panaseer

Panaseer 2022
Security Leaders Peer Report

Contents

Introduction

Cybersecurity, and the roles and responsibilities of security leaders enforcing it, has become increasingly urgent as ransomware, phishing attempts and other malicious attacks have become common obstacles for the modern enterprise. At the same time, cybersecurity has become more complex and challenging due to the mass migration to remote working witnessed since the COVID-19 pandemic, and the ever-growing plethora of security tools available to those managing security risk. Our **2019 Security Leaders Peer Report** found that all industries included in our research faced challenges regarding visibility, manual reporting and an overwhelming amount of security tools used to overcome these challenges.

Using that report's findings as a benchmark, we launched the Panaseer 2022 Security Leaders Peer Report in a bid to understand if and how the industry has evolved in response to the extraordinary challenges before it. This report explores the new state of play after two turbulent years that no one could have predicted. It revisits the core themes of our 2019 research to consider what has improved or worsened, and the impact on how security leaders and their teams keep organisations secure.

Key findings

Senior security executives are still in the dark with asset visibility.

Databases now top the list of assets that security leaders have least visibility on (**27%**), which correlates with a sharp rise in ransomware attacks.

Tool overload continues to rise.

Security teams from big enterprises now have an average of **76** security tools – an increase from 2019 when the average team was grappling with **64** security tools.*

Manual overload of reporting is increasing.

Security teams are now spending over half of their time (**54%**) manually producing reports. This is a sharp increase from 2019 when it was **40%**.*

A lack of insight is driving control failures.

82% of security leaders have been surprised by a security event, incident, or breach, which evaded a control that they thought was in place. On average, they experience five control failures. Only **36%** are very confident in their ability to evidence controls are working as intended.

Increased ransomware risk is charging stakeholder interest in better visibility.

84% of security leaders confirmed that their board was actively interested in ransomware protection levels across the business, and **91%** of them are regularly reporting on it to their board. Ransomware protection is now a budgeted priority for **86%** of organisations over the next two years.

There is a drive for Continuous Controls Monitoring.

79% of security leaders are likely to implement a Continuous Controls Monitoring platform to measure and advise on their control effectiveness, within the next two years.

* Note that for a true like-for-like comparison, Panaseer has segmented the data from its 2019 Security Leaders Peer Report to focus on the comparable companies sized 5,000 to 10,000+ employees.

SECTION 1:

Security leaders in the dark over controls coverage

As external threats rise in frequency and sophistication, security leaders are overwhelmed by threat actors looking to exploit known and common vulnerabilities, infiltrate private networks and con users via increasingly intelligent social engineering techniques like phishing and pretexting. Such attacks, particularly ransomware, have only become more popular throughout the COVID-19 pandemic as opportunistic attackers across the globe have capitalised on gaps in policy and controls coverage caused by the rush to establish universal cloud and remote access to corporate systems and data.

When asked what changes they have experienced in security metrics since the beginning of the pandemic, respondents cited:

All told, organisations continue to demonstrate a lack of visibility of their technical assets. Combined with a similar lack of knowledge of their security controls, security teams remain in the dark with limited insight into their true cyber hygiene and therefore their risk posture.

In 2019, Internet of things (IoT) topped the list of technical assets where senior security executives had the least visibility, with one in five (**20%**) citing it as their chief concern. This year's results list databases as the leading asset that security leaders have the least visibility around.

42% experienced an increase in the number of incidents

42% experienced an increase in unpatched vulnerabilities

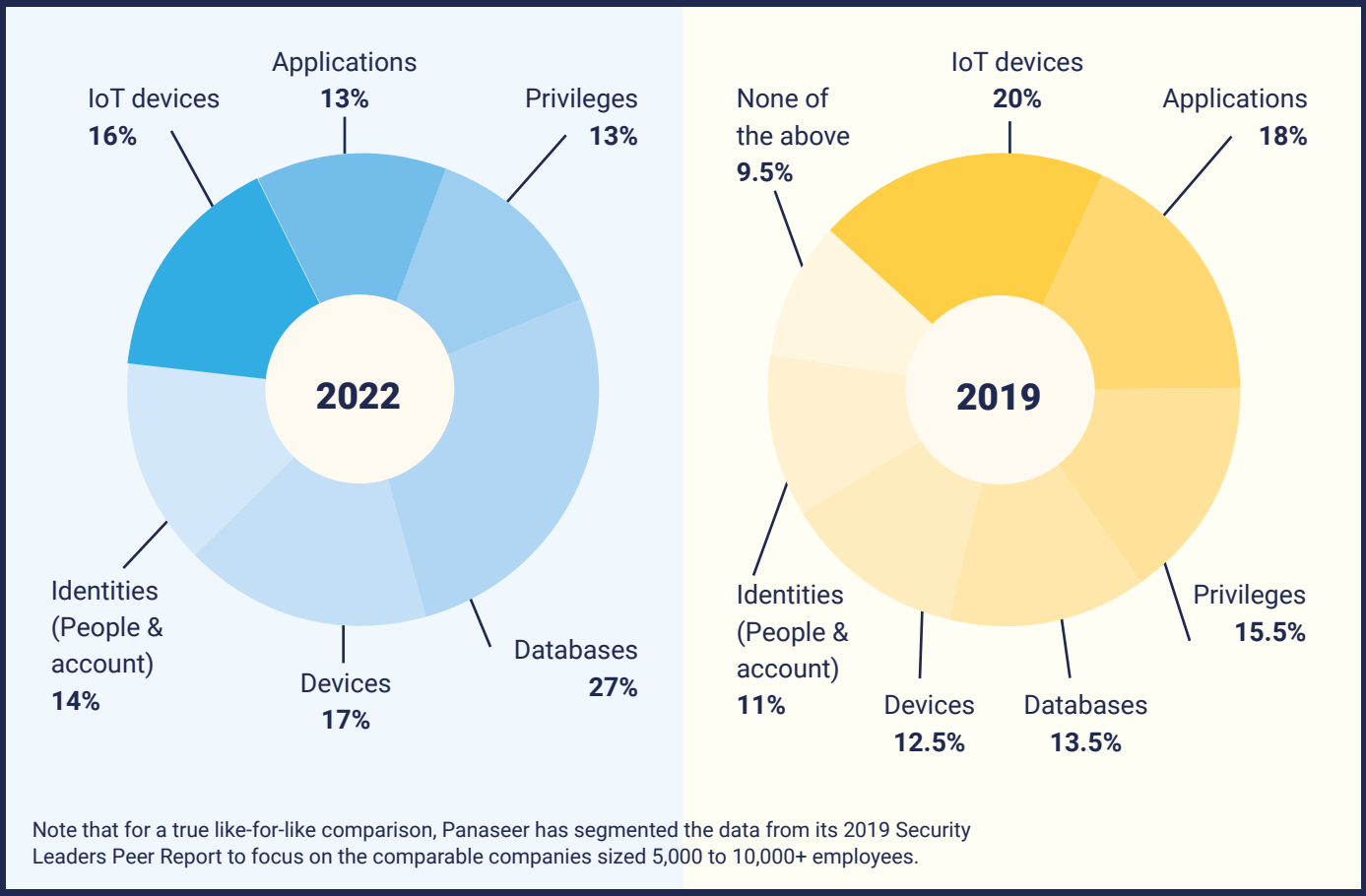
43% had to spend more time rolling out new security tools

44% had to spend more time remediating device issues

46% experienced an increase in the number of events

47% experienced an increase in the number of breaches

Assets that security teams have the least visibility of



Note that for a true like-for-like comparison, Panaseer has segmented the data from its 2019 Security Leaders Peer Report to focus on the comparable companies sized 5,000 to 10,000+ employees.

The lack of visibility around databases over the past two years correlates with a sharp rise in ransomware attacks since the beginning of the pandemic. This, in turn, has led to more focus on regulations and data security as enterprises shift their priorities to concentrate on improving data protection. However, while their priorities may have shifted, without strong visibility businesses are still struggling to pinpoint the right information to inform security metrics for their cybersecurity and risk posture reporting. This is despite universal agreement among our respondents (**99%**) that it is valuable to be able to report and prioritise security risk based on the business process it supports.

With the continued uptake of Continuous Controls Monitoring and a growing number of systems and solutions supporting total asset visibility, there are fewer reasons for excusing any of today's security professionals for not having established a unified view of their cyber exposure and control gaps.

SECTION 2:

Security teams facing further tool overload

The number of security tools in use among enterprise security teams has increased relatively sharply over the two years, by around 19%.

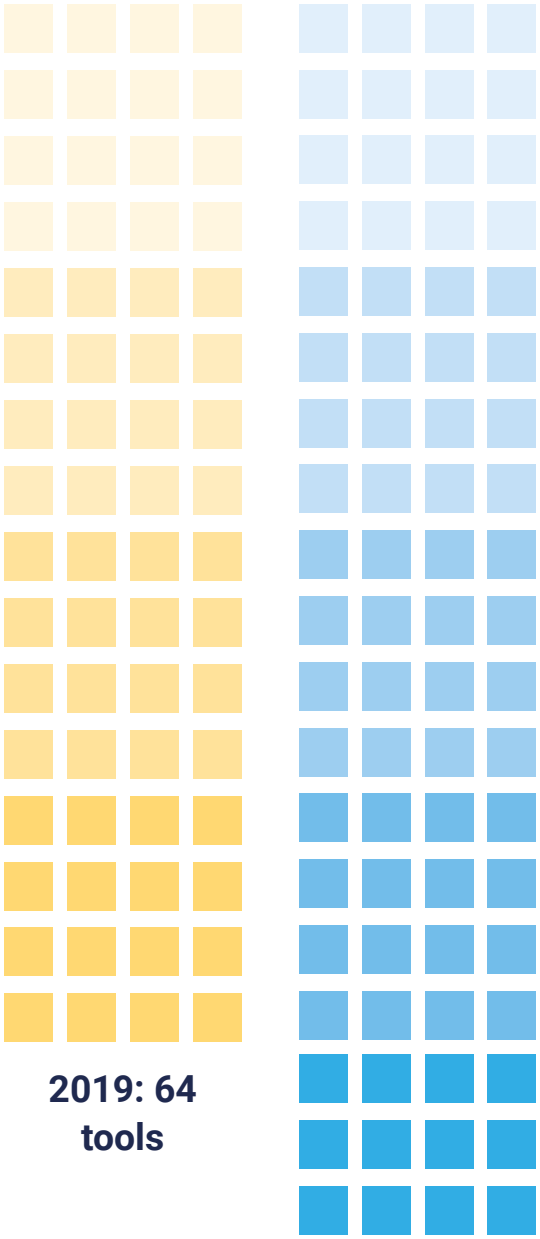
Reaching for more security tools is an understandable reaction when threats are rising in severity, frequency and complexity.

However, where the addition of tools is warranted, a commensurate increase in cyber effectiveness should be the goal. As we show in later findings, fewer than expected security leaders report the highest levels of confidence in matters relating to security controls and visibility.

Simply anticipating a more secure posture by virtue of deploying more tools would be a short-sighted strategy. Far better would be to have a robust strategy in place to ensure each tool is optimised in its deployment, and demonstrably contributing to reduced risk.

The rise may be expected as businesses implement niche tools that look to solve a particular problem alongside the existing tools that address issues elsewhere. The following findings have also likely risen in line with increasing budgets as a direct response to the pandemic and the security obstacles – from a rise in threats to cloud-enabled remote working – it has posed.

The average number of security tools used by enterprise security teams

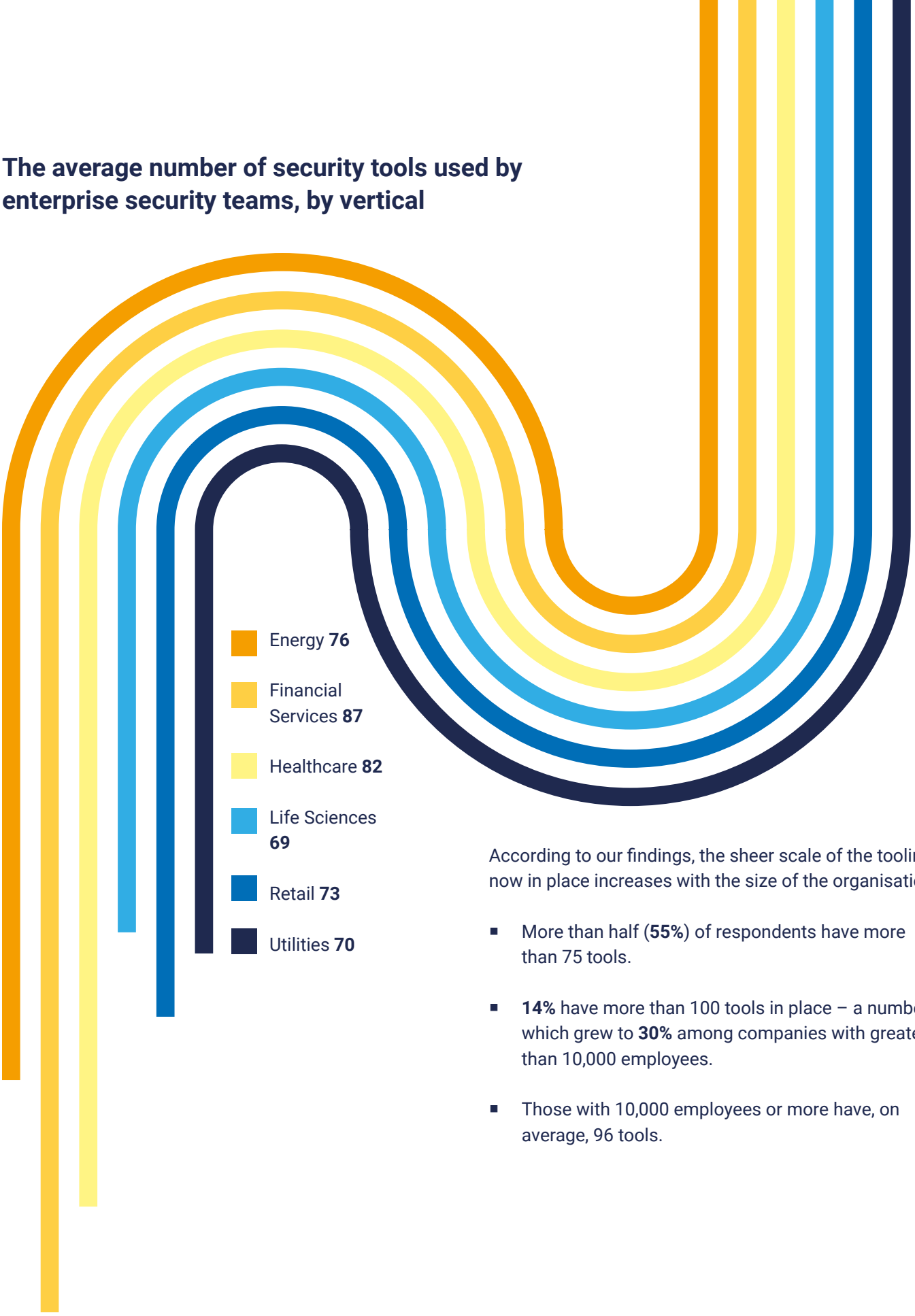


2019: 64 tools

2022: 76 tools

Note that for a true like-for-like comparison, Panaseer has segmented the data from its 2019 Security Leaders Peer Report to focus on the comparable companies sized 5,000 to 10,000+ employees.

The average number of security tools used by enterprise security teams, by vertical



According to our findings, the sheer scale of the tooling now in place increases with the size of the organisation:

- More than half (**55%**) of respondents have more than 75 tools.
- **14%** have more than 100 tools in place – a number which grew to **30%** among companies with greater than 10,000 employees.
- Those with 10,000 employees or more have, on average, 96 tools.

SECTION 3:

Time spent on manual reporting is unsustainable

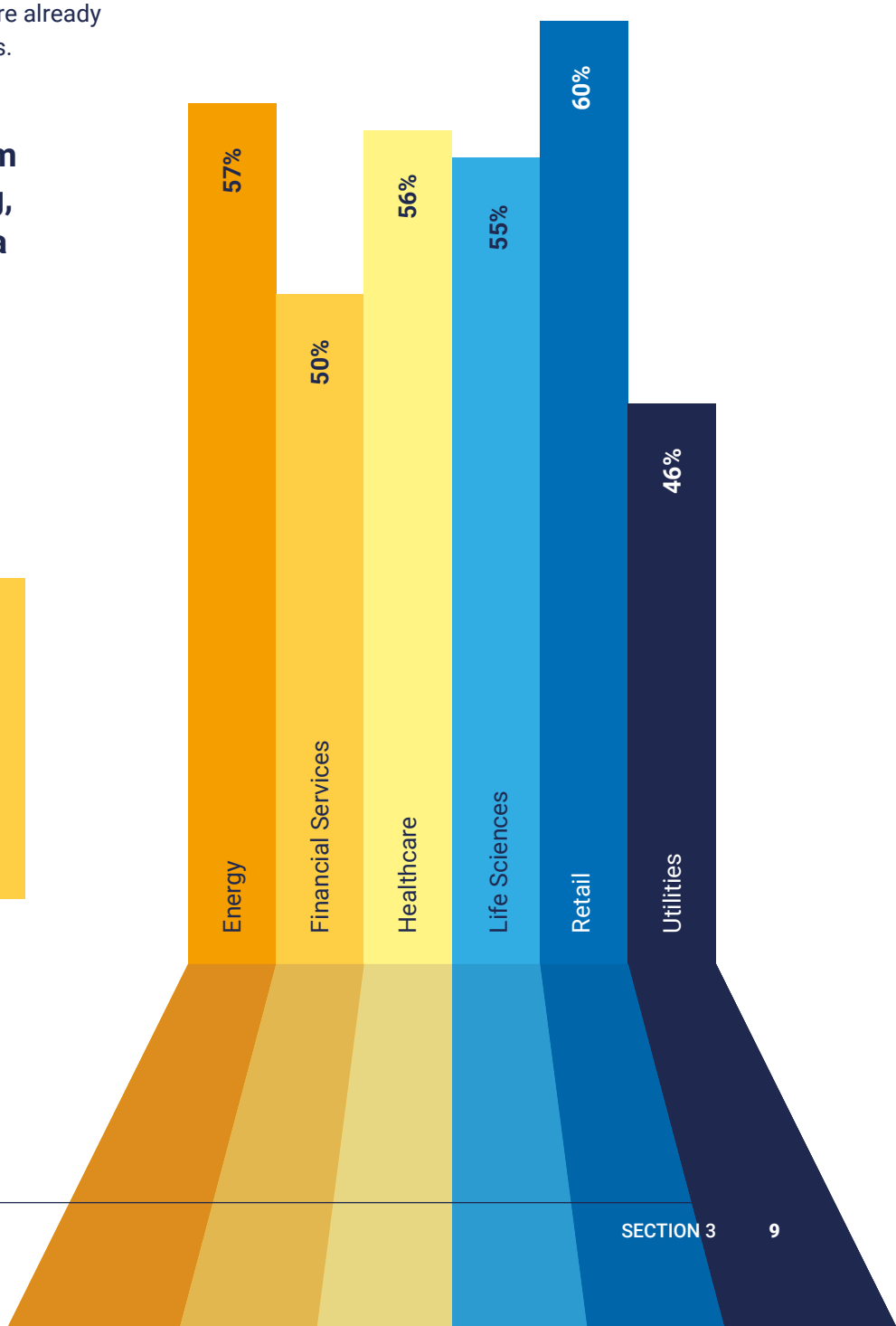
Despite the many tools they have in place today, or perhaps because of them, security teams spend more than half their time (**54%**) manually producing reports, formatting and presenting reports. This is up by **35%** on a like-for-like basis compared to 2019 when security teams were already overwhelmed by manual reporting demands.

The average percentage of overall enterprise security team time spent manually producing, formatting and presenting data

40%
in 2019

54%
in 2022

The average percentage of overall enterprise security team time spent manually producing, formatting and presenting data, by vertical



Note that for a true like-for-like comparison, Panaseer has segmented the data from its 2019 Security Leaders Peer Report to focus on the comparable companies sized 5,000 to 10,000+ employees.

This rise in implemented tools and manual reporting may be attributed to a combination of factors, including greater regulatory pressure on security teams, the rising threat landscape, and more interest from boards compared to previous years. For example, due to a more mature knowledge of cybersecurity, stakeholders and board members are increasingly active in the security aspect of their businesses.

When asked about their leaderships' awareness and understanding of ransomware protection levels across the business, 84% of respondents agreed that their board was actively interested in this subject, with 91% regularly reporting to their board on ransomware protection.

Naturally, heightened understanding of cyber hygiene among this stakeholder group leads to more informed requests to, and assessments of, their security teams. Ultimately this causes a positive ripple effect across the organisation as security teams strive to meet the needs of the stakeholders. It may explain why, for example, our research found **ransomware protection is a budgeted priority for 86% of organisations over the next two years.**

Whatever the case, it's clear that security teams are spending an inordinate amount of time focusing on manual reporting compared to the functions of their role. The fact that these teams are spending more than half their time creating these reports indicates a lack of solutions available to support them in this area. From marketing to field support and back-office admin, no other branch of a business requires such extraordinarily manual endeavor from its teams.

This is all the more remarkable considering the great strides in automation achieved across modern organisations; strides that predate our 2019 research, let alone 2022. Across business functions, automation can be widely implemented to not only alleviate inefficiency but also to ensure data accuracy. Manual reporting to the extent revealed within security teams will almost certainly bring with it data quality issues. Whether manual or otherwise, spending more than half of your time (**54%**) reporting on activities rather than conducting them is a breathtaking return.

One could argue that, compared to more established business functions, security teams are still finding their way to the optimum processes, industry standards and best practice. And that being left to their own devices to report on the metrics that matter to them and their customers, it is no wonder that inefficiencies may result. The deep and profound worry is that such a hypothesis should show a gradual improvement over time. Teams are consuming more of their time on manual processes, not less.

Our findings also reveal that knowledge sharing, an exercise common in many industries, is lacking among security professionals.

43% of security professionals have little-to-no understanding of the best practice measures, metrics, policies and risk appetite used by peer organisations, even though 99% of them believed this information would be valuable to them.

The security industry must mature to a point that efficient, industry-wide solutions for monitoring and reporting on controls can become commonplace – much like Salesforce is for the sales function. Only then can professionals easily see the extent and success of their security measures and identify the right metrics for the right stakeholders.

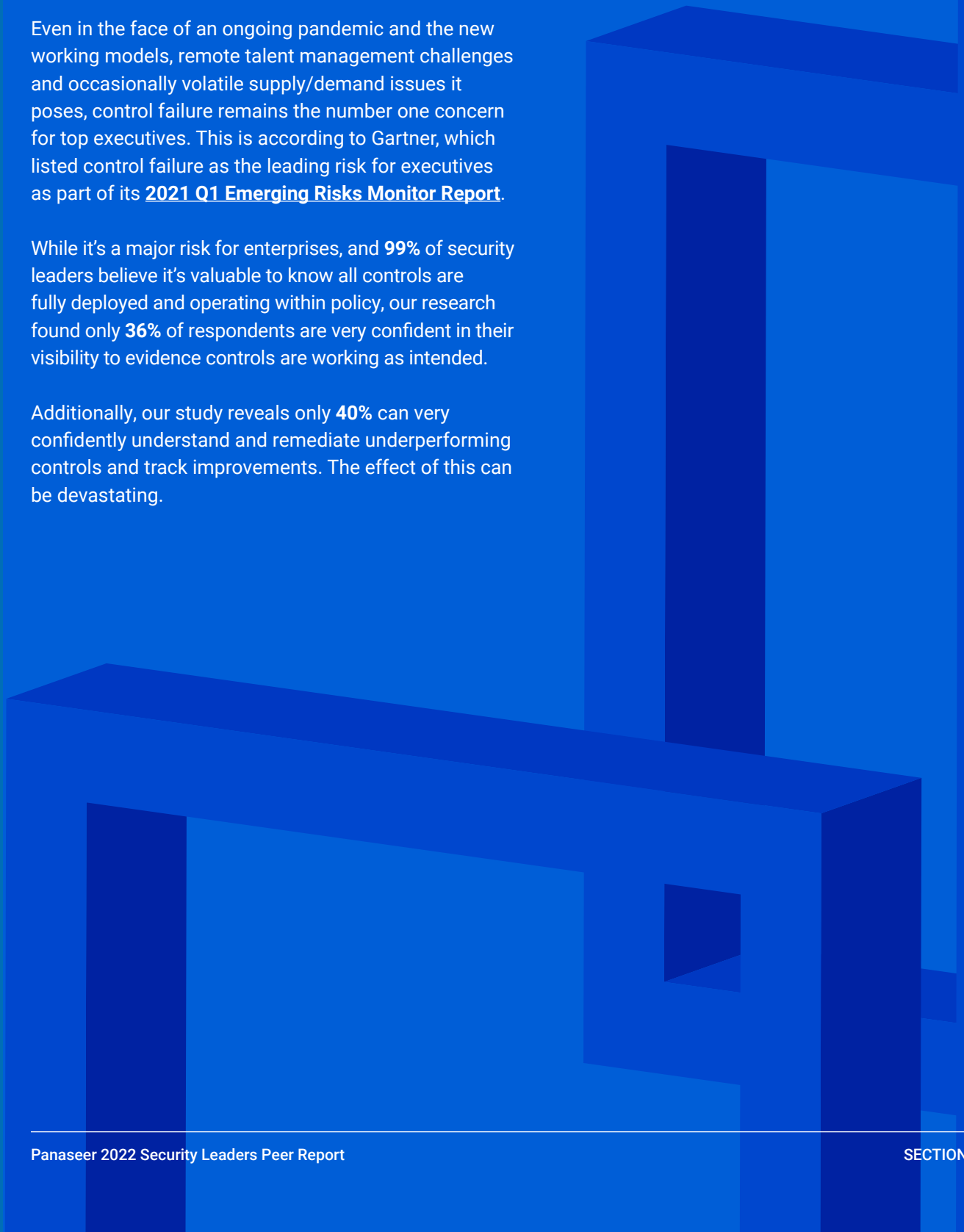
SECTION 4:

Lack of insight driving security control failures

Even in the face of an ongoing pandemic and the new working models, remote talent management challenges and occasionally volatile supply/demand issues it poses, control failure remains the number one concern for top executives. This is according to Gartner, which listed control failure as the leading risk for executives as part of its **2021 Q1 Emerging Risks Monitor Report**.

While it's a major risk for enterprises, and **99%** of security leaders believe it's valuable to know all controls are fully deployed and operating within policy, our research found only **36%** of respondents are very confident in their visibility to evidence controls are working as intended.

Additionally, our study reveals only **40%** can very confidently understand and remediate underperforming controls and track improvements. The effect of this can be devastating.



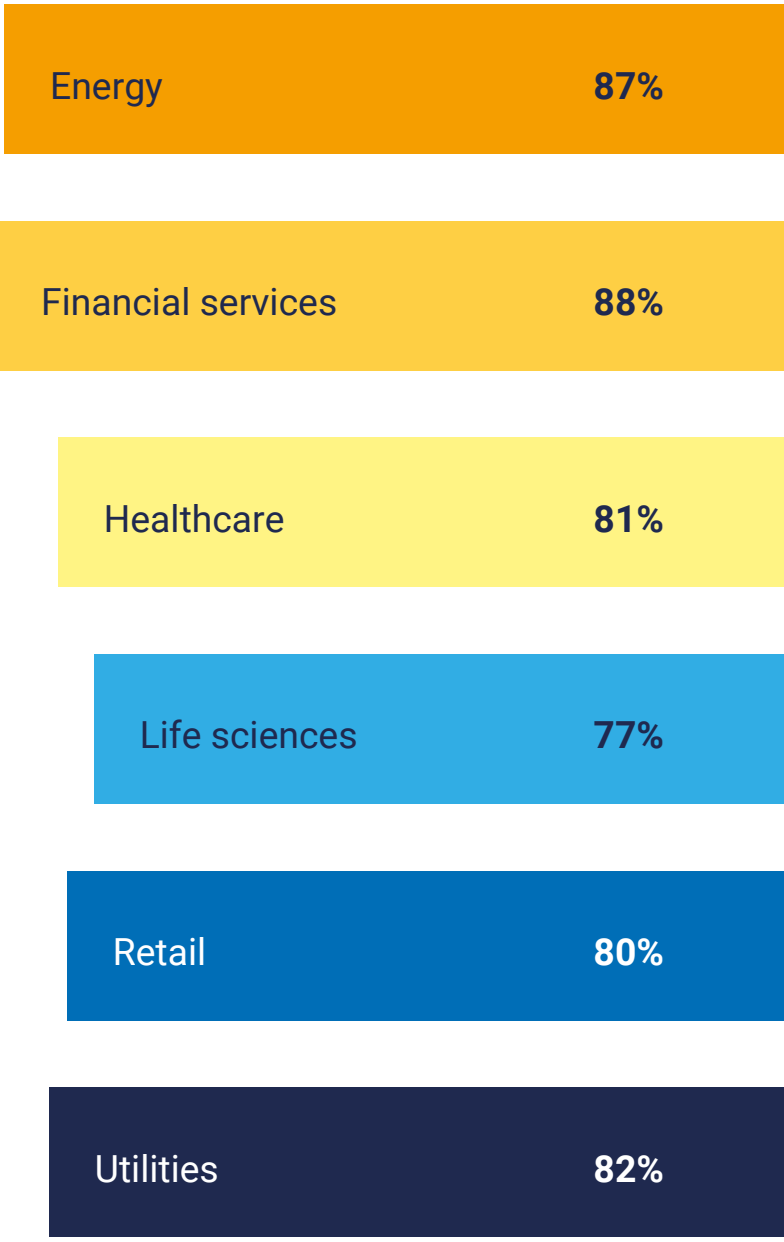
This apparent lack of self-confidence is further borne out when discovering that an astonishing **82%** of security leaders have been surprised by a security event, incident, or breach that evaded a control(s) thought to be in place.

It's usually multiple control or compensating control failures that occur, on average five times, that leads to a significant event, incident (an event that compromises the integrity, confidentiality or availability of an information asset), or breach (an incident that results in the confirmed disclosure of data to an unauthorised party).

On average, an event, incident or breach is the result of **five** control failures.

Enterprises in both the UK (**87%**) and US (**78%**) are falling victim to these control failures, with financial services firms (**88%**) appearing to be most vulnerable compared to other industries.

Percentage of enterprises surprised by a security event, incident, or breach which evaded a control they believed was in place to prevent it



58% of respondents do not have a high degree of confidence in their ability to continuously measure security controls that mitigate the infiltration, propagation and exploitation of a successful ransomware attack – a level that decreases the larger the organisation is (only **52%** of the 5,000–5,999 employee cohort are very confident, compared to just **30%** for organisations above 10,000 employees). Furthermore, just **40%** of security leaders are very confident they can remediate underperforming controls and automatically track improvement over time. Even this level of confidence is likely to be misplaced, given the evidence of actual events.

There is also a clear dissonance between how security teams perceive their performance and the reality of their ability to properly understand and act upon their cyber hygiene. As stated above, over **80%** of security leaders were surprised by an event, incident or breach as a result of a control failure. And yet **99%** of respondents claim to be satisfied with their ability to prioritise security risk and make security decisions. Once again, looking in more detail reveals that only **34%** are "very satisfied" – something that many of them may be overstating.

Evidently, confidence among respondents does not ensure control success, and improved Continuous Controls Monitoring looks to be the only solution that is able to provide control assurance.

The last word

Security leaders have encountered extraordinary headwinds between 2019 and 2021 and pulled off incredible feats to allow the rapid and sustained transition to cloud and new remote working practices. This, coupled with the inexorable advance of cyber threats, continues to make the job of identifying and managing cyber risk incredibly challenging.

Against this backdrop, the reality of life at the coalface of an enterprise security team appears somewhat more precarious than even the stated confidence levels of security leaders may claim. Teams must be struggling under the increasing weight of tooling and manual processes; how else to explain the continuing absence of clear asset visibility, or the 'surprise' breaches and other security events caused by controls that were thought to be in place but were not?

Most security leaders are candid about being less than supremely confident about core functional responsibilities: knowing that all necessary controls are in place, being able to continuously measure key controls that mitigate the spread and impact of ransomware attack vectors, identifying and taking action to improve underperforming controls, and more.

Almost half of organisations (**43%**) still have limited understanding of, or access to, best practice measures, metrics and policies. A full **99%** of security leaders believe it would be valuable to be able to report and prioritise security risk based on the business process it supports and crown jewels of the business. Another strong area of consensus among the sample points to a possible solution to these misgivings; one that introduces much-needed automation of visibility, controls management and coverage through a single console, thereby avoiding additional burden on already overburdened cyber personnel.

In total, 79% of security leaders are likely to implement a Continuous Controls Monitoring platform to measure and advise on control effectiveness across their entire security estate within the next two years.

A little over **20%** of enterprises in our sample have already implemented a Continuous Controls Monitoring platform.

Such platforms promise an enterprise-wide view of assets and wider cybersecurity posture to enable the continuous monitoring of controls and measurement of their performance against a range of essential metrics.

A notable aspect of this projected adoption is that the largest organisations appear most likely to implement CCM solutions. Correlating this with our other findings, which show larger organisations must contend with the greatest number of tools, controls and technologies, highlights the urgency in addressing the scale and complexity of the security controls challenge.

Methodology

In September 2021 we commissioned Censuswide to survey 1,200 security decision-makers in security roles at the VP level and above. The respondents are split evenly, with 600 from the UK market and 600 from the US.

Respondents include CISOs, senior risk officers and more, working across companies with 5,000 to 10,000 plus employees (compared to 2019's respondents hailing from companies sized 1,000 to 10,000 plus) covering the life sciences, energy, healthcare, retail, utilities and financial services industries.

For a true like-for-like comparison, we have segmented the 2019 data to focus on comparable companies sized 5,000 to 10,000 plus employees.

About Panaseer

Panaseer is the first Continuous Controls Monitoring (CCM) platform for enterprise security. The platform uniquely correlates data from all security tools to identify and measure missing assets and control gaps so that organisations can optimise security controls, tools, processes, and personnel.

CCM has become a required capability for regulated organisations as it solves one of the biggest challenges in cybersecurity today – control failure. This emerging technology has been recognised in Gartner's Hype Cycle for Risk Management in 2020, and featured in Momentum Cyber's Cybersecurity Almanac in 2021 as a next generation technology that will shape the future of cybersecurity. Panaseer has been included as an inagural vendor in both.

Panaseer customers include the world's largest institutions and enterprises.

For more information visit: www.panaseer.com

We've got you covered

Continuous Controls Monitoring for enterprise security