failure and risk would likely have a bigger impact on their security posture than buying additional tools providing more controls.

Security leaders are hugely frustrated by security tools and data.

The inability to continuously measure enterprise-wide security posture and identify control failures is ranked first among senior cyber professionals' frustrations. Tool and data frustration is cited as a bigger reason for staff churn than demands for higher salary and greater seniority.

'Too much time' is spent on reporting as resources become scarcer and reporting burden rises.

The average security team dedicates **59%** of their time to manual reporting tasks – a **9%** increase on the previous year's research. **70%** of security teams now spend more than half of their time on these tasks. Lack of internal resources is cited as the biggest reason for control failure by leaders.

Uncertainty reigns over what constitutes a high-impact security metric.

Security leaders are unsure of which metrics to monitor for best effect and most do not have the resources to help them do it. This affects their ability to evidence the impact of security investments, get the most accurate view of their security posture, and to benchmark against peer organizations.

Interest in CCM reaches its highest level.

88% of security leaders are likely to implement a Continuous Controls Monitoring (CCM) platform in the next two years. That compares to **79%** who said the same in our 2022 study.

SECTION 1:

The extent of security control failures and their impact on organizations

Avoidable security control failures continue to blight organizations, with four out of five security leaders saying they've been surprised by a security incident which evaded a control thought to be in place to stop it. This year's figure shows a slight improvement (**79%** vs. **82%** in 2022) though the rate remains uncomfortably high. Overall, **42%** of security leaders say this has happened on more than one occasion.

Security leaders surprised by a security incident evading a control they believed would stop it

2023: **79%**

2022: **82%**

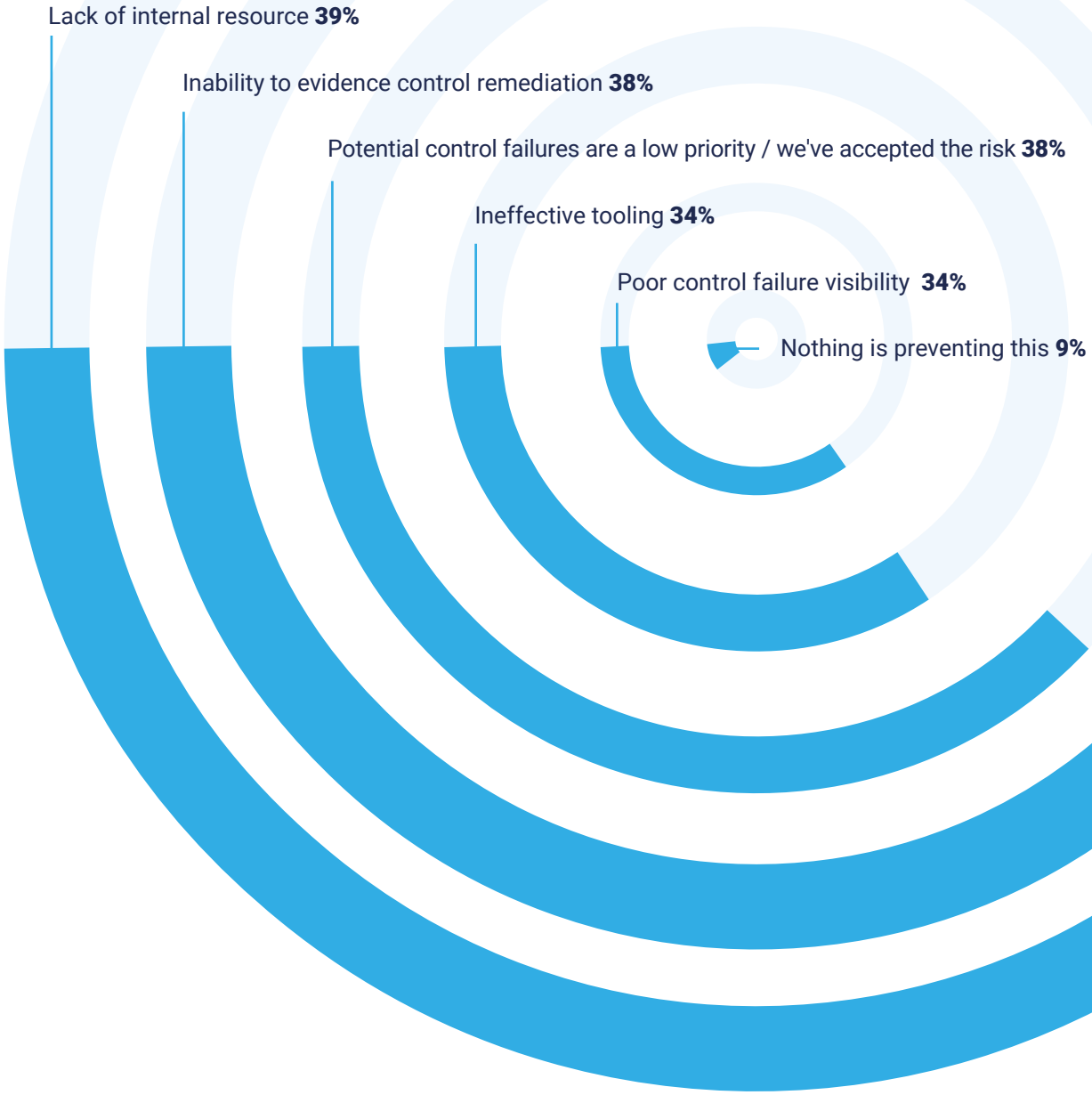
This is cause for concern, as **88%** of security leaders agree that control failures and gaps are the primary reason for cyber breaches. This position is broadly consistent across industry sectors.

Overall, only **44%** of organizations are extremely confident in their ability to continuously measure their technical control gaps, which signals there's more work still to be done. When the whole group was asked what prevents them from having a high degree of confidence that no failures or gaps exist in expected security controls, the most common answers were a lack of internal resources and an inability to evidence control remediation.

Do you agree that control failures and gaps are the number one reason for breaches?

Well over a third of security leaders (**38%**) say they have accepted the risk of potential control failures or deem it a low priority. This could be because of the high number of incidents or vulnerabilities that teams face, which forces them to be more reactive rather than proactive and accept a high level of risk in their security posture.

Reasons preventing security leaders having high confidence of no failures/gaps in expected security controls



SECTION 2:

Control of tools, not tooling itself, demands greater priority

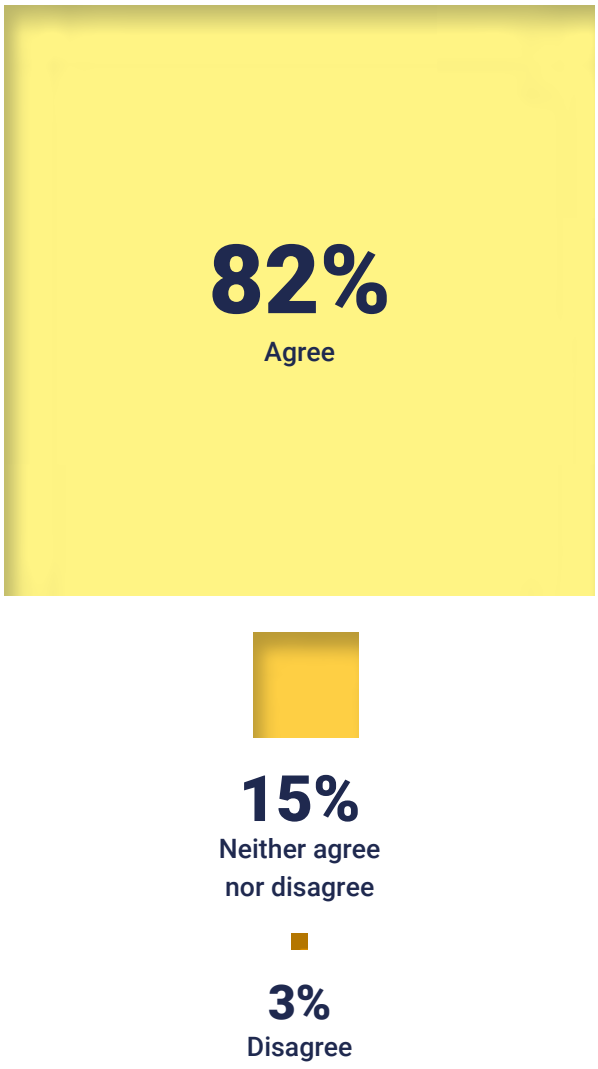
Previous editions of the Panaseer Security Leaders Peer Report asked how many security tools are typically used by organizations – finding that more than 75 or even 100 tools was not uncommon. In preparing our research for this edition, we accept the premise that enterprises are typically working with a high number of different security tools and vendors. Also, that almost all attacks can be prevented by properly implementing basic cyber hygiene. Microsoft asserts, in its "cybersecurity bell curve", that **this applies to 98% of cyber-attacks.**[1]

We assume, therefore, that organizations typically own the required tooling and have implemented the controls to prevent most breaches and incidents. Our research indicates these resources are not being correctly managed, leading to gaps in controls coverage and effectiveness.

It is illuminating to find that **82%** of security leaders agree that monitoring and addressing expected controls failure and risk (i.e. their current environment) would have a bigger impact on their security posture than buying additional tools that provide more controls. Barely **3%** disagree with this statement. This demonstrates the awareness among CISOs and other senior cyber professionals that more tooling is not the route to better security.

Also, more security leaders (**32%**) believe that ensuring expected tooling and controls are fully deployed and active has the greatest impact on improving posture than those who cite hiring more talent (**26%**), faster patching (**25%**) and increased internal training (**20%**) as having the greater impact.

Would monitoring and addressing failure of your existing controls and controls risk have the bigger impact on your security posture vs. buying more tools?



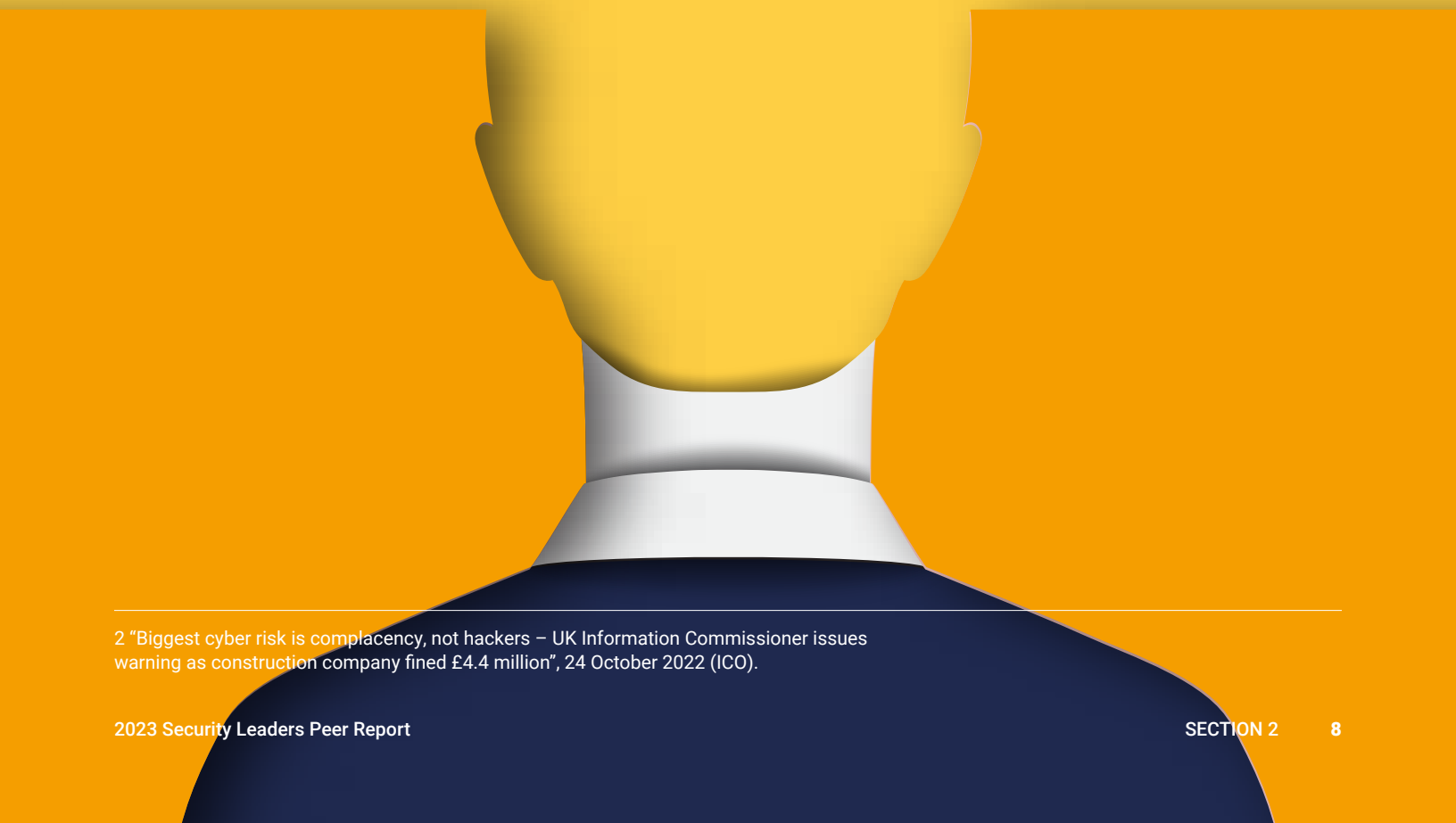
1 Digital Defense Report, 2022 (Microsoft)

And they are right to prioritize this low-hanging fruit, not only to improve security posture and stop preventable breaches but also to mitigate the kind of scrutiny and punishment being meted out by regulators. One example of this is the £4.4m fine issued by the UK Information Commissioner's Office (ICO) in October 2022 to a large UK-based construction resourcing company – following a breach that exposed the personal data of up to 113,000 employees.

The fine was the fourth largest ever levied by the ICO and related to failures that were contrary to the company's own policies and controls, i.e. failing to **"follow-up on the original alert of suspicious activity, (using) outdated software systems and protocols, … a lack of adequate staff training and insufficient risk assessments."**[2]

It's hardly surprising, then, that **37%** of security leaders say that within the next two years they are very likely to implement a solution to measure and advise on security control effectiveness across their entire organization. We examine this in more detail in section six.

> **"Security leaders have to know their security stack; what tools they have, their utilization and how they interconnect. This impacts the data you surface and what you can do with it to improve prioritization. Complexity is your enemy, so the focus is on keeping things simple and leveraging what you have to achieve an end-to-end view."**
>
> Mark Ashworth, Information Security Lead at Panaseer



2 "Biggest cyber risk is complacency, not hackers – UK Information Commissioner issues warning as construction company fined £4.4 million", 24 October 2022 (ICO).

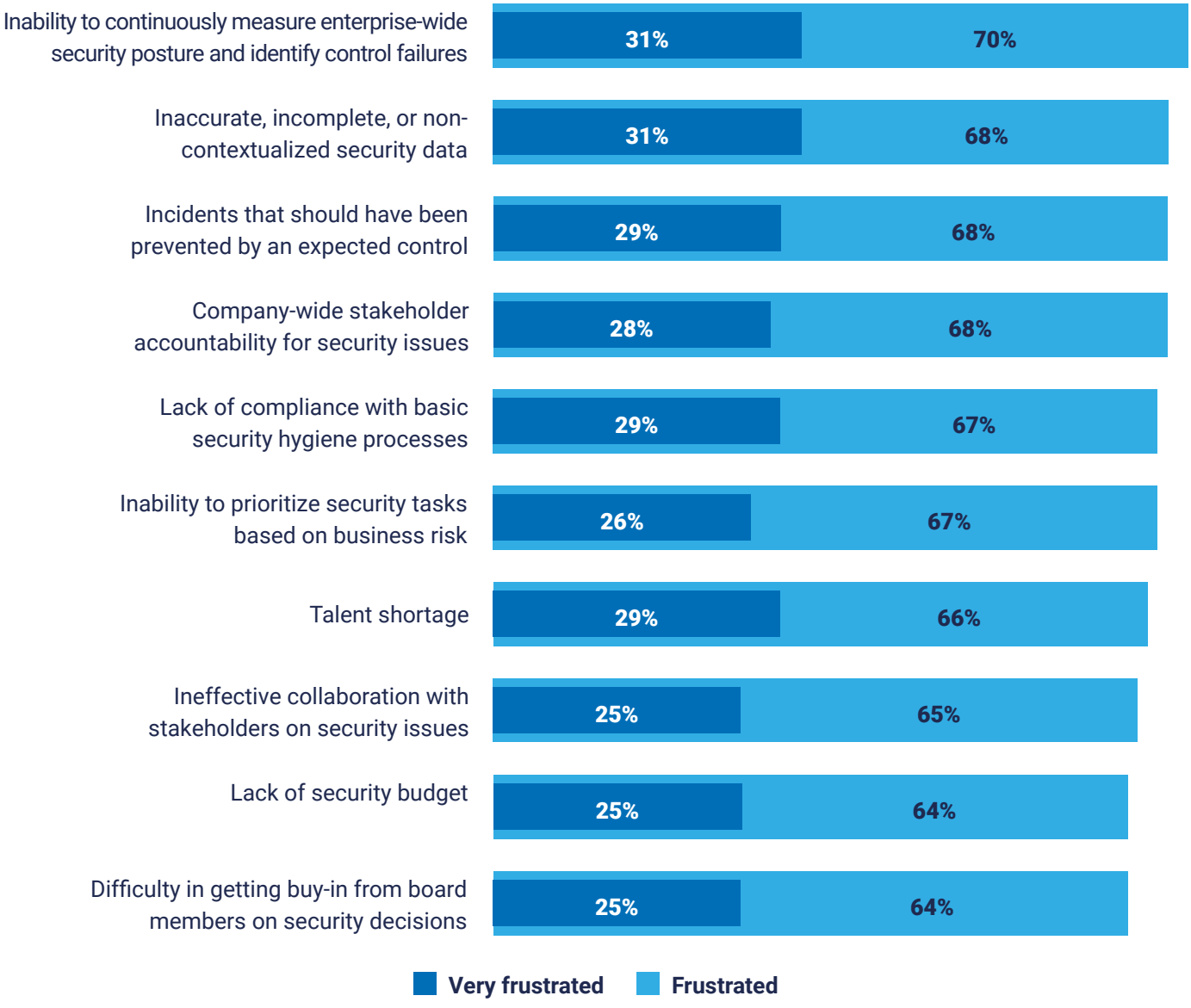
SECTION 3:

The human impact of security limitations and frustrations

To get a deeper understanding of the challenges facing security leaders, we asked what they find most frustrating about cybersecurity in their organization. The inability to continuously measure enterprise-wide security posture and identify control failures came top — **31%** stated this is "very frustrating" and a total of over **70%** said it is frustrating. Among C-suite security leaders the figure is **76%**.

Similar exasperations ranked almost as high, such as incidents that should have been prevented by an expected control (**68%** frustrated). This group of factors all came out as more frustrating to security leaders than more general complaints such as talent shortages (**66%**), lack of security budget and issues obtaining board member buy-in (both **64%**).

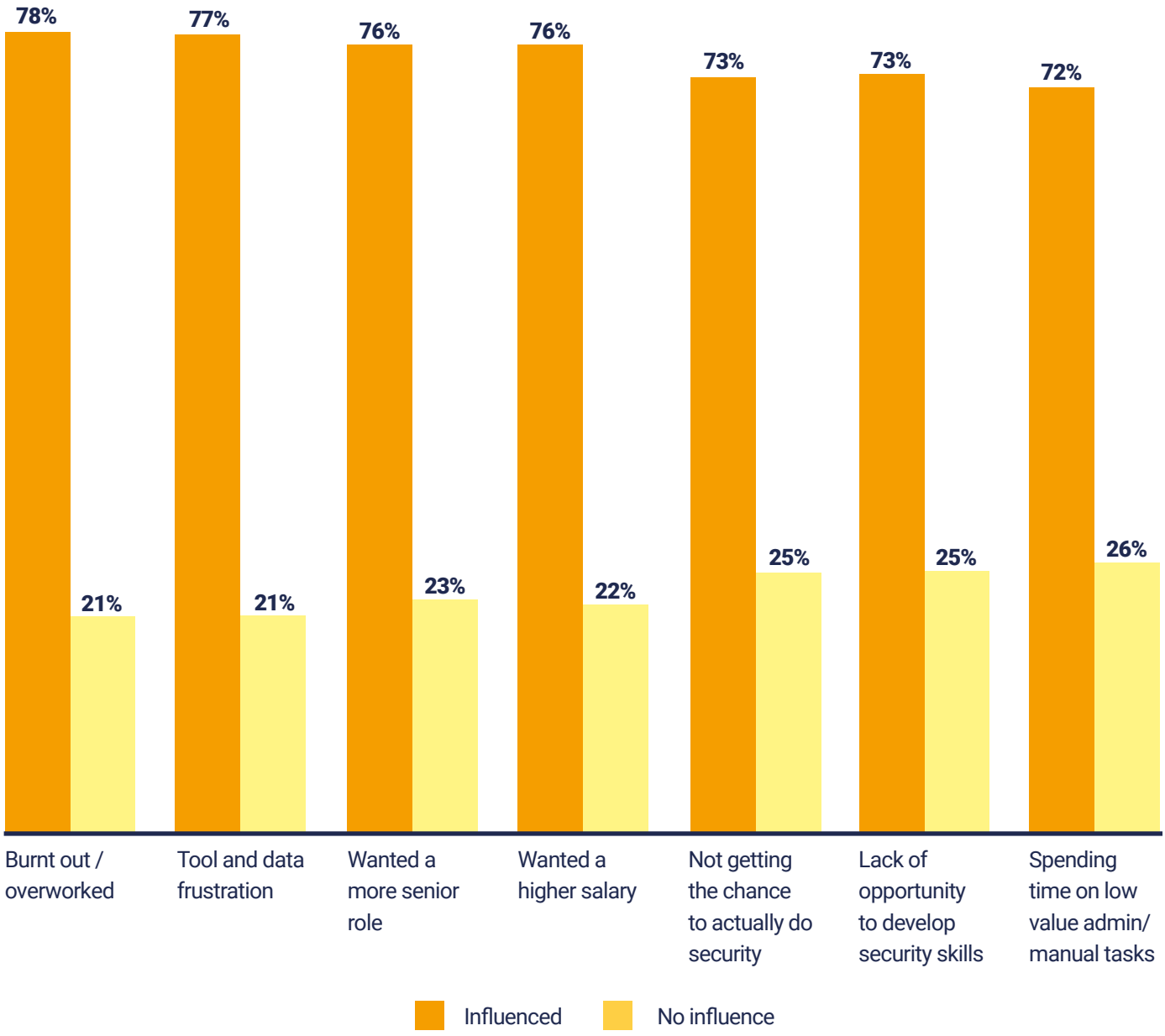
What's most frustrating about cybersecurity in your organization?



Senior cybersecurity practitioners are not alone in venting about irritations and obstacles that disrupt their personal effectiveness. But the acid test comes when these factors compromise staff wellbeing and contribute to employee churn. It appears that security leaders think that tool and data frustrations can be even more influential in staff resignations than the desire to get paid more or move to a more senior role.

Indeed, tool and data frustration (i.e. volume of alerts, false positives, lack of correlation across multiple tools) was the second most influential factor in employee churn. It came after employee burnout, which was cited by **78%**.

Factors influencing security team resignations in preceding 12 months



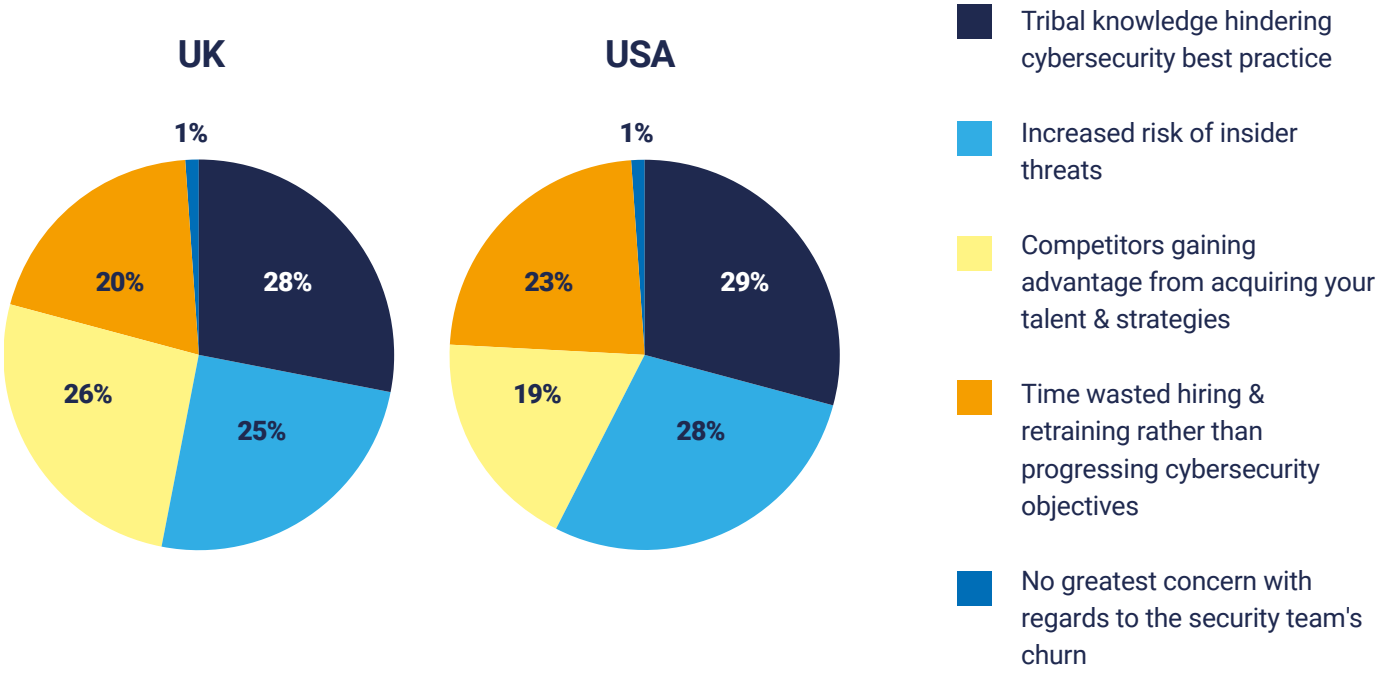
Spending time on low-value admin/manual tasks (**72%**), not getting the chance to actually do security (**73%**) and lack of opportunity to develop security skills (**73%**) were also seen as having a big impact on employee churn. Introducing automation would help address the root of these issues by eliminating manual tasks, enabling security professionals to apply themselves more usefully.

Employees leaving due to avoidable reasons is particularly frustrating for CISOs in the context of a cybersecurity skills shortage, where around **3.5m positions worldwide are unfilled.**[3] There are significant impacts associated with losing skilled team members. The biggest concern among security leaders (**29%**) is the loss of "tribal knowledge" hindering their internal best practice and weakening security posture.

Tribal knowledge – the unique intelligence bespoke to a small group – holds greatest value in the vacuum of undocumented and incomplete processes, so this concern betrays a heavy reliance on individuals to hold the organization's cybersecurity posture together.

> **"Security professionals tend to be relatively well paid, so it isn't surprising that churn is down to other factors. Among my own peers, several have left positions because they didn't have the tools to do their job. In an age of automation, having to work on endless spreadsheets is – for people who are technical and creative thinkers – an unbearable waste of their time."**
>
> Mark Ashworth, Information Security Lead at Panaseer

What is your greatest concern with regards to the security team's churn?

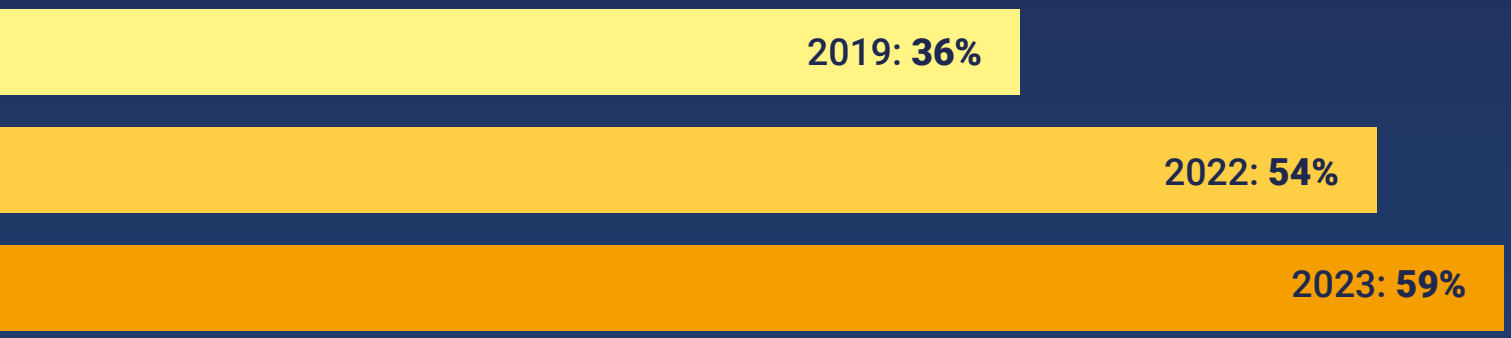


3 "Cybersecurity jobs report: 3.5m openings in 2025", 9 November 2021 (Cybersecurity Ventures)

SECTION 4:

Almost two-thirds of security teams' time now spent on manual reporting

On average, how much of their time do security teams spend manually producing, formatting and presenting data?



As enterprise security leaders grapple with the challenge of security controls monitoring, they do so with more and more of their resources used up elsewhere. The reporting burden has now reached unprecedented levels with the average security team spending **59%** of its time on manual reporting tasks. In 2022, this figure was **54%**, and in 2019 it was **36%** – a significant increase over the last few years.

Security teams come under reporting pressure from multiple angles including regulatory compliance questionnaires, intensifying board-level interest, and even sales engagements. But this does not explain the increased strain of manual reporting, which has a negative effect on other security priorities by reducing the amount of time spent on remediation and creative problem solving.

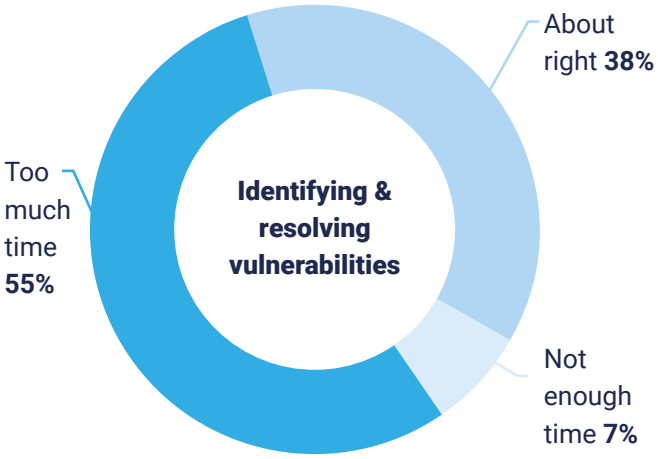
Despite this, **46%** feel their current time allocation for reporting is "just right". This strongly indicates a lack of awareness of the technology solutions to address this issue.

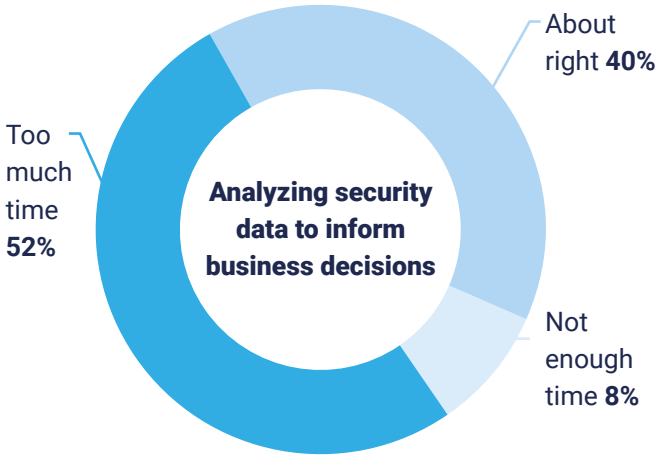
Without greater automation, this issue is unlikely to improve, given the added context of a cybersecurity skills crisis and increasingly complex enterprise technology environments. If security control reporting, monitoring and other tasks are done manually, then they are likely incomplete, prone to error and very inefficient to manage – a poor starting point from which to optimize security posture and prevent breaches.

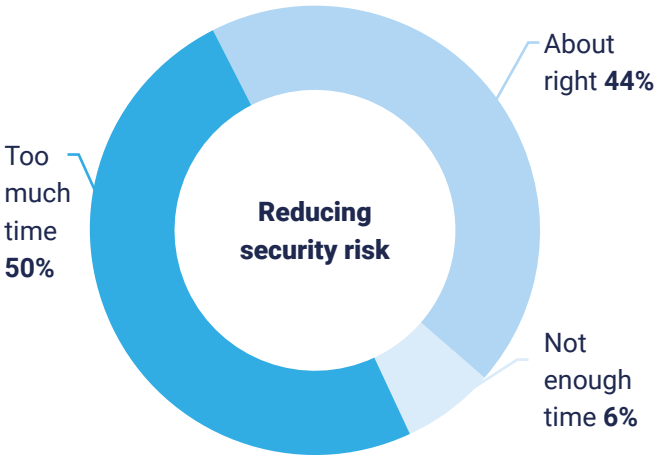
With limited resources, security leaders think their teams are having to spend too much time on certain aspects of security. This is particularly pronounced in areas such as identifying and resolving vulnerabilities, analyzing security data to inform business decisions, and reducing security risk.

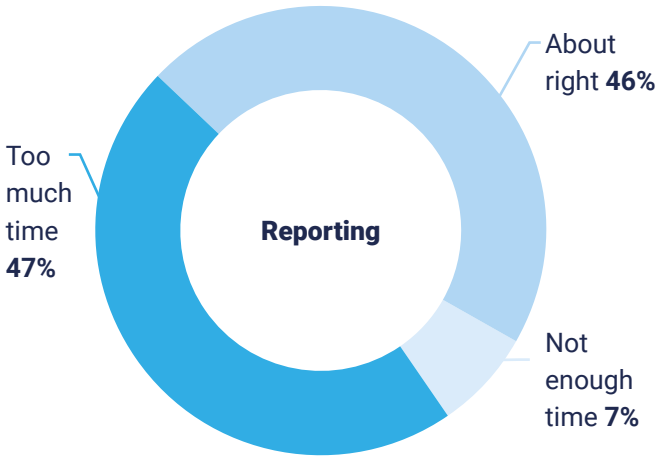
> **"Over the last four years, increased scrutiny on the value and performance of security investments has exacted a heavy price in reporting time. The automation, metrics and risk management to cope with it is still not mature enough in many enterprises."**
>
> Andreas Wuchner, Advisory Board Member and Field CISO at Panaseer

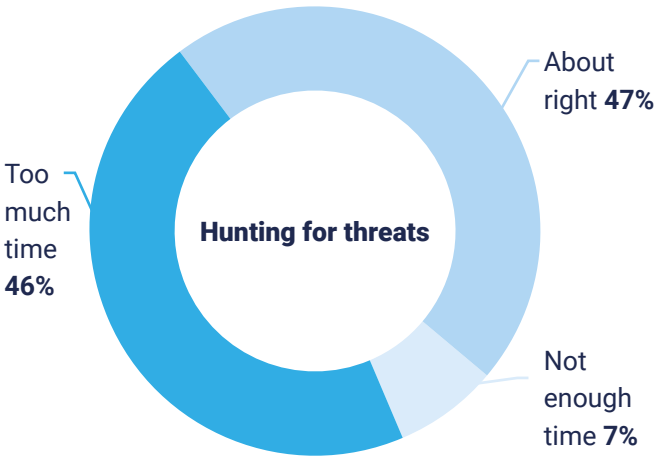
How much time do you feel your security team spends on the following aspects of security?

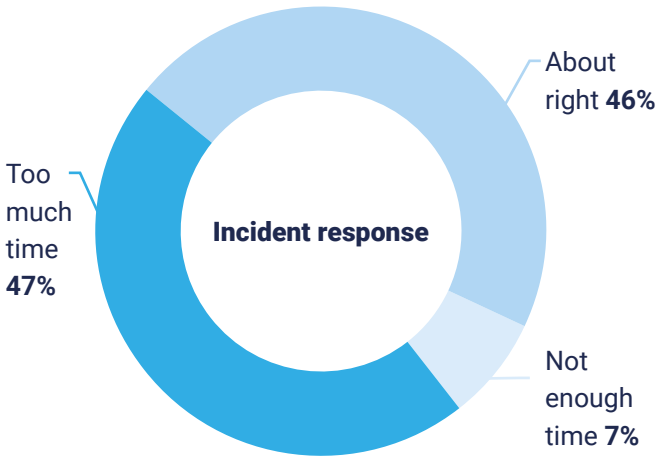












SECTION 5:

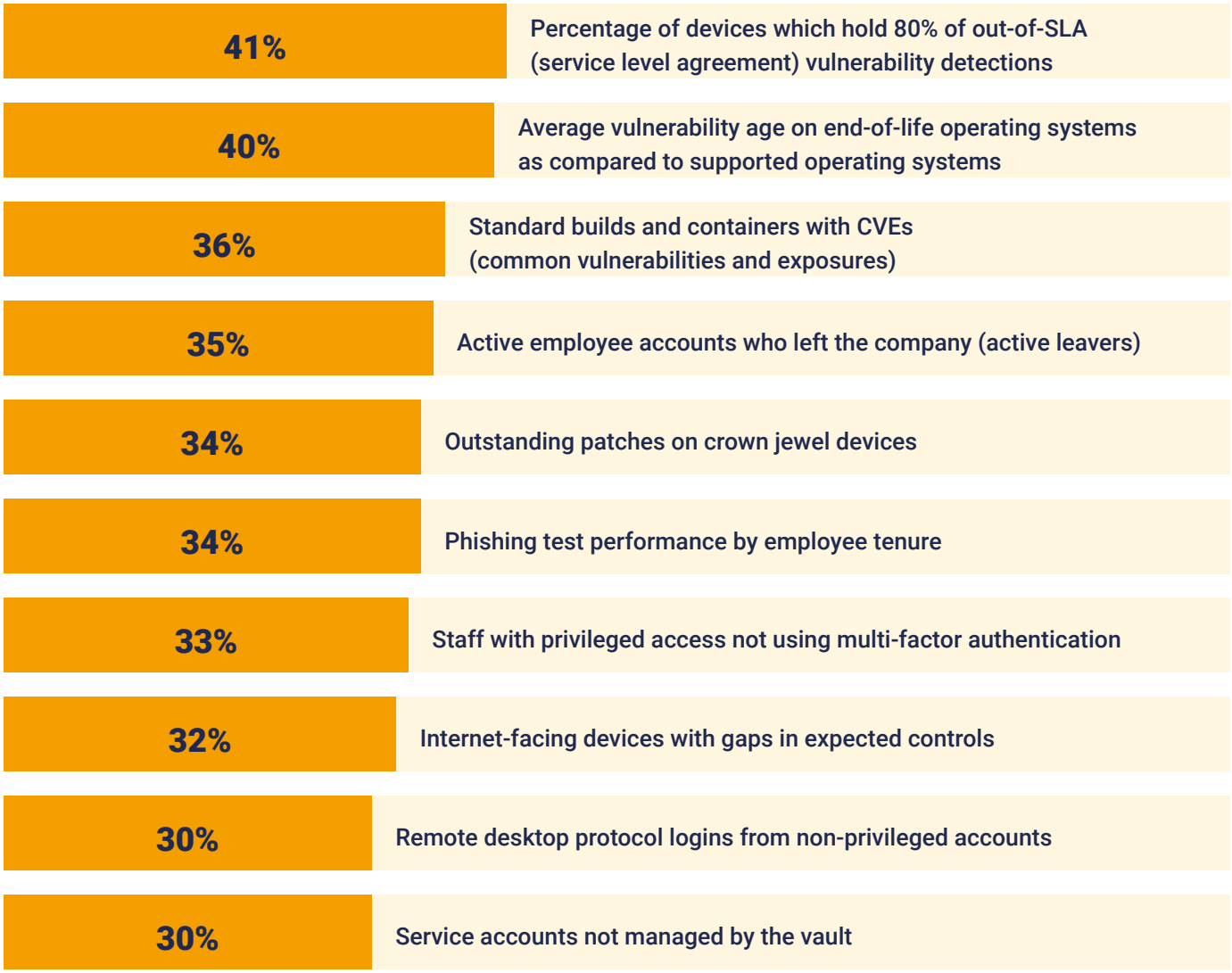
Monitored security control metrics are too limited and too few

Despite clearly grasping the importance of continuous controls monitoring and optimization, security leaders appear uncertain about how to measure and improve their security posture.

As part of our research, respondents were asked for their views on a group of security metrics. Based upon Panaseer's experience, these metrics are highly pertinent to the prevention of security incidents and are associated with organizations that have a mature approach to security posture management.

Respondents were asked to verify which of these they continuously measure and, for those they do not measure, how valuable it would be to continuously measure them.

Which security metrics do you continuously measure?



Each organization requires security controls that are geared to their unique risk management strategy, so readers are invited to draw their own conclusions from our findings. However, while the high level of perceived value in the metrics was expected, we were surprised by the relatively low adoption of continuous measurement of metrics in general. By these figures, many organizations lack some of the critical security metrics one would associate with a mature security team.

It is also important to understand other factors that may explain the absence of security metrics, besides a lack of relevance to the organization's risk management posture.

For example, according to our research, organizations often don't know the most impactful security metrics to measure. Only **43%** are highly confident they are continuously evaluating best practice security metrics specifically aligned to their organizational size and industry. Of the remainder, **47%** simply don't know the right metrics to monitor and **51%** don't have the resources to help them do it.

A lack of best practice metrics can often be alleviated by matching security practices against peer organizations and over **99%** of our sample is actively engaged in trying to benchmark their security metrics, policies and standards. However, nearly three-quarters (**72%**) admit they are not absolutely satisfied with their ability to do so currently. It is hardly surprising, therefore, that **93%** would find measurement capability benchmarks of high value and **94%** would find policies and standard benchmarking of high value.

> **"Security is a moving target, so uncertainty around which control metrics to measure is inevitable. To be 100% sure smacks of complacency, or suggests the organization is at a standstill. The challenge remains to improve controls coverage in the right areas in response to changing demands."**
>
> Mark Ashworth, Information Security Lead at Panaseer

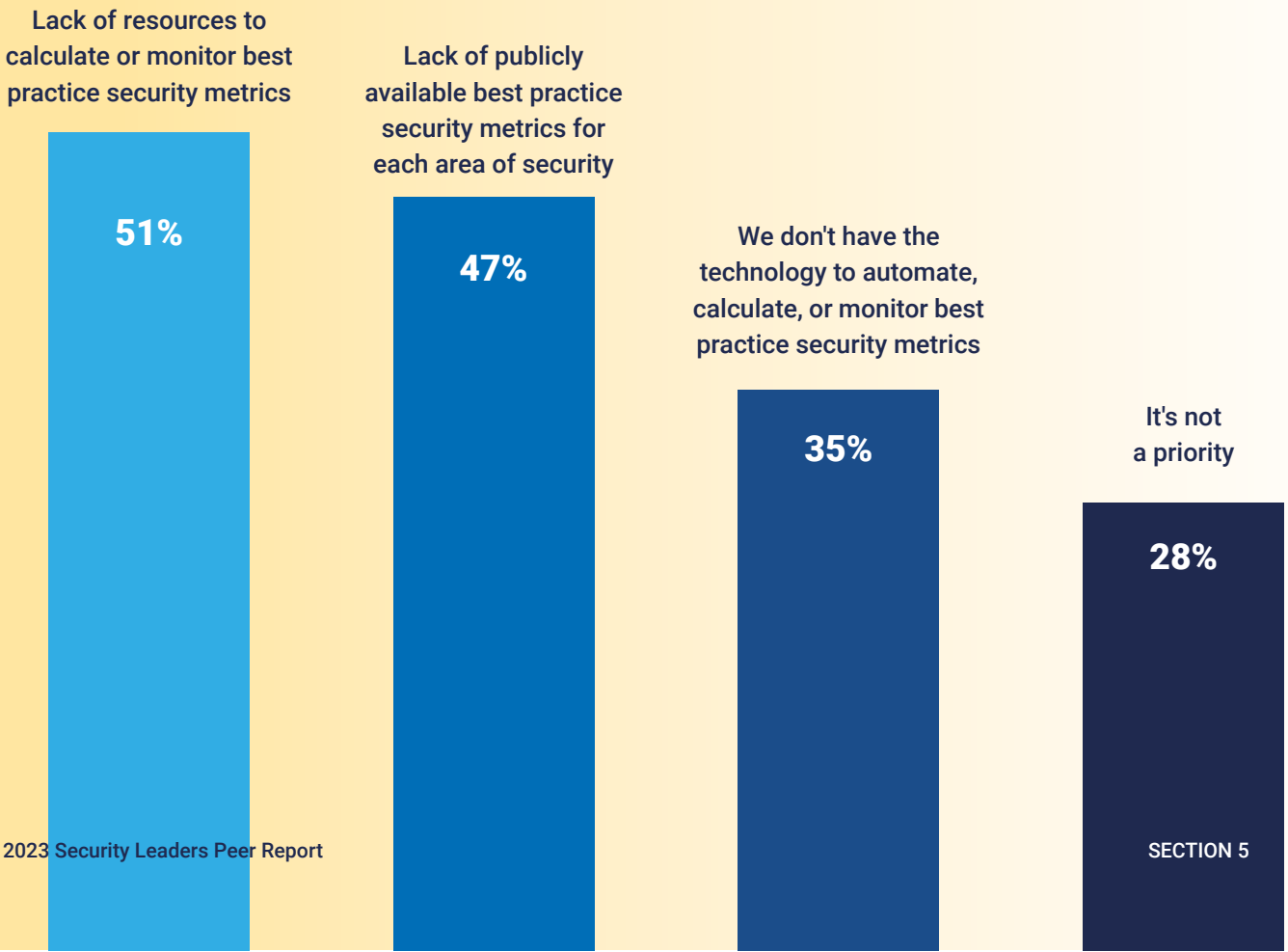
There's also evidence that this lack of automated control measurement and visibility creates stakeholder challenges that go beyond cyber risk. For example, security leaders are frequently required to justify investments both pre and post-implementation. But **53%** said they were less than extremely confident in evidencing security posture improvements based on new investments – a challenge made significantly more straightforward with effective controls measurement and visibility in place.

As stated in section three, security leaders are frustrated by various factors, not least the inability to influence internal stakeholders, collaborate with internal teams and prioritize security tasks – all of which are relevant to the issue of understanding and evidencing controls coverage and effectiveness.

When it comes to cybersecurity governance, have you ever asked yourself: *"What does good look like?"*

To find out how you measure up against your peers, read our guide to 18 crucial benchmarks for your cybersecurity control objectives and standards

What's preventing security leaders from being confident in their teams' ability to determine and continuously measure best practice security metrics?

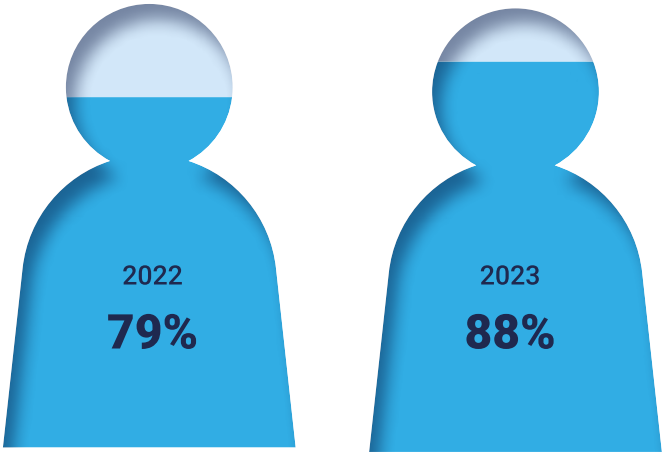


SECTION 6:

Heightened interest in security automation solutions

The challenges of efficiently managing security controls and the high-pressure environment facing security leaders make a strong case for greater use of automation. The promise of automation is to alleviate all the key frustrations that security teams encounter while optimizing security posture, eliminating preventable breaches and generating greater trust in security data.

Security leaders likely to implement CCM in the next two years

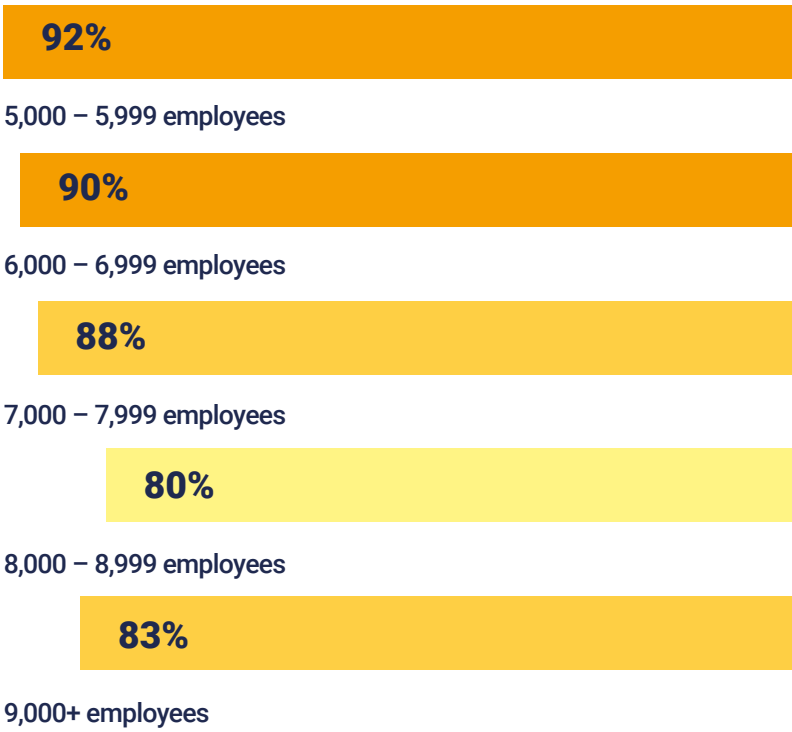


As with previous editions of this report, we asked security leaders how likely they are to deploy a **Continuous Controls Monitoring (CCM) platform** to measure and advise on effectiveness of their security controls.

Almost **9 out of 10** of respondents said it was likely or very likely they would implement a CCM platform in the next two years. That's an **9%** rise from our 2022 Panaseer Security Leaders Peer Report. Only **2%** of our sample said it was unlikely or very unlikely they would commit to a CCM project in the next two years.

Likely CCM adopters are evenly distributed across industry sectors, though it is interesting to note slightly elevated interest among the smaller enterprise organizations.

Security leaders likely to implement CCM in the next two years (by size of organization)



The figure is over **90%** of security leaders at businesses between 5,000–6,999 employees, versus around **80%** for businesses sized at 8,000 employees and above.

Running contrary to any assumption that CCM is best suited to the very largest organizations, this data reflects the perceived suitability of CCM for a far broader range of enterprise-scale businesses.

Conclusion

The central focus of this report series has been to chart security leaders' success at managing their security controls. The picture that emerges in 2023 is the degree of preventable breaches and incidents arising from gaps in security controls and how this is leading to frustration for security leaders, their teams and other stakeholders.

By branching out to explore the human dimension, our study has found significant frustration around the lack of visibility and control over tools and data. CISOs and other security leaders must also contend with a deepening cyber skills shortage that can leave departments understaffed and scrambling to cover the bases.

Our findings correlate the most frustrating aspects of a security professional's role with the motivating factors behind staff churn. We already know that mental health and wellbeing is at risk within security teams during periods of ransomware attack, to the extent that **42%** of security professionals **are considering leaving their role in the next two years.**[4] What our study uncovers is the added dissatisfaction and burnout resulting from the day-to-day grind of ensuring security controls coverage is sufficient and demonstrably performing as expected.

Set against this is the reality that successfully mitigating controls failure and optimizing security posture rarely needs to go beyond security tools that are already deployed and operating. This doesn't necessarily make life simpler, however, especially as organizations have so many tools and an increasingly complex technology environment to protect.

Among our other findings are those showing how security metrics are a continuing source of uncertainty for security leaders. Far more certain are the metrics this report series has tracked, particularly in terms of the time security teams spend on manual reporting.

The picture that emerges is of security teams no longer focusing their resources on security, but instead acting as data collation, presentation and reporting engines. Automation is sorely needed to alleviate this pressure, and in doing so support security professionals in focusing their creative energies on high-value tasks.

All roads appear to be converging on Continuous Control Monitoring (CCM) as the route to optimizing and managing security posture without the burden of manual overheads. The appetite for CCM among our sample comes from the clarity it brings to understanding all assets and the appropriate security controls.

This kind of solution prevents the all-too inevitable, and preventable, security incidents where threats evade controls that were thought to be in place to stop them. But it also promotes efficiency, accuracy and a single source of truth. With CCM, security leaders can and will escape the cycle that constrains them.

4 "The State of Ransomware Readiness 2022" (Mimecast)

Methodology

The primary research findings in this report are taken from a Censuswide survey conducted between 12–19 October 2022 and published here for the first time. The survey, commissioned by Panaseer, was carried out among 801 senior security decision makers (VP level and above) in cybersecurity-related roles working in organizations with 5,000+ employees. Respondents were segmented equally across UK and US jurisdictions (401/400) and across business services, oil and gas, financial services and pharmaceuticals industry sectors (201/200/200/200).

Where the commentary in this report makes references and data comparisons to earlier Panaseer Security Leaders Peer Reports, it does so on the basis that each individual report in the series – while differing somewhat in industry sector coverage – is a representative sample of senior security leaders at large enterprise organizations in line with the above definition. Please refer to the published methodologies of each report for full details of how each sample is composed.

About Panaseer

Panaseer is an enterprise cybersecurity automation and data analytics company that helps organizations stop preventable breaches by ensuring security controls are fully deployed and working effectively — maximizing their security investments and resources. Control failures are the biggest problem in cybersecurity, with 79% of organizations admitting to being surprised by a security event that evaded existing controls.

Panaseer's Continuous Controls Monitoring platform gives a complete, trusted view of security controls, with metrics and measures guidance aligned to best practice frameworks that improve collaboration and prioritization. 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.

We've got you covered

Continuous Controls Monitoring for enterprise security