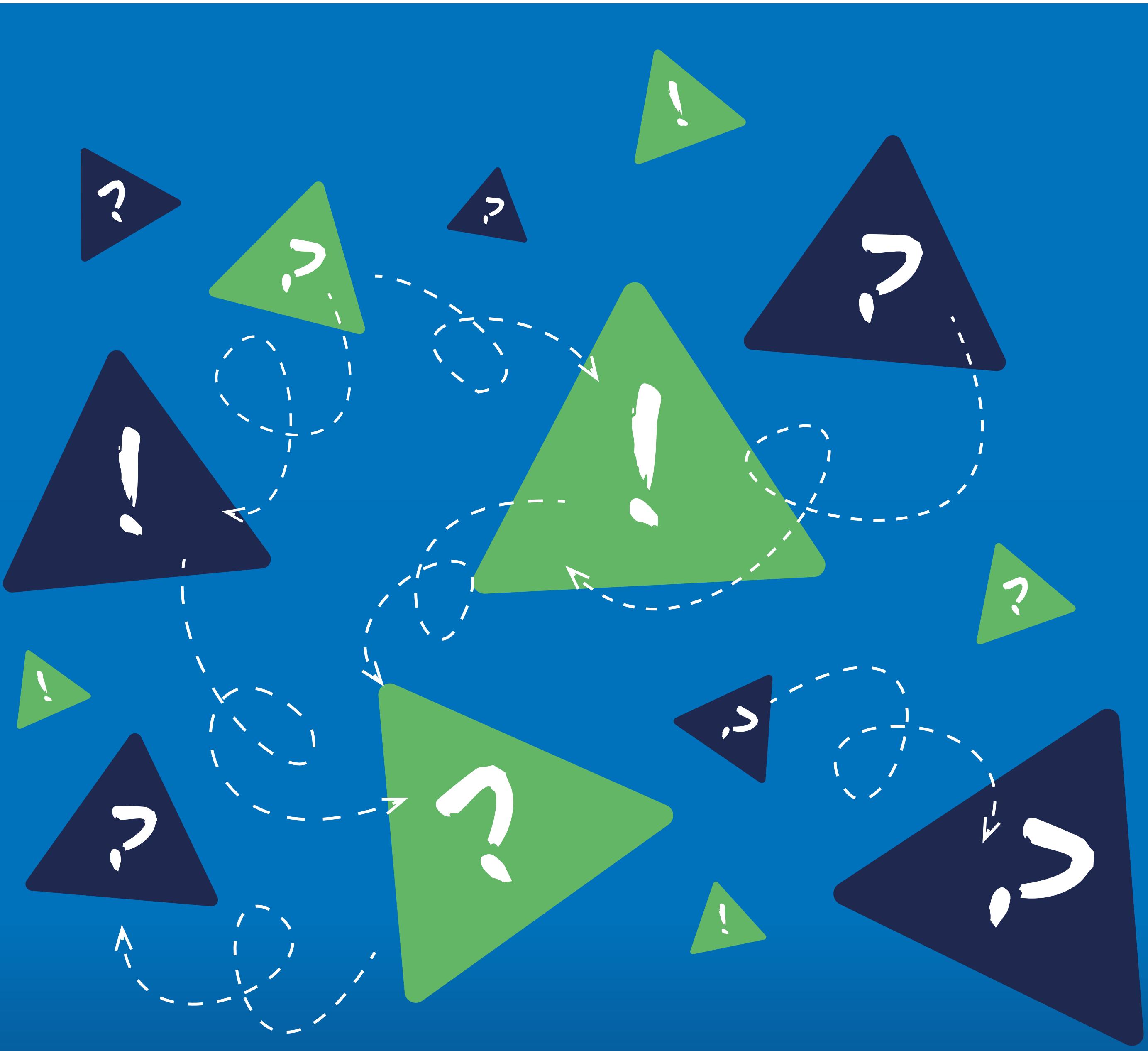


2024 Security Leaders Peer Report:

Solving the CISO's controls conundrum

ABOUT THE EXPERTS

Shawn M Bowen

SVP and CISO of World Fuel Services

Shawn has over 20 years' experience in information technology, primarily in cybersecurity, and was previously CISO for Restaurant Brands International and the US Marine Corps. He's a Certified EC-Council Instructor (CEI) for the CCISO course and is regarded as a passionate and transformative thought leader in IT security.

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

Introduction

For the fourth year in a row, we find that security teams are spending almost half their time on the drudgery of collating and analyzing data. But despite it consuming so much of their resources, security leaders remain conflicted about the purpose and value of security controls data.

In this, the 2024 Panaseer Security Leaders Report, we look at the challenges organizations face in understanding and improving their security posture. In particular, we investigate how confident security leaders are in the effectiveness of their controls and how they get the insights needed to aid decision making and reduce business risk.

The results show palpable tension between optimism and evidence; CISOs trust their security controls and believe they're protected despite continuing to suffer control failures. Our research probes what's causing this conundrum and what can be done about it.

We also look at the personal concerns of CISOs and what they see as their most important priorities. They're being asked to do more with less while facing increased scrutiny as boards mature in their understanding of cyber risk and new regulations make them more accountable. Better use of security controls data can help, but to what extent?

Resolving these problems is a clear priority. Can security leaders confront the contradictions and use their controls data to get a broader, trusted view that transforms how they manage their security posture?

This report examines how organizations can harness automation to enrich the accuracy and completeness of security controls data at scale. This can give them the knowledge and insights to do their job more easily, efficiently and effectively.

Expert commentary is provided throughout our analysis by Shawn M Bowen, Marie Wilcox and Andreas Wuchner.

SECTION 1:

Perception vs. Reality: are your security controls as effective as you think?

Our research set out to understand how organizations manage and monitor their security controls. We surveyed 404 security leaders in the US and UK, with a specific focus on how they use controls data to improve decision making and reduce business risk.

The results show a disconnect between what they perceive and the reality of what's happening.

The positive perception of security controls data

Security leaders all want to deliver on the expectations of their role and make their organizations more resilient. Security controls data is seen as a crucial foundation for cybersecurity operations, and respondents consistently reported high levels of confidence both in the accuracy of security controls data and the purposeful way it is applied.

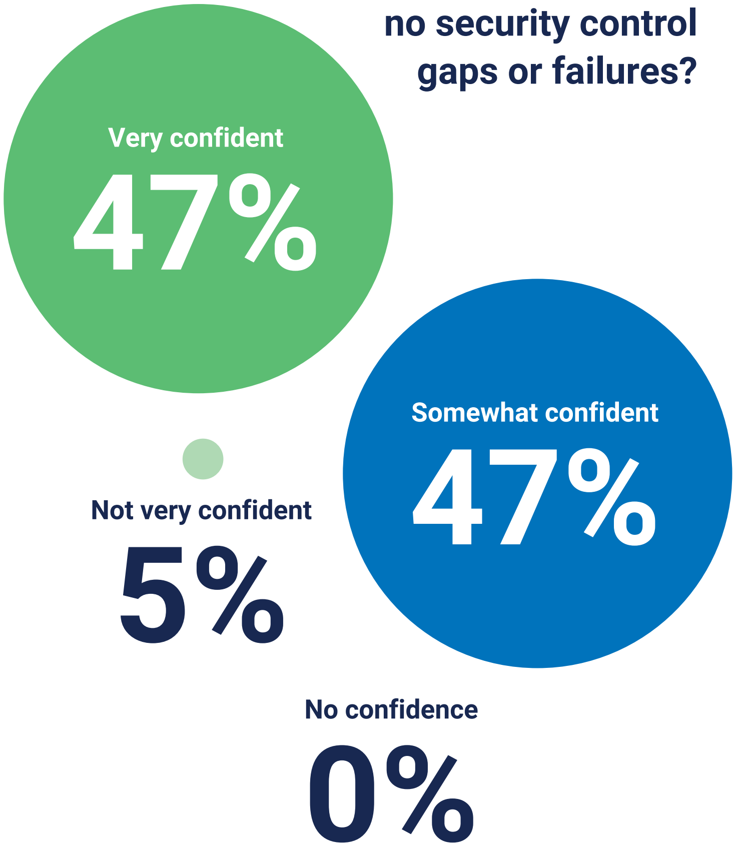
Nearly half (**47%**) of organizations are highly confident that security controls are working effectively all the time. In total, **95%** are highly or somewhat confident. This shows a very strong level of trust in security controls data.

The accuracy and completeness of data is also extremely important to improving cyber resilience, giving organizations a true measure of their security posture, and a better understanding of weaknesses and gaps. Our survey found that **88%** of respondents trust that their cybersecurity data is accurate, while less than **5%** do not.

Finally, we know that security controls data is highly pertinent to making the right security decisions, addressing risk, and prioritizing vulnerabilities and incident response. Accordingly, over half (**54%**) of security leaders are very confident in their ability to use security data to prioritize actions to have the greatest impact on risk reduction (**96%** are confident to some extent).

All in all, a very positive picture.

How confident are you that you have no security control gaps or failures?



Evidence suggests reality doesn’t match perceptions

However, though security leaders are confident in their controls data, closer analysis of the research suggests this trust is built on shaky foundations. The perception is that everything is okay – that security leaders have done everything they can – while the reality is that breaches are occurring.

For example, **79%** of organizations have been surprised by a security incident that evaded their controls. This is the acid test for whether security controls data is being properly used and interpreted to improve security posture. Evidently it is not and, looking back to past editions of this report, it’s a stubbornly familiar pattern.

Shawn M Bowen, Senior Vice President and Chief Information Security Officer of World Fuel Services, has sympathy with security leaders who feel they have robust security controls but are still getting breached.

“Most controls are pretty exact – like you need to validate something every seven days. But often the reading of a control comes down to your individual interpretation. Even with auditors, one auditor will interpret a control completely differently to another. So you have a lot of people with the best intentions, but there's deviation in there,” says Shawn.

“Added to that, you’re normally validating a sample set of your controls – we’re rarely ever validating 100%. So the size and complexity of the problem means there’s always an opportunity for something to be missed.”

This problem is exacerbated by the siloed business functions that exists in many organizations.

“IT teams are often responsible for implementing controls but they don't feel the pain when they go wrong – the security team does,” explains Marie Wilcox, VP of Marketing at Panaseer and Board Member at The Chartered Institute of Information Security (CIISec).

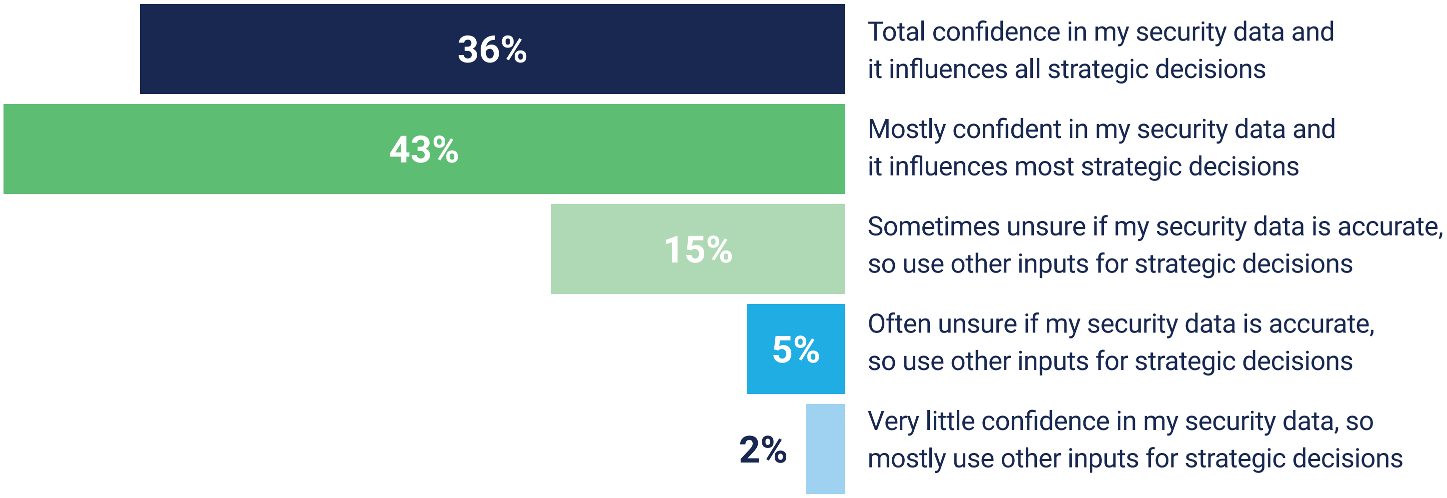
> **“The size and complexity of the problem means there’s always an opportunity for something to be missed.”**
>
>
>
> Shawn M Bowen, SVP and CISO at World Fuel Services

“Furthermore, security teams are focused on indicators of compromise (IoCs), not the security controls data that can help them better manage risk.”

Our survey found **36%** of security leaders are totally confident in their security data and use it for all strategic decision making. Why such a low figure when confidence is so high that data is accurate and controls are working effectively?

Over one-fifth (**21%**) lack confidence to the extent that they look for additional inputs when making strategic decisions (it is **27%** of US respondents).

Does security data help decision making?



Another sign of the disconnect between perception and reality is that few respondents are taking the measures that would give cause to be that confident; employing the necessary practices to optimize the use of security controls data for protecting their organizations. For example, only **30%** prioritize vulnerabilities using contextual analysis of security controls data in their environment.

There are many instances where this approach makes a crucial difference, such as in the recent MOVEit mass exploit[1]. In this and other examples, contextual analysis of security controls data helps organizations quickly get to grips with their exposure to specific CVEs, identifying all instances of vulnerabilities and applying business context to see exactly which systems, processes, business units, and locations are affected.

Marie Wilcox believes this indicates a need to shift mindsets away from reporting and towards action.

“Security data and reporting has historically been used for compliance and audit purposes, or to produce a report for the board. It's a mindset shift in the sense of using security controls data as a tool to defend your security posture in the here and now, rather than as a mechanism for documenting how you're protecting the organization. The **30%** using contextual analysis are likely on a journey to achieve that mindset change first.”

> **“Security data has historically been used for compliance and audit purposes. It's a mindset shift to use security controls data as a tool to defend your security posture in the here and now.”**

Marie Wilcox, VP Marketing at Panaseer and Board Member at CIISEC

> **“A friend says that solving security problems is like raking up leaves on a windy day. For me you’re looking at the symptom, not the problem. Cut down the damn tree so there’s no more leaves to be raked.”**

Shawn M Bowen, SVP and CISO at World Fuel Services

We also explored the reasons behind the problems with security controls data. Over one-third (**38%**) cite the inability to evidence remediation of control failures. A similar number (**37%**) classifies control failures as a low priority (**43%** in financial services companies). Based on this, security controls data does not appear to be widely viewed as a strategic asset for cyber protection.

“As an industry, we're good at using data to report the problem. But we're just generating an unresolvable backlog of tactical responses," says Shawn.

"We have all the right tools, but if every week they’re finding the same ’new’ problems again, then those aren't the problems, those are the symptoms. Nobody is using data to do that root cause analysis to understand the underlying issues."

“A friend of mine says that solving security problems is like raking up leaves on a windy day. I get what he’s saying, but for me you’re looking at the symptom, not the problem. Cut down the damn tree so there’s no more leaves to be raked.”

[1] Panaseer (2023), *How to accelerate remediation of the MOVEit zero-day vulnerabilities using Panaseer*

Recognizing the need for better data quality

The vast majority (**90%**) of security leaders said that improving the accuracy of cybersecurity data is a priority for them in the next 12 months.

This is a laudable objective for any organization harnessing security controls data for risk reduction (rather than simply for reporting or compliance purposes), but it also illustrates urgent demand for action. This is borne out with the finding that organizations – on average – only have visibility of **61%** of their devices in their CMDB or asset management inventory. This chimes with Gartner's finding that only **25%** of organizations are receiving meaningful value from their CMDB investments[2].

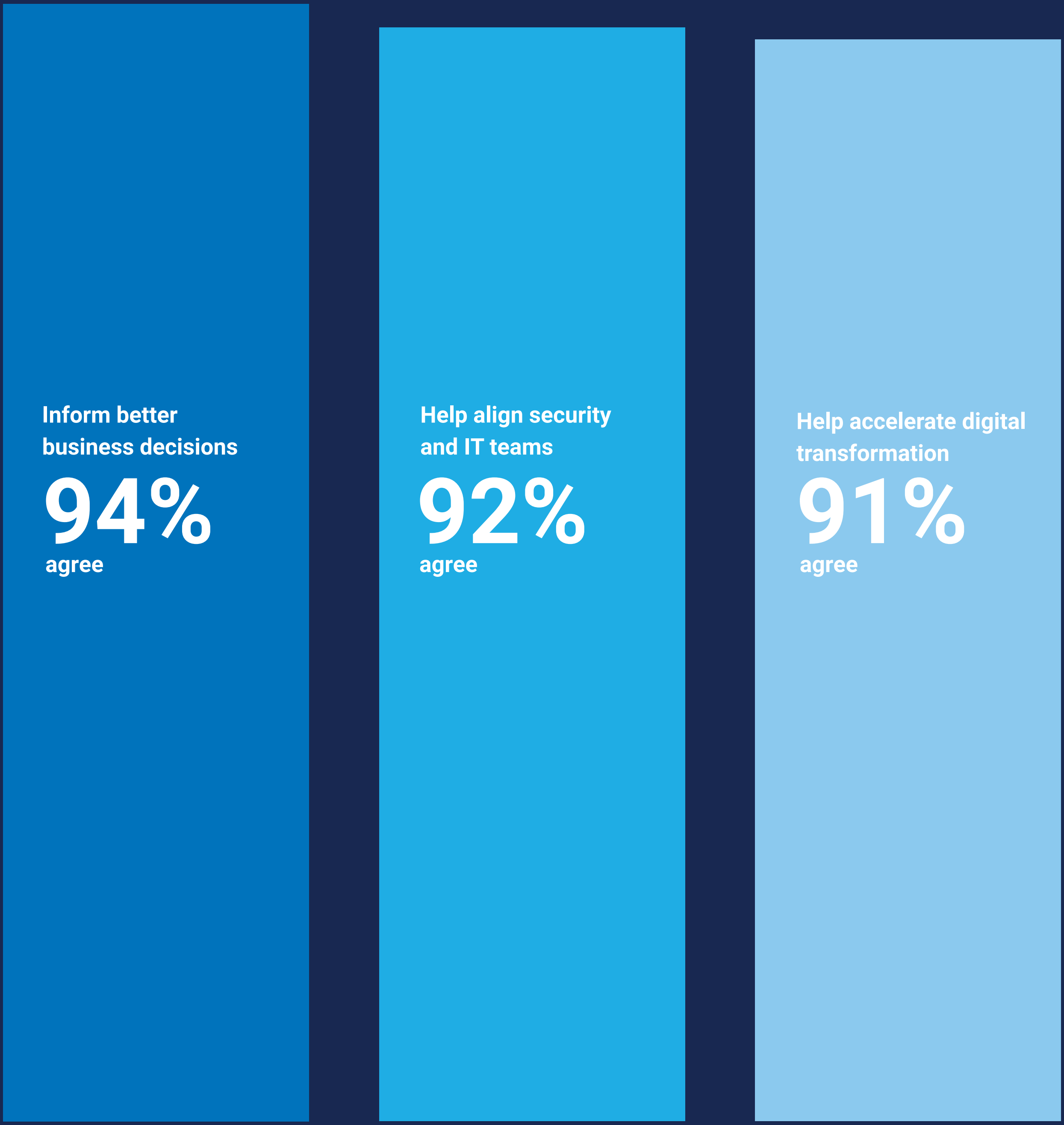
On the issue of data accuracy, Andreas Wuchner, Field CISO at Panaseer, highlights how the CISO role becoming less technical and more focused on risk management may harbor an unintended consequence: security leaders who don't realize they have poor data and controls gaps.

"When you're basing decisions on inaccurate or incomplete data, you aren't acting on what's true, you're acting on what you believe because that's what you've been told.

"As CISOs evolve to become less narrowly focused on technology defense layers and silos, they become less technology savvy and rely on what they get told. I am very supportive of CISOs embracing a risk management approach aligned to business priorities, but not when it dilutes attention on things like technical controls coverage, visibility of devices and so on. Fewer board reports have any performance data (KPIs) at all; it's all key risk indicators (KRIs). There needs to be a better balance of the two."

[2] Gartner (2020), *Break the CMDB Failure Cycle With a Service Asset and Configuration Management Program*

If you had more accurate security controls data, what would be the benefits for your organization?



SECTION 2:

What do CISOs need to overcome their controls conundrum?

The clear mismatches in perception versus reality regarding the use of security controls data highlight a CISO conundrum that needs to be addressed, whether security leaders realize it or not. For maximum clarity, unaffected by the circumstances of their current roles, we invited respondents to share their views on what they saw as the biggest concerns and challenges when taking on a new CISO position.

Recognizing the personal impact and stress that comes with being a CISO, we wanted to delve into their private concerns as well as what they saw as the biggest professional challenges in that scenario.

Biggest CISO concerns stem from uncertain data

> “An assessment of the current state is essential but so is looking at the stakeholders, their concerns, business priorities and how much board support there is for your role.”

Andreas Wuchner, Field CISO at Panaseer

Beginning with personal concerns, as expected we saw issues relating to budget and resources show up, but the most pressing related strongly to the availability of reliable security controls data.

The biggest concern when taking on a new CISO role is getting an inaccurate audit of the company’s security posture (**54%** of respondents). This shows that security leaders value having a true measure of their security posture, but also nods to the likelihood that they may be given inaccurate data. Clearly they acknowledge the consequences of false information that masks points of weakness and misdirects available resources to the wrong priorities.

This concern is almost twice that of the **30%** of respondents worried by “lack of senior buy-in for transforming security processes”.

“I would expect to see getting board-level buy-in as the most pressing issue for incoming CISOs so this is surprising,” says Andreas. “In my experience, an assessment of the current state is essential but so is looking at the stakeholders, their concerns, business priorities and how much board support there is for your role.

“This broader outlook should help CISOs assert themselves and avoid situations that inevitably descend into constant firefighting, always being two steps behind, always competing for every piece of budget.”

Biggest concerns when taking on new CISO role

54% Receiving an inaccurate audit of the company's security posture

44% Lack of budget to make necessary investments

44% Being scapegoated/held personally accountable for a breach

The other major concerns are consistent with trends captured in Panaseer's recent *Optimizing cybersecurity* research report, which uncovered deep disquiet in the lack of resources needed for security teams to function, despite budgets growing on average **29%** a year[3].

On the point of personal accountability, we found this phenomenon growing in line with the emergence of stronger cyber regulation – such as the **Digital Operational Resilience Act (DORA) in the EU** – that places the emphasis on board members to carry the can for deficiencies in how they handle ICT risk. Prosecutors in the US have already established a precedent in the prosecution of Uber's former CISO Joe Sullivan for his response to a hacking incident[4].

Good data central to addressing CISO challenges

The most cited challenge for incoming CISOs was obtaining "a true picture of weaknesses in organizational security posture". This and the other top three challenges reflect respondents' desire to get to grips with the current state so they know what they're dealing with as soon as possible.

For instance, third is "getting trusted data to enable strategic decisions" (**43%**), highlighting the recognition of trusted data as a critical factor in security decision making, and the perceived difficulty in getting data up to the required quality.

"One of the most important things in the world is credibility. If you lose credibility, it's the hardest thing to earn back from people. So, when your data lacks credibility, that's the same problem. You need to know where your data is inaccurate and be up front about it, otherwise if someone else finds the inaccuracies they aren't going to trust you again," says Shawn Bowen.

Top challenges when starting a new CISO role

49%	Getting a true picture of weaknesses in organizational security posture
45%	Understanding threat landscape
43%	Getting trusted data to enable strategic decisions

In less mature organizations, improving the quality of data and building an accurate understanding of its deficiencies will be a heavy lift and requires a cross-functional transformation in how security is done.

Organizations spend half their time manually curating security data

Whether starting a new CISO role or not, one fact has persisted throughout the four years of the Panaseer Security Leaders Peer Report: organizations spend huge quantities of their time on manually collecting, formatting and presenting security data – **46%** in any given month, by the latest research.

"If this is the cost of getting trust in your data – spending almost half the security team's time on manual processes – then leaders should know there is an easier way," says Marie. "Use an automated platform to achieve a single, trusted source of truth for security controls data and get better insights.

[3] Panaseer (2023), *Optimizing cybersecurity: Striking the balance between people and technology*
[4] Dark Reading (2023), *Judge Spares Former Uber CISO Jail Time Over 2016 Data Breach Charges*

“Not only that, but you can claim back all that time and effort to focus on harnessing those insights to achieve a stronger cybersecurity posture.”

It’s true that security leaders and their teams have a lot on their plate already. Successive studies show that pressures are increasing as threats continue to rise in volume and complexity along with board-level expectations for effective risk management. New regulatory requirements, budgetary constraints and skills shortages all add to a general sense of being more reactive than proactive, resulting in high instances of workplace stress and job dissatisfaction.

A recent Proofpoint survey[5] found that **61%** of CISOs feel they face “excessive expectations”, up over a fifth on the previous year. Panaseer’s own studies show that lack of security skills, budget, and headcount are deemed the principal factors negatively influencing security posture, with **75%** of organizations saying their lack of resources impacts cyber risk mitigation[6].

The CISO conundrum discussed earlier, as with all concerns and challenges faced by incoming CISOs, has to be viewed through this prism. With so little time available, surely the key is a more focused approach to trusted data that’s made possible through automation.

[5] Proofpoint (2023), *2023 Voice of the CISO*

[6] Panaseer (2023), *Optimizing cybersecurity: Striking the balance between people and technology*

SECTION 3:

Time for a fresh approach to cybersecurity

Something clearly needs to change to solve this CISO controls conundrum. Confidence in security controls data is seemingly misplaced, coming not from empirical evidence but from the belief that all that can be done is being done.

Security leaders need to find a fresh approach. Rather than continually reacting to urgent incidents, they should enable their teams to make better use of their controls data to drive decisions and stop problems before they occur.

> **“Too often, we're starting with technology to solve the process problem or to solve the people problem.”**
>
> Shawn M Bowen, SVP and CISO at World Fuel Services

Trusted data is a key part of that, but it’s more than just a technology problem. It requires a change in mindset and willingness to do things differently.

“In security we need to think in terms of people, process, and technology. But it should be people, process, *then* technology, it’s an order of priority. That means you need to have the right people first – the right critical thinking – to build a process that makes sense, then leverage technology to exploit that process,” says Shawn.

“Too often, we're starting with technology to solve the process problem or to solve the people problem.”

Getting to truly trusted and complete data

First up, how can security leaders obtain controls data that can be trusted by stakeholders across their organizations?

The last of our hypothetical questions about taking on a new CISO role aimed to uncover the top three priorities for security leaders. As with their concerns and challenges outlined earlier, these can all be addressed by access to trusted security controls data: understanding security posture (**39%**), understanding processes for data collection and analysis (**38%**), and running an audit of security tooling (**37%**).

Top three priorities for new CISOs

39% Understanding security posture

38% Understanding processes for data collection and analysis

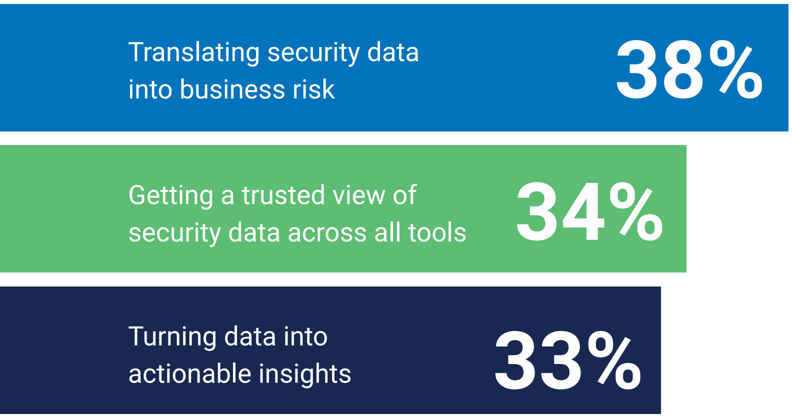
37% Audit of security tooling

The benefits of improving data quality and trust are clear, with **84%** of security leaders believing that increasing trust in their data would help them secure more resources to protect their organization. Yet only **47%** of security leaders strongly believe that the C-suite trusts their security data and reporting.

“Security leaders are making sense of security controls data and understanding its impact – but there's a trust issue,” says Marie. “If trust in data can be restored, then security leaders can use that data to work differently. Leaders can choose to embrace this change or resist it and miss out on the benefits.”

The most significant challenge with managing security data is translating it into business risk (**38%**). This is crucial to understanding the controls conundrum. Without the ability to put business context onto security risk, security leaders are unable to communicate effectively and get the support they need from the rest of the business and the board. The other main challenges are “getting a trusted view of security data across all tools” (**34%**) and “turning data into actionable insights” (**33%**).

Top three challenges with managing security data



Why isn't this happening, asks Andreas. “Usually because security leaders don't believe in the trustworthiness of their own data. They say their data quality is bad; there are so many loose ends and therefore aggregating and correlating it all will make matters worse. But security experts aren't necessarily data experts.

“Most are surprised to learn that the opposite is true; that taking three sources each of 60% data quality and combining them together can give you a single source at 95% quality. Data doesn't have to be perfect to begin with. And enriching it through automation is easier than people think.”

Boards need to support transformative security change

The mindset shift that needs to happen concerns the whole organization, not just the CISO or security leader. This is partly about resetting the purpose of security controls data, dispelling the myth that it’s just for compliance and reporting.

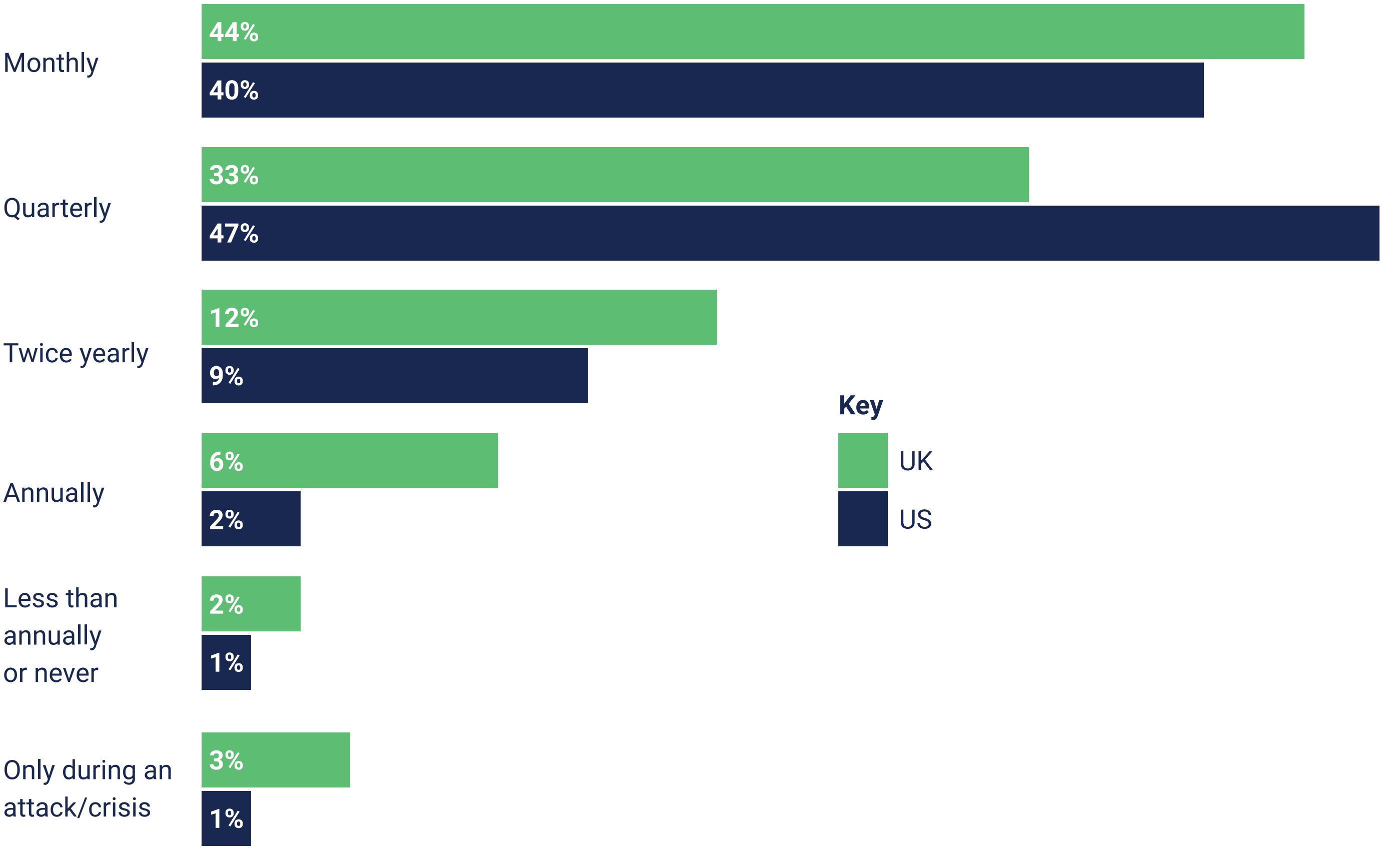
However, according to our survey, barely half (**47%**) of security leaders are fully confident that their C-suite actually understands cybersecurity risk at all. Boards should be deeply concerned that their security experts have such a low opinion.

“The biggest changes to security happen after a breach,” continues Andreas. “It's human nature to wait to be taught a lesson by an event that you convinced yourself was unlikely to happen. That's not to criticize security leaders – they know this, but the challenge is getting senior decision makers on board.”

With boards under increasing pressure from regulations like the SEC (Security & Exchange Commission) rules on cyber disclosure and DORA holding them accountable for ICT risk, it's likely that security leaders will be asked to report more frequently and be more closely scrutinized on exactly what they report.

Our research found an even split between monthly (**42%**) and quarterly (**40%**) cybersecurity risk reporting cadences, though it is more biased toward monthly reporting in the UK than in the US. It seems likely that all board meetings – in time – will have cybersecurity risk as a standing agenda item, relying upon the most accurate and complete data.

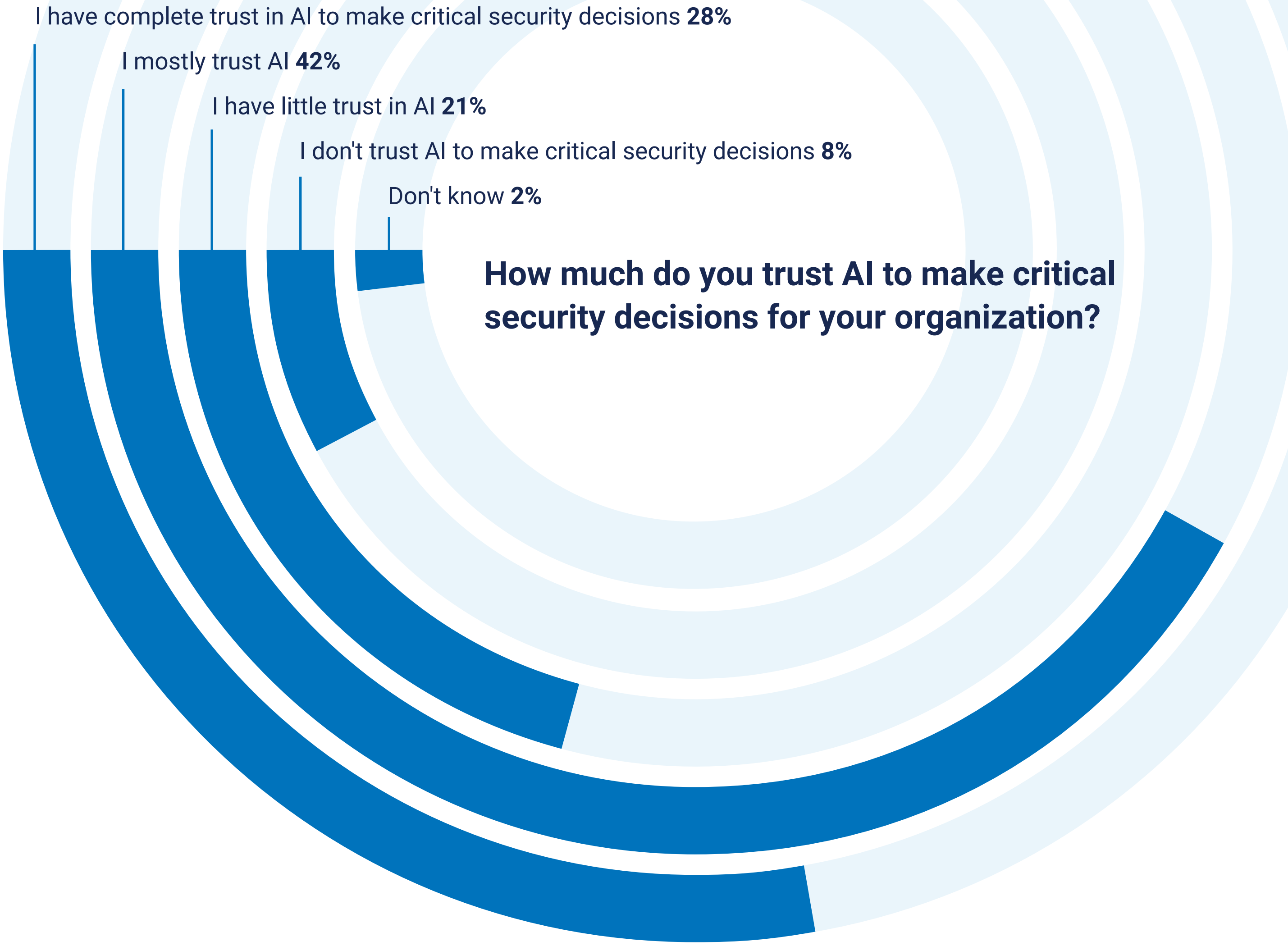
How often do security leaders report to the board on cybersecurity risk?



Does AI have a role?

Respondents were asked to consider the impact of artificial intelligence (AI), both as a cyber attack and cyber defense tool. Given the focus of this report, it’s important to recognize that AI won’t be able to ease any CISO challenges without access to accurate data.

There is healthy AI skepticism among security leaders, with over **28%** having little or no trust in AI to make critical security decisions. However, the same number (**28%**) stated they have complete trust in AI when it comes to decision making. These potentially represent the organizations most advanced in their use of trusted security controls data, and benefiting accordingly.



How much do you trust AI to make critical security decisions for your organization?

On the flip side, around **76%** are concerned about threat actors using AI to find gaps in their organizations' security controls. Certainly if gaps exist – because security controls status cannot be trusted – then they risk being exploited. The **24%** who are not concerned will hopefully be equipped with the necessary trust in their data.

"A lot of budget is going towards automation and exploring how AI and machine learning can help improve cybersecurity," says Andreas. "The problem isn't that we don't have data, it's that organizations don't understand it well enough or do enough with it. Pure correlation of the data sources to get a proper inventory is so simple when you talk about it, but it's tricky to do and not many people are doing it. Do it manually and it takes forever and is prone to error."

Solving the CISO controls conundrum with CCM

According to Marie, if you're committed to a mindset shift that elevates the role of security controls data, Continuous Controls Monitoring (CCM) solutions can help deliver the change, enabling trusted data and all the benefits this brings to cybersecurity posture.

"The industry needs to change and CCM can be the catalyst. It isn't a better reporting tool, it's a way of knowing what to do next – making day-to-day cybersecurity firefighting easier and getting ahead of the game on strategic risk. At the moment, many leaders don't know that security controls data can help them do this. It's understanding the value of a big picture view and single source of truth rather than multiple siloed perspectives.

"Crucially you need visibility into how the raw data has been correlated in your automated tool to have complete trust in the data, or risk having to double-check. That makes some solutions problematic, like CAASM [Cyber Asset Attack Surface Management] and particularly CMDBs. If you're drawing on your CMDB for controls-related decisions then your basis for trust is low and you're going to need further analytics correlated with other data sources to get a trusted, accurate picture."

Conclusion

In the 2023 edition of this report we found that almost **90%** of security leaders believe that security control failures are a primary cause of breaches. One year on and professionals continue to acknowledge the same problem — it seems clear that something needs to change in how the industry approaches security, both day to day and strategically.

Experienced security leaders will know what it's like going back to the board asking for more resources to deal with cybersecurity risk. And it's hard to then admit that things still aren't fully under control. "To the best of my knowledge" shouldn't feel like an appropriate justification to letting control failures slip through. Failing to convert the value of accurate and complete security controls data is leading to many missed opportunities.

The solution to this "security leaders' conundrum" is at their fingertips. CISOs can change the narrative themselves and instigate a mindset shift through better use of the data they have, unearthing the insights that show them the true status of their security posture. Rather than wasting their time manually processsing data simply to tick a box and populate a report, this data should be used to drive the right conversations and decisions across the organization.

They can then reduce cyber risk by understanding and prioritizing what they need to do to improve, with Continuous Controls Monitoring (CCM) also enabling them to measure the impact of their efforts and build trust with stakeholders.

The change opportunity around CCM embraces technology, process, and people. All those siloed functions that are used to working on their own can draw on a single source of truth that brings them together, especially IT and security teams.

By driving more value from their controls data, CISOs can close the gaps in their defenses, as well as the gap between their perceptions and reality.

Methodology

The primary research findings in this report are taken from a Dynata survey conducted in August 2023 and published here for the first time. The survey, commissioned by Panaseer, was carried out among 404 senior security decision makers in cybersecurity-related roles working in organizations with 1,000+ employees. Respondents were segmented equally across UK and US jurisdictions.

About Panaseer

Panaseer is an enterprise cybersecurity company that helps organizations improve their security posture by continuously measuring whether controls are fully deployed and working effectively. It has been recognized by the World Economic Forum as a Technology Pioneer helping to solve the world's most pressing issues.

Panaseer's Continuous Controls Monitoring (CCM) platform gives CISOs a true picture of their security posture by measuring performance of their cybersecurity defenses against established frameworks and regulations. This enables them to take targeted action to reduce cyber risk and provide accurate data to stakeholders and regulators. CCM also drives more efficient use of resources through automated processes and improved prioritization.

Read previous editions of the Security Leaders Peer Report:

panaseer

Panaseer Security Leader's
Peer Report

Why poor visibility is hampering cybersecurity

Over the years the emphasis placed on cybersecurity has increased, placing security leaders and their functions at the heart of the modern enterprise. Amidst a fast-changing threat landscape, regulatory hurdles and limited budget and resources, many security leaders are understandably looking to improve their cybersecurity posture.

Panaseer commissioned Censuswide to conduct a survey of 200+ senior security leaders working in large enterprises to create a peer report with an objective to understand the issue that hamper cybersecurity posture in an organisation.

panaseer

Panaseer 2022
Security Leaders Peer Report

panaseer

2023 Security Leaders
Peer Report

Read SLPR 2019

Read SLPR 2022

Read SLPR 2023

Automated security posture management

Continuous Controls Monitoring for enterprise security