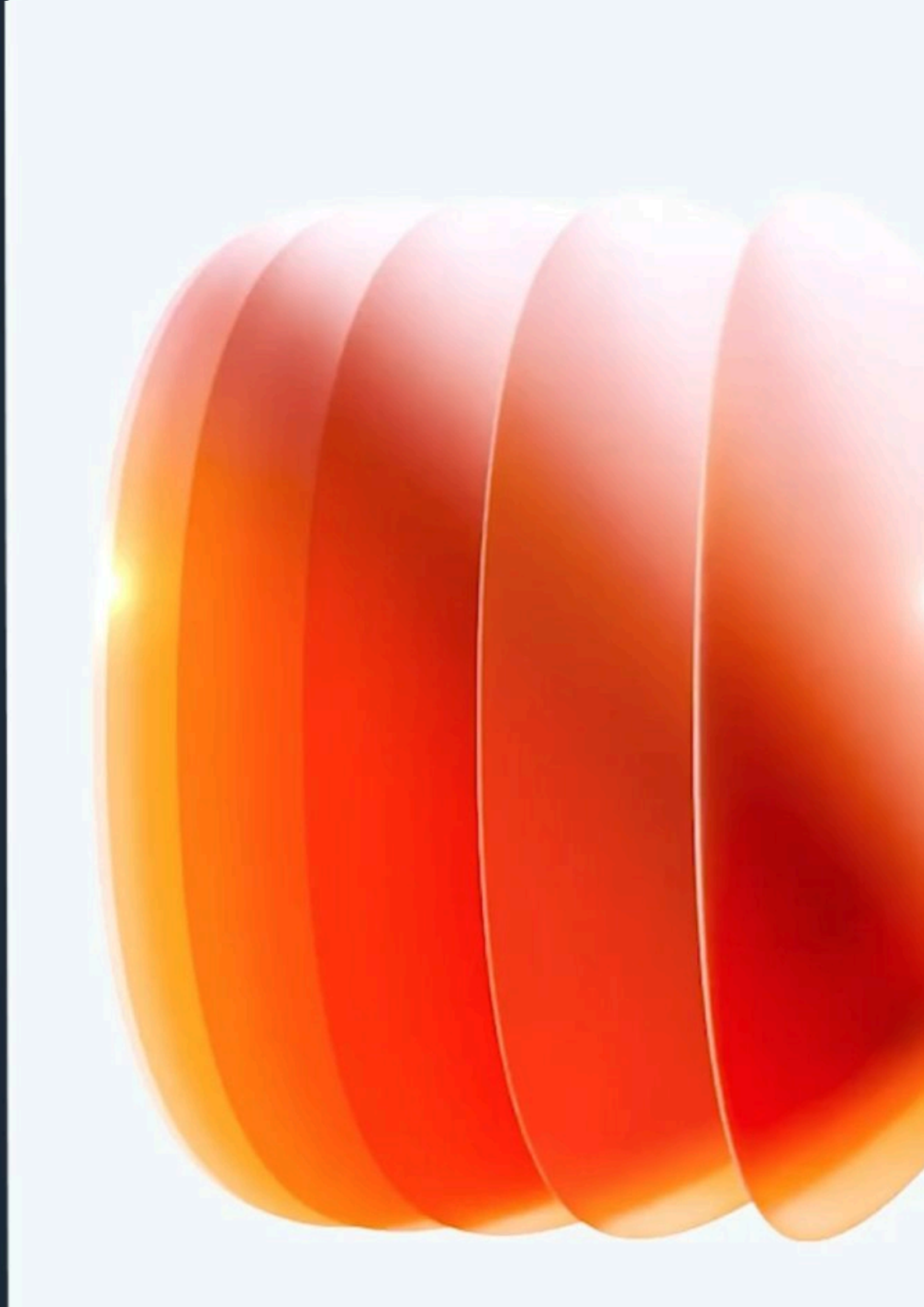
Tipping the Cyber Scales: How Defenders Can Get back in the Game

Qodea

Google Cloud Partner



Qodea

Foreword by Ed Russell

CISO Business Manager

Foreword by Ed Russell

CISO Business Manager

Organisations that have experienced a cyber attack understand only too well the lasting damage it can cause. Those that have not, read every day about data breaches, denial of service attacks and ransom demands with a sense of foreboding. The impact of even a relatively small cyber attack can be severe, with financial, operational and reputational repercussions.

As cyber attacks become more frequent, advanced and insidious, continually evolving your cybersecurity measures is the only way to protect against an ever changing threat. Businesses must outpace and outsmart an increasing number of unexpected and invisible opponents, or shoulder the risk of potentially catastrophic harm to your business.

As Europe's largest Google Cloud technology partner, we've been working for almost two decades with organisations across a range of sectors, to help them ensure their digital environment is safe and secure, both in the here and now and for the future.

Executive Summary

Executive Summary

The cost of cybercrime is **predicted to reach $10.3 trillion annually by 2025,** with businesses shouldering the lion's share of these losses. Across all the sectors we surveyed, investment in cybersecurity is increasing, yet there is a perception that the cost of cyber attacks is outstripping cybersecurity investment.

The reasons for this are multifaceted. The attack surface (i.e. the range of entry points for unauthorised access to a company's systems) is widening, the complexity of IT is increasing, and there is a growing scarcity of skills and resources to tackle the problem.

With the rapid evolution of game-changing new technologies like GenAI, we wanted to get a deeper understanding of the key concerns facing IT leaders from across the retail, financial services, manufacturing and public sectors.

Here's what we've found:

The level of risk is growing across all sectors with 90% of respondents saying the risk and severity of cyber attacks has increased in the past year.

The 'attack surface' is a major issue with 61% saying the attack surface is 'impossible to control'.

Cyber investment is increasing, but many feel it's failing to make the right impact. 97% of the businesses we surveyed have increased cyber investment, but 55% still feel less secure today than last year.

Security risks weigh heavily on teams' minds, with 87% telling us that security risks keep them awake at night. Ransomware/malware, a lack of visibility and identity were the top three concerns.

The explosion of new technologies is a concern, with 79% of security and IT leaders believing that GenAI is going to 'change the game' for cybersecurity, leaving them feeling unprepared.

Many data governance and controls is a challenge, with an alarming 71% of respondents lacking access to and control over data, while 67% felt unable to apply governance and controls consistently.

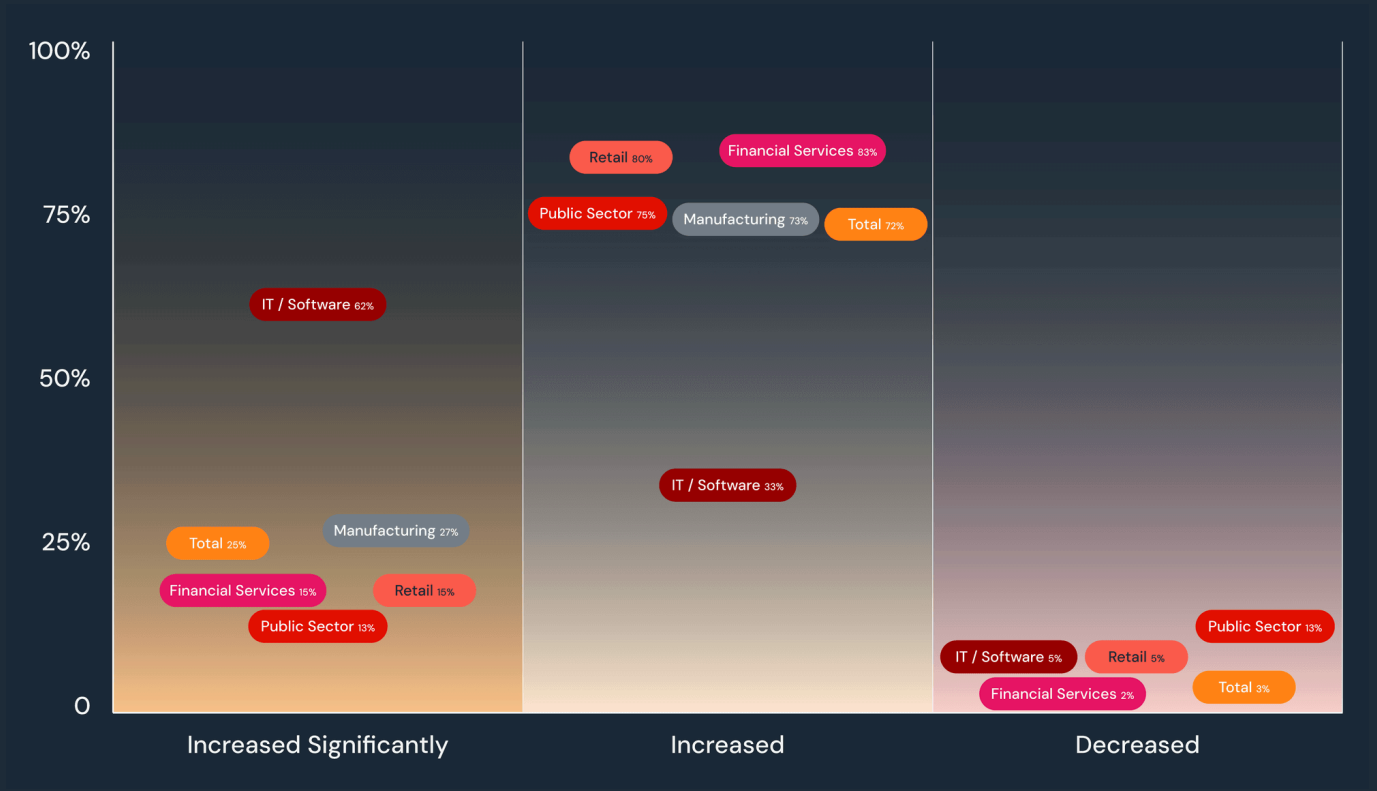
Qodea

Investment is increasing, but it’s not touching the sides

Investment is increasing, but it's not touching the sides

Almost all respondents (97%) said they have increased cybersecurity spending in the past year (see fig. 1), with 62% of respondents from IT companies saying they'd had significant increases. Public sector had some budget cuts though, with 13% saying their budget had decreased.

Fig. 1: **To what extent has your security budget changed in the past twelve months?**



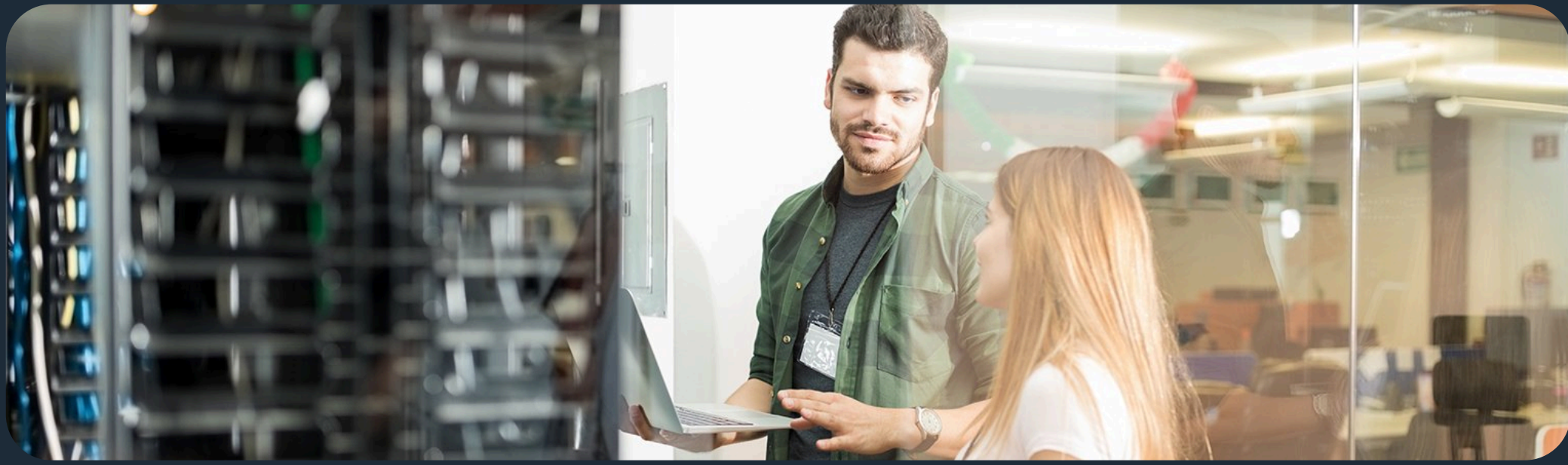
Despite higher investment in security measures, many of our respondents feel the threat is still ever present. Money alone cannot stem the tide of cyber threats. Ultimately, in the face of determined attackers, businesses need to ensure that investments are being made in effective security that reduces the attack surface.

71% believe that any company that thinks it's secure is lying to itself.

61% don't feel confident that the level of investment they are making in cybersecurity will be enough to reduce their overall risk.

55% say despite continued / increased cybersecurity investment they feel less secure now than they did a year ago.

57% say it doesn't seem to matter how much they spend on cybersecurity, the bad guys keep on winning.



While there is an element of realism to those who feel they are fighting a losing battle, this does not mean security teams' prospects are doomed. Many attackers will pick off the lowest hanging fruit – meaning those who are able to shift to the middle of the pack greatly improve their risk posture. Key to this is smart investment and measurement. Effective deployment, controls and purchasing, coupled with proactive, continuous testing and measurement is crucial.

Ed Russell, CISO Business Manager

Case in point: sky

LINK TO CASE STUDY

Challenge: As a multi-cloud consumer, Sky needed a smarter, more consistent, and efficient way to identify fail points and breaches faster.

Solution: Qodea implemented a cloud-based automation solution to speed up processes and improve security, while migrating from a custom DNS to Google Cloud DNS.

Benefits:

Reduced cost and risk of manual errors introduced by manual policies.

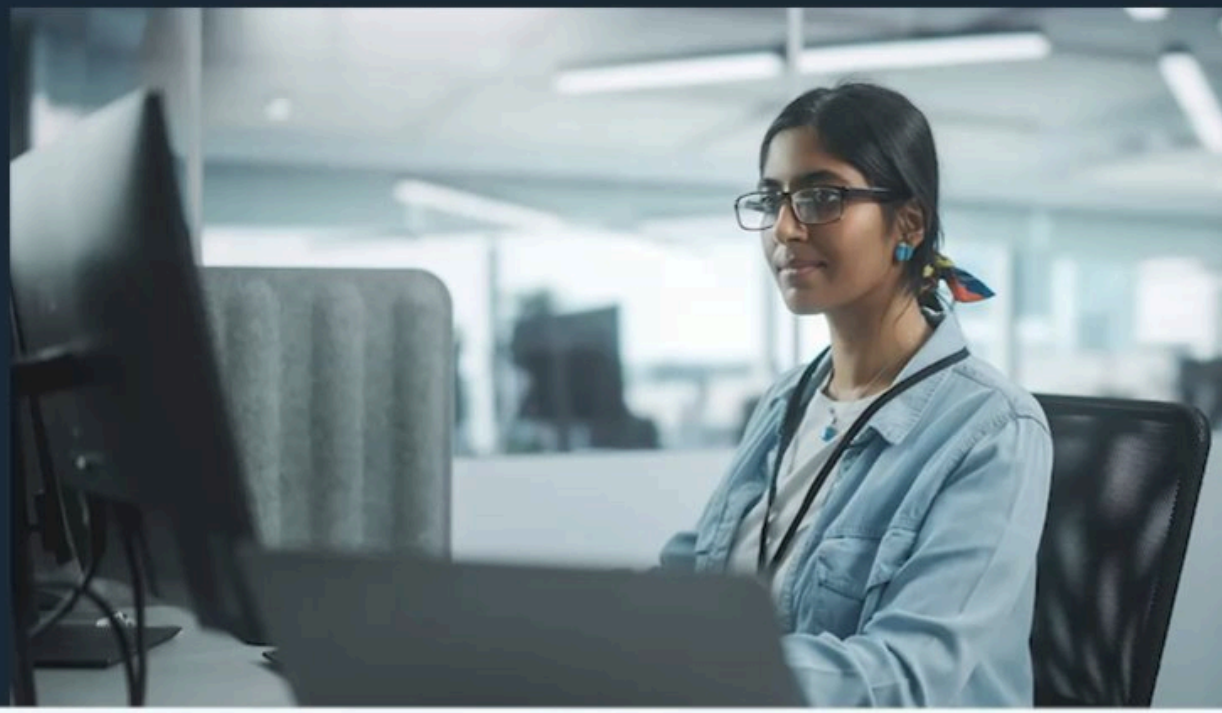
Eliminated hardcoded credentials to improve security.

Reduced risk of breach while paving the way for future innovation.

Qodea

More to protect, greater complexity

With a splash of déjà vu



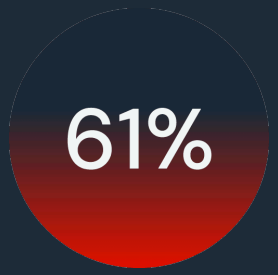
More to protect, greater complexity – with a splash of déjà vu...

As new technologies like Generative AI (GenAI) become readily available to businesses, **they offer exciting opportunities to driver greater efficiency and transform customer engagement.**

While this is an exciting prospect for businesses, it is also an opportunity for cyber attackers.

These risks must be managed effectively for companies to reap the rewards, yet many businesses lack the expertise, tools and processes to ensure their secure deployment.

90% say the risk and severity of cyber attacks has increased in the past year.



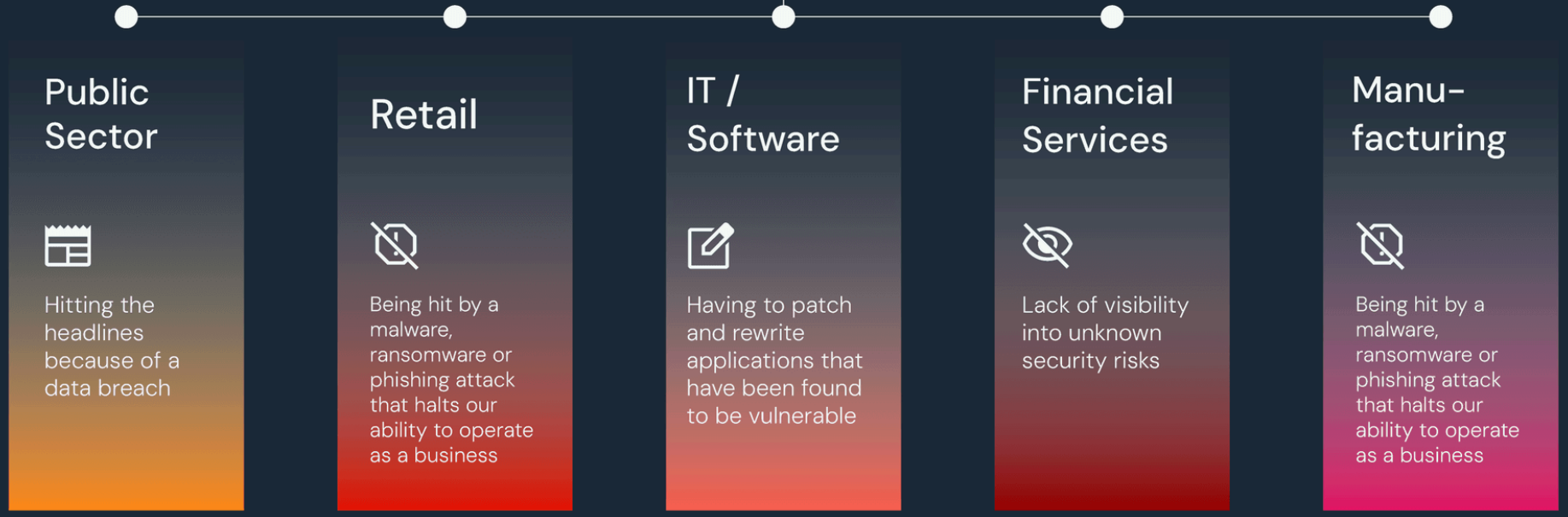
61% think the attack surface is getting so wide, it's impossible to control.

79% believe Generative AI is going to change the game when it comes to cyber attacks and they are not prepared - a figure that rises to 94% for those in the public sector.

The Cyber Opportunity for GenAI:

While cutting edge technologies like GenAI open up new opportunities for cyber-criminals, many of the threats and challenges security teams face are familiar territory (see fig. 2). 87% of respondents said security risks keep them awake at night, putting teams under a heavy burden. Yet when looking more closely at those threats – such as social engineering, malware, ransomware, identity, lack of visibility, vulnerability exploits – they are all areas that have been on the CISO watch list for many years. The difference and challenge is that the context and severity of these threats keeps evolving and must also be viewed through an industry lens, as priorities and operations vary from business to business.

Fig2. Number one threat keeping IT and security leaders up at night, per industry

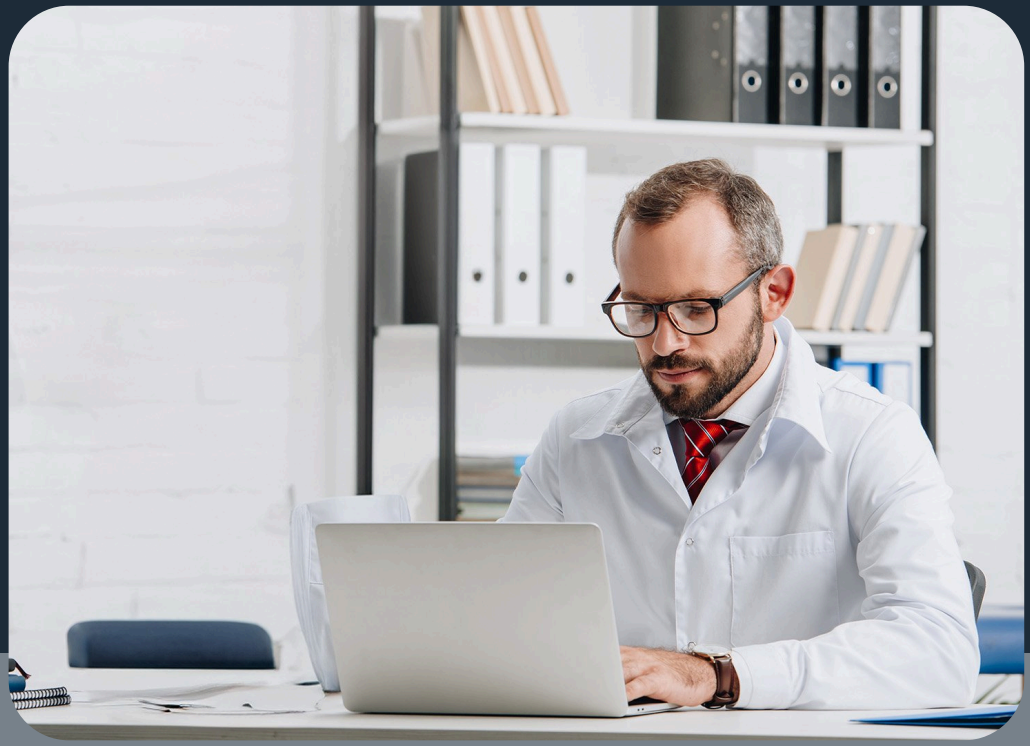


Case in point: GSK

LINK TO CASE STUDY

Challenge: GSK wanted to move away from manually-created and configured organisational policies to make its cloud platform more secure, compliance and auditable.

Solution: Qodea helped GSK to bring in automation migrating over 200 policies, project, and folder exceptions to make it easier for GSK users to make changes.



Benefits:

Reduced duplication, while preventing security violations at the organisation, folder and project level.

Provided a foundation to automate more deployments into Google Cloud.

A more efficient method with a repeatable, single source configuration.

Qodea

The Data Dilemma:

Managing your most valuable asset

The Data Dilemma: managing your most valuable asset

As the old adage goes: if you can't see something, you can't protect it. Yet, as our survey reveals, many organisations have lost sight of their crown jewels – i.e. their data. While most organisations know where data is when it's centrally stored, that data is then often federated by other systems. Complex webs of systems, solutions and services create data silos, making it hard for IT and security teams to know where data resides and how it moves around the business.

This leads to inconsistencies, with data being handled differently across various systems and clouds, resulting in a disparity of control. As data becomes impossible to benchmark, organisations struggle to understand their current data footprint. Building a secure roadmap and applying controls therefore becomes harder, and this could result in some organisations facing regulatory consequences.

67%

67% say their inability to apply governance, policies and controls across environments means security is applied inconsistently.

71%

71% say a lack of access and control over data is opening them up to security risks.

Case in point:

Gloucester Rugby

LINK TO CASE STUDY

Challenge: Gloucester Rugby has a large supporter and membership base and a strong leisure and hospitality business operation, which was resulting in multiple datasets, making it hard to get a single view.

Solution: Qodea built a Google Secure Cloud Foundation platform for internal stakeholders to build a single customer view and become a secure data-enabled business.

Benefits:

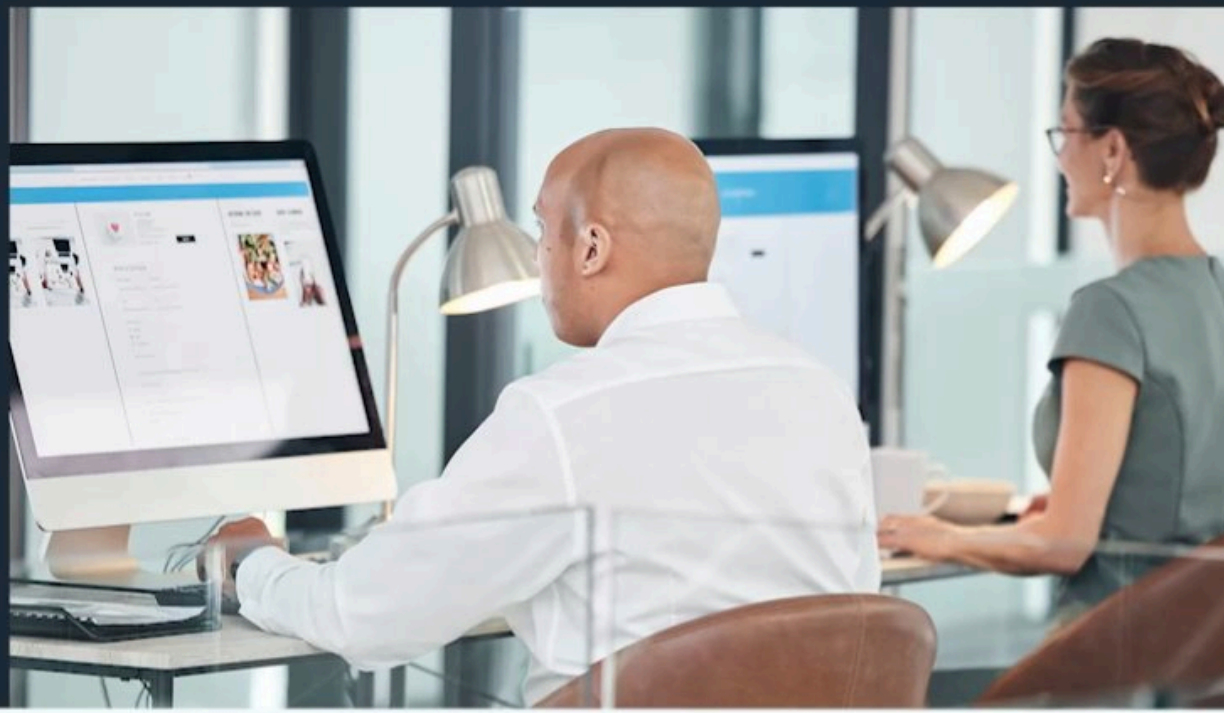
Able to do away with disparate sets of data in multiple systems.

Gained highly relevant information pulled together into a single customer view.

Provided foundational security to improve its digital capabilities.

Qodea

Is Zero Trust the answer?



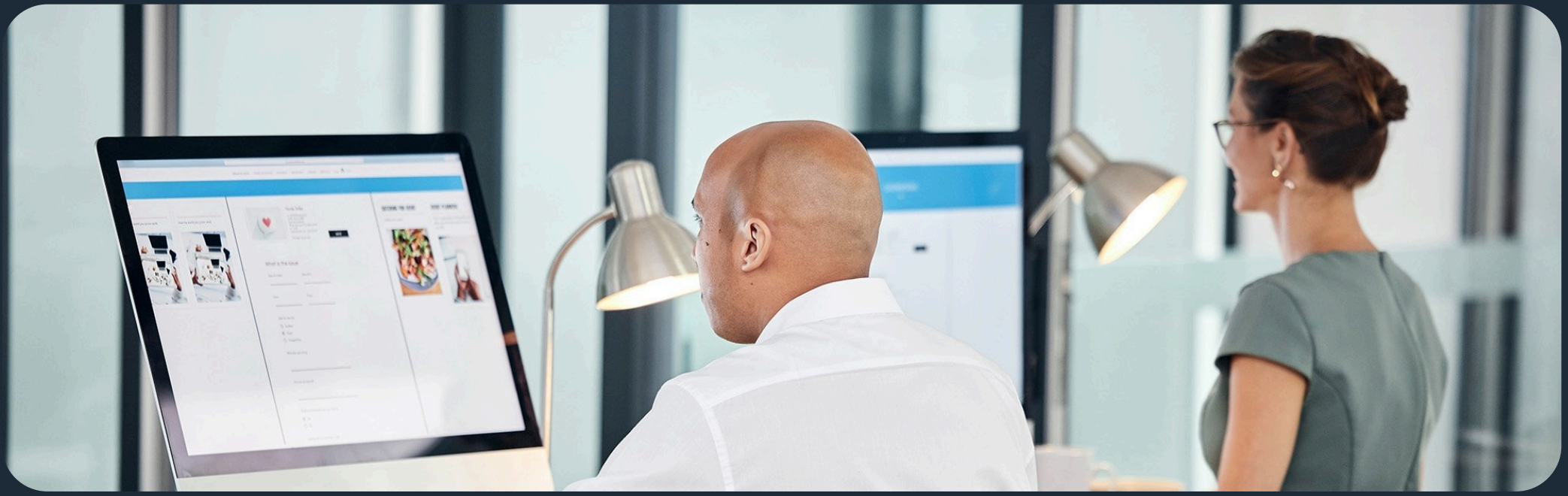
Is Zero Trust the answer?

There has been an industry shift towards 'Zero Trust' models of security –with **over half of respondents (53%) saying they had implemented at least some Zero Trust controls**. Google describes Zero Trust as "a security model used to secure an organisation based on the idea that no person or device should be trusted by default, even if they are already inside an organisation's network." By taking this approach, organisations can contain the impact of attacks. If a system is compromised, then additional checks or verification will be needed before an attacker can move laterally to other systems.

Yet implementing advanced controls like Zero Trust is extremely challenging. While organisations like Google – who implemented a system of Zero Trust in the wake of the Aurora breach in 2013 – have the heft, motivation and resources to embed a Zero Trust ethos, most other companies do not have this at their disposal. Businesses operating at scale lack the visibility and skills to implement controls effectively, leaving gaps and blindspots that can be mobilised by attackers. This is why having systems and tools with Zero Trust already built in has become such a priority.

Top 5 barriers to Zero Trust:

1. Cost
2. Legacy integrations
3. Complexity and size of organisation
4. Lack of resources
5. Lack of skills and understanding



If you're not Google, or in a Google environment, it is really difficult – if not impossible – to really implement Zero Trust. But automation is key. We have worked with companies – like GSK's Global Products and Tech team, to automate the deployment of new policies and configurations, accelerating their Google Cloud journey along the path to Zero Trust. It can be done!

Ed Russell, CISO Business Manager

Qodea

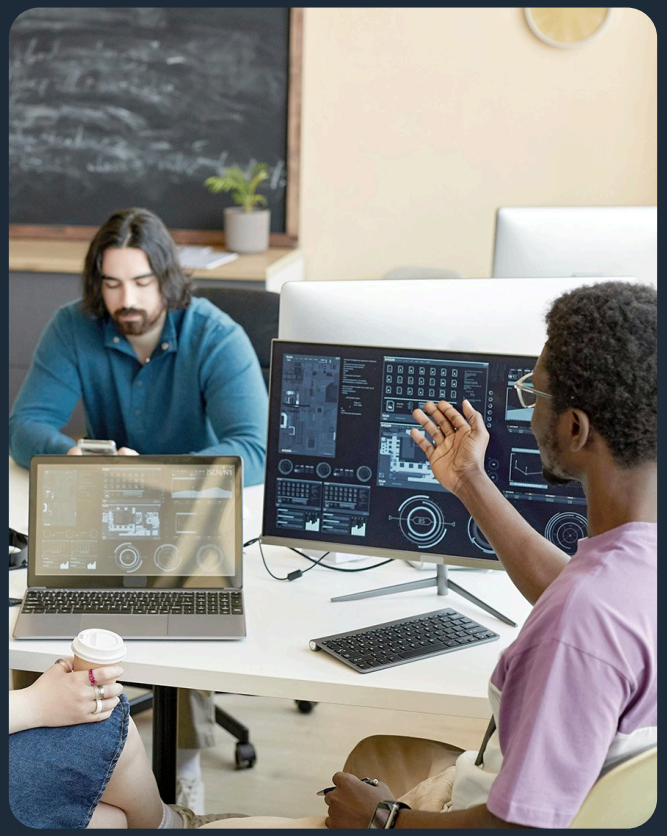
Tipping the cyber scales back in our favour

The importance of a secure foundation

Tipping the cyber scales back in our favour – the importance of a secure foundation

More than two thirds (71%) of our respondents believed that any company that thinks it's secure is lying to itself. When it comes to keeping your business safe, there's simply no room for compromise. You need best-in-class technology, underpinned by the right skills and processes.

As digital regulation changes shape across the UK and Europe, it's not only business entities that will find a greater weight of responsibility on their shoulders. The NIS2 Directive also imposes direct liability on the individuals that lead the businesses within its scope, who could find themselves facing fines or dismissal for compliance failures.



In today's complex digital supply chains, it's no longer simply necessary to protect data while it's 100% in your control; you also need to make sure all third parties with access to that data are keeping it safe and secure. This is the only way you can keep your business compliant and provide complete reassurance to your customers that their information is in safe hands.

With industry best practice frameworks as our building blocks, we use the latest intelligence to stay ahead of emerging threats and adapt our responses, adding to Google's technology with custom tools, so you get the best possible protection across your entire environment.

This may all seem like a daunting reality. The good news is that there are practical, achievable steps that businesses can take -today -to mitigate against risk and ensure they can safely reap the rewards of the digital revolution.

1 

Understand your risks and current security state.

One of the first obstacles to providing your business with better protection against the risk of cyber attack is poor visibility. It can be difficult to know what you don't know, or to outsmart opponents that can navigate your code undetected. Taking time to delve into your security - looking at areas such as system access and authentication, responsiveness, service settings, Mobile Device Management and Preparation and Monitoring - will help you to get a clear picture of the here and now, highlighting gaps.

2 

Create a roadmap with actionable recommendations and opportunities to improve.

You won't be able to do everything all at once, so understanding what the biggest areas of risk are and how they can be addressed is key -helping to identify quick wins that will have the biggest impact. Remember that most attacks are opportunistic, so taking time to ensure you have the right basic controls in place will swiftly move you into a more secure position.

3 

Measure and benchmark to track progress and increase RoI.

Setting goals and measurable targets will help to ensure the project stays on track, while also giving you vital information on which controls are having the most impact. No business has an endless budget: you need to know what is moving the needle and having the greatest impact. This can help to guide future investment and increase RoI on your security tooling.

4 Design and build security into your foundations.

By considering security at the outset of every project, it is easier to embed secure practices than trying to retrofit them down the line. Equally, overhauling legacy SOC processes can help to ensure you can use new tooling effectively -creating templates for how security should look. For instance, by embedding security to the seam of the data pipeline you can create a 'golden image' for every other machine to replicate, so they inherit the same level of security.

5 Invest in the right training and tooling to stay up to date.

Technology moves fast as we know, so embedding a continuous learning culture is key to success. This includes updating processes and standards to become multi-cloud, whilst staying secure, through to investing in training and certification to ensure engineers are up to date on cloud security -right through to ensuring users understand their role as new threats emerge.

While this may feel like a daunting task, **you are not alone.** Working with third party experts can help you to understand your cyber constraints, shining a light on blindspots, while also advising on how to prioritise and move forward.

Qodea

How Qodea can help you on your security journey

How Qodea can help you on your security journey

Google Cloud Partner

SPECIALIZATION
Security
Google Cloud

As Europe's largest Google Cloud and security partner, we've got almost two decades of experience helping organisations lay the right foundations and put essential guard rails in place. Our agility allows us to do this at pace, so that security concerns are no longer an obstacle to innovation.

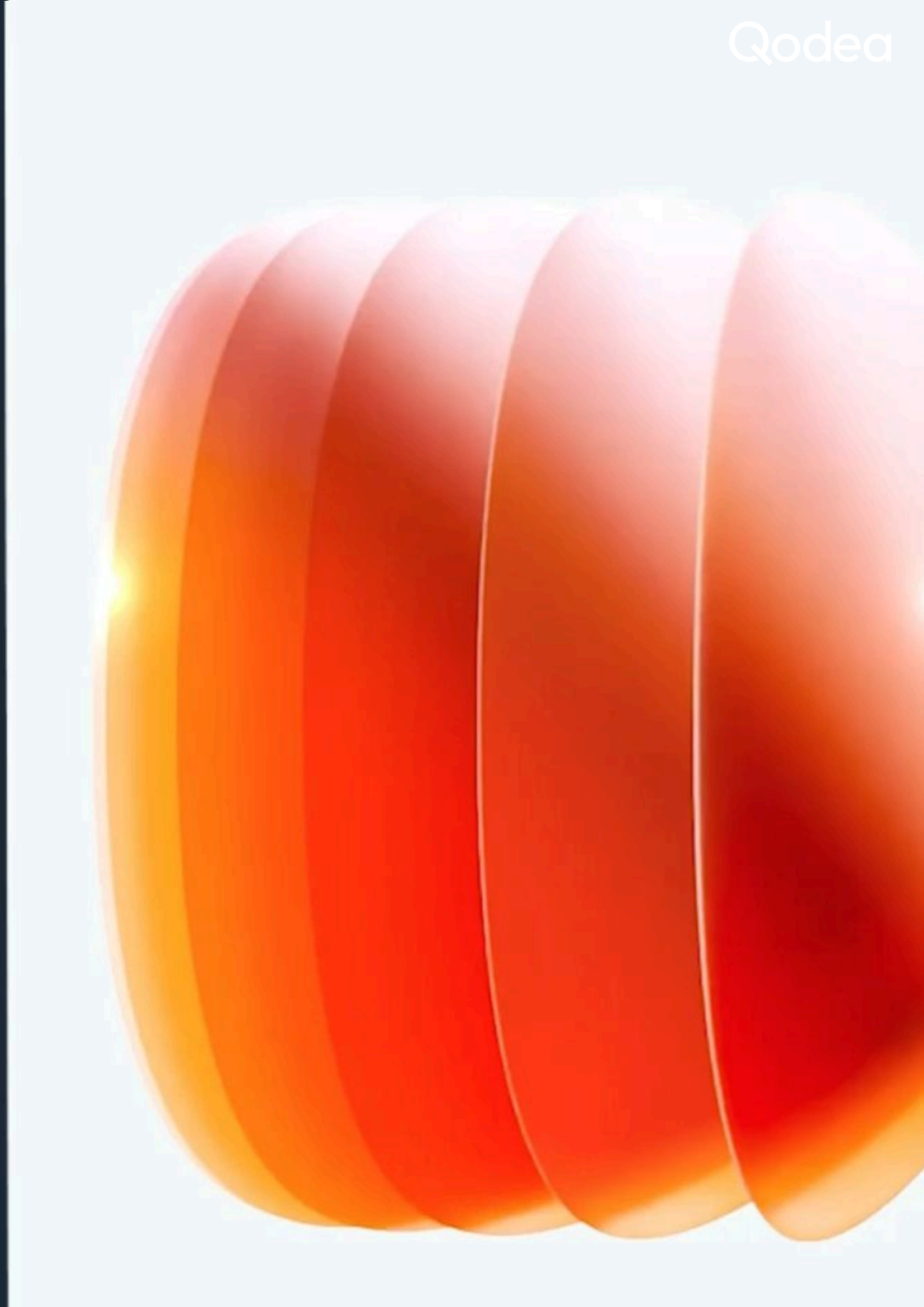
Our talented engineers will support you to protect your entire digital environment as it grows and changes, providing scalable solutions that can evolve as your business does, so you can focus on your broader goals and priorities.

We'll meet you wherever you are on your cybersecurity journey, acting fast to help you define and implement the best solutions for your budget. We'll even help your people adapt to the business changes new security processes will require; using innovative training tools to help your teams understand why security is so critical, how they can make a difference and how to maximise the value of the platforms available to them.

Plan for tomorrow by laying secure foundations today.

Methodology

This survey was conducted by independent research consultancy Sapio Research. 150 UK IT decision makers, working in organisations with 500+ employees were interviewed via an online survey.



Thank you for reading

Tipping the cyber scales: How defenders can get back in the game