

FSNTalent



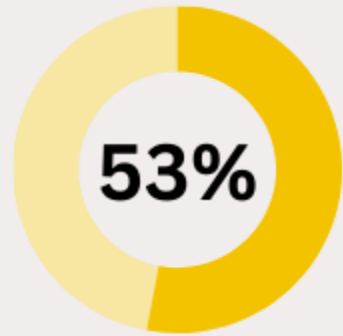
FINDINGS

Cybersecurity and The Role of The Finance Function

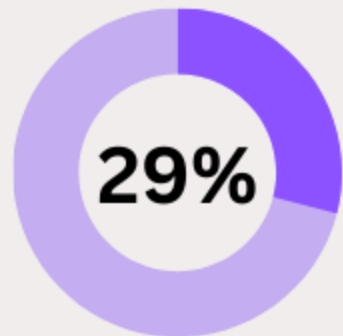
Brought to you by the founders of the Modern
Finance Forum on LinkedIn



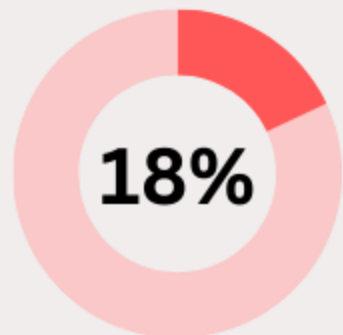
Size of organisation



Small less than 500 employees

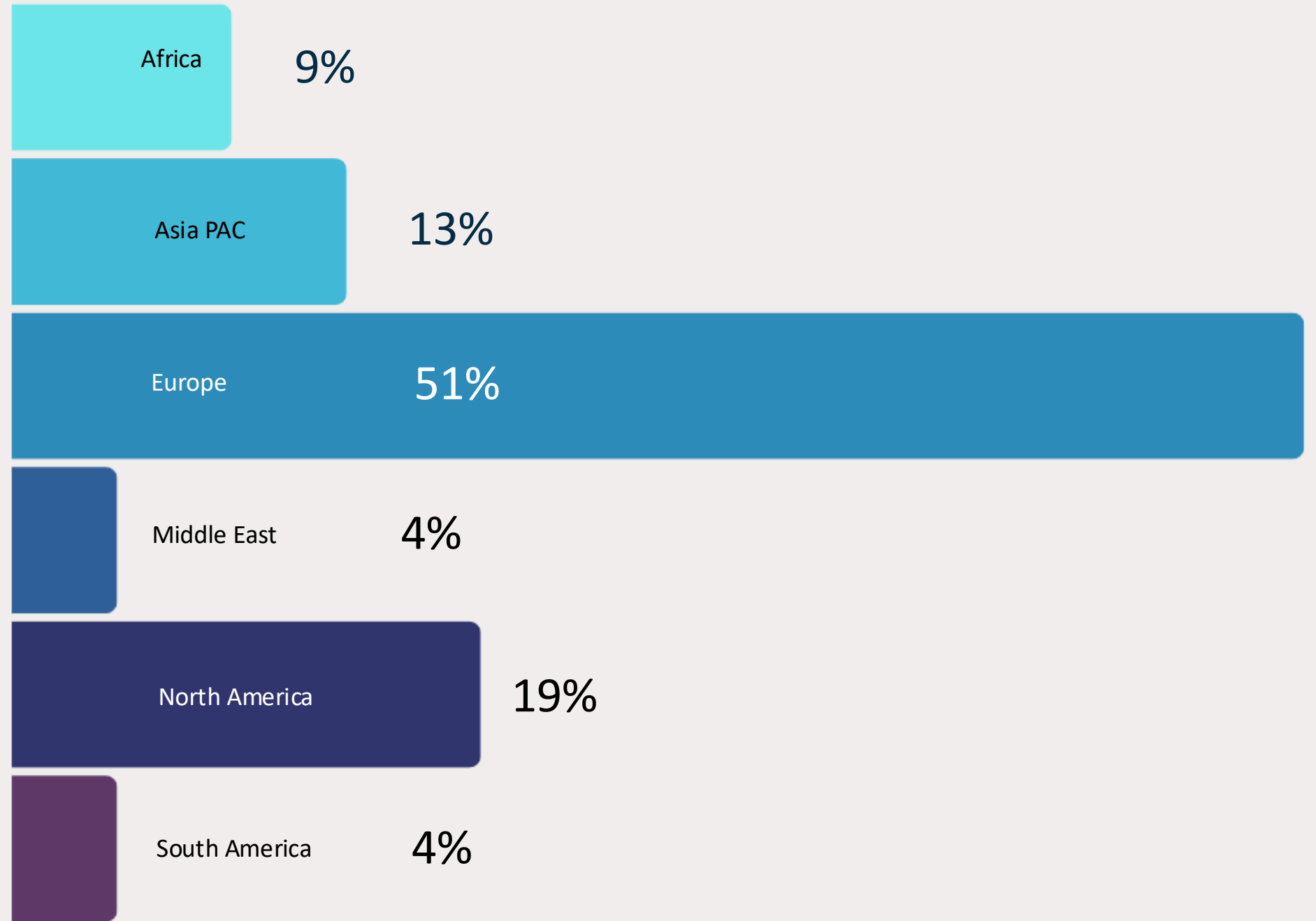


Medium 501 to 5000 employees



Large more than 5000 employees

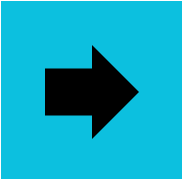
Geography



This report highlights that the **modern finance function is ill-prepared** to master the complexities of cybersecurity.

The modern finance function is responsible for the safe stewardship of a company's assets, yet the rapidly evolving threat from cybersecurity, means that most finance functions neither have the means nor technical knowledge to provide adequate safeguards for their company's operations and data. Only forty-two percent of finance functions are fully engaged in the management of cybersecurity. Ninety-one percent lean heavily on their IT function to provide critical support they need.

So the finance function faces an unenviable dilemma. It is held responsible for the internal control environment, i.e. ensuring that financial data is complete, accurate and authorized, yet its efforts can be easily undermined by weaknesses in data security and confidentiality. Just fifty-three percent of organisations are confident or very confident in their company's ability to secure, sensitive regulated data.



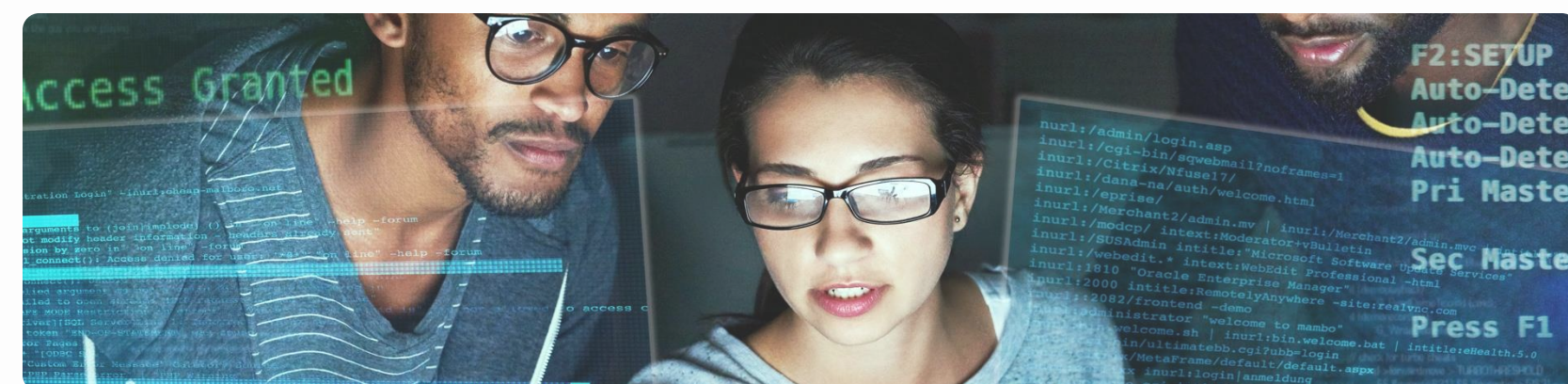
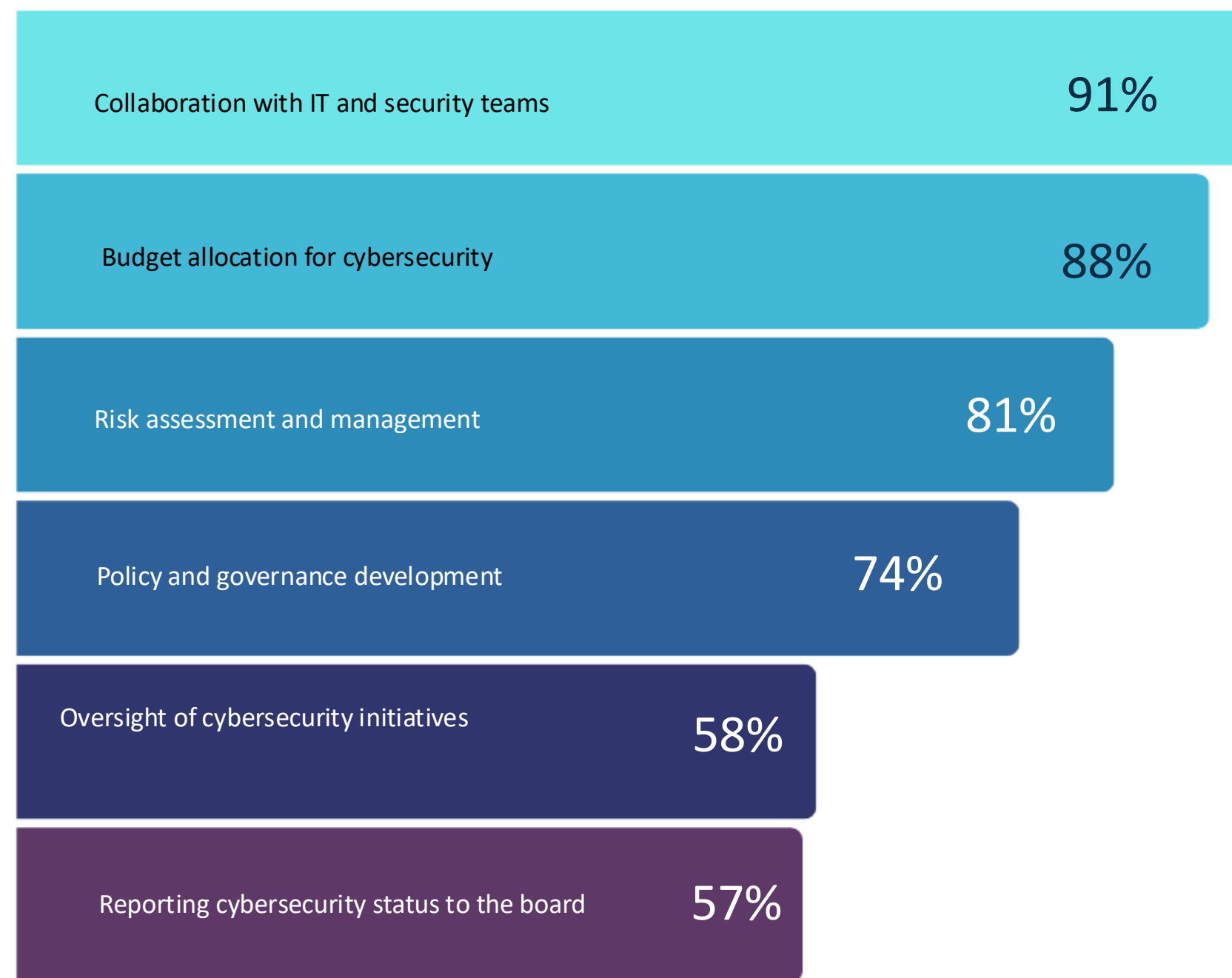
The **internal control** environment is unhelpfully **split** between the finance and IT functions.

Historically, finance functions are the guardians of financial control, but their accounting training leaves them woefully unprepared to deal with the modern complexities of cybersecurity. Although prevention of cyber-breaches could be viewed as part of the internal control environment, ninety-one percent of finance functions, lean heavily on their security team for the technical expertise they need.

Nevertheless, the vast majority of finance functions see it as part of their role to ensure that there are adequate budgets for cybersecurity (eighty-eight percent) and more than three quarters are involved in risk assessment, risk management, policy and governance.

However, board reporting on the status of cybersecurity is judged to be out of scope for forty-three percent of finance functions. Arguably this leaves an unhelpful divide in the management of the internal control environment and raises doubts about who is in overall control.

What specific responsibilities should finance have in managing cybersecurity within their organisation?



Ninety-One percent of finance functions rely on their security team as the first line of defence, yet two-thirds of them outsource cybersecurity to some extent.

In an era where cyber threats are increasingly sophisticated and frequent, the confidence of organisations in their cybersecurity capabilities is alarmingly low.

As a result, many organisations have outsourced much of the burden to third parties, raising the issue of whether it is appropriate to rely so heavily on an external provider for such a sensitive and crucial area of operations.

How self-sufficient is your organisation's cybersecurity?

16%

Poor: We heavily rely on external consultants for the skills, tools and resources we need.

53%

Average: We can provide an adequate level of cybersecurity, but often need external help for complex issues

However, recent events, show that even external providers can stumble. This raises the difficulty of how much capability in cybersecurity should be retained in-house. **In effect, should it be viewed as a core competency for organisations?**

31%

Excellent: Our team is highly skilled in cybersecurity, regularly keeping up with the latest threats and implementing advanced security measures without external assistance.



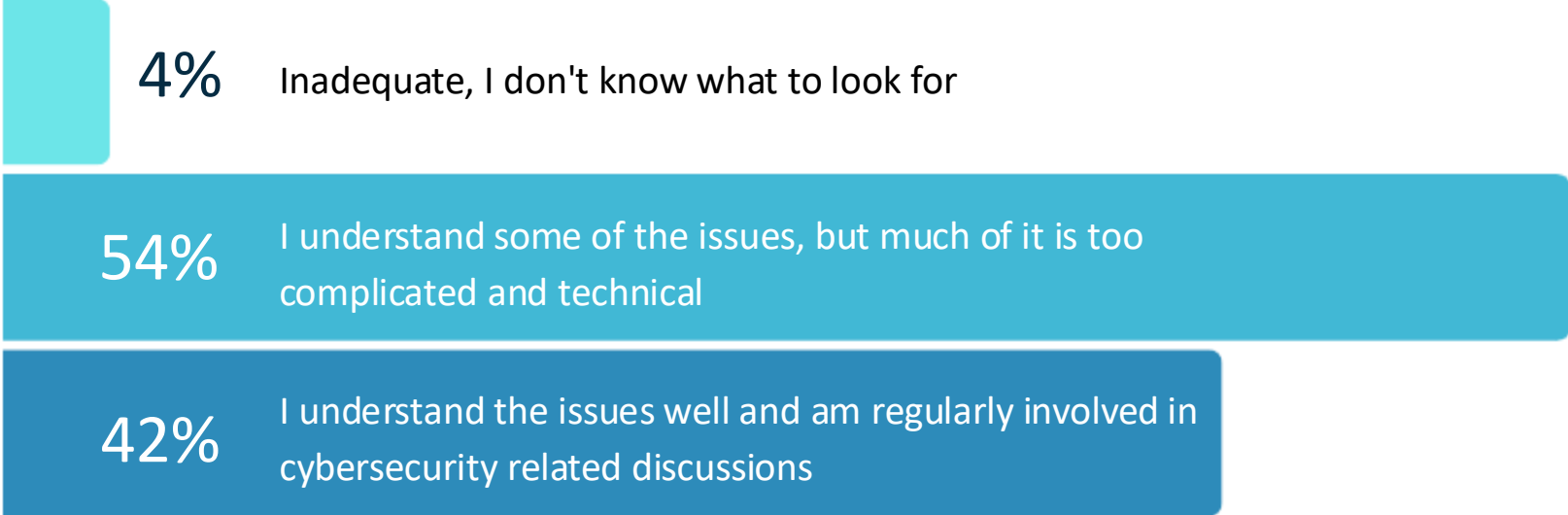
Only forty-two percent of finance functions are **fully engaged** in the management of cybersecurity.

Cybersecurity is a constant threat and challenge to the modern finance function and not something that can be readily brushed aside. In recent months there have been many high-profile data breaches and ransomware attacks in some of the world's leading organisations. In the last year alone, large organisations globally including, Change Healthcare, CDK Global, Ticketmaster, Christies, the NHS (National Health Service) and the MoD (Ministry of Defence) in the UK have all been subject to so called, 'threat actors'.

The causes of cybersecurity incidents are many and varied, leaving organisations constantly on the 'back foot' to defend their systems and data. But, for the finance function cybersecurity is more of an Achilles Heel, because of the profound lack of knowledge and technical expertise.

Only forty-two percent of finance functions fully understand the issues surrounding cybersecurity in their organisations and are regularly involved in cybersecurity related discussions. This leaves fifty-eight percent of finance functions struggling to master the ever-changing threat landscape.

How well do you understand the cybersecurity risks your organisation faces?



Forty-seven percent of finance functions do not take the risks of cybersecurity seriously. Ignorance and lethargy are the biggest barriers.

Finance functions are already time-poor, having to cope with the relentless pressure of the regular financial reporting cycles. So, the growing threat of data breaches and cybersecurity adds an unwelcome burden to a business function already pressed for time.

Perhaps more worryingly, almost half of finance functions believe their active role in cybersecurity is impeded by organisations failing to take the risk seriously enough and sixty-two percent struggle to understand the business risks they face as a result of data breaches.

Everything points to the pressing need to professionalise the management of cybersecurity in the finance function to provide the knowledge and expertise to enable and maintain adequate security.

Failure to do so has unwelcome consequences. Apart from the direct cost of, say, a data breach, businesses that ignore the perils of cybersecurity face hefty fines from regulatory authorities and the indeterminate cost of reputational damage

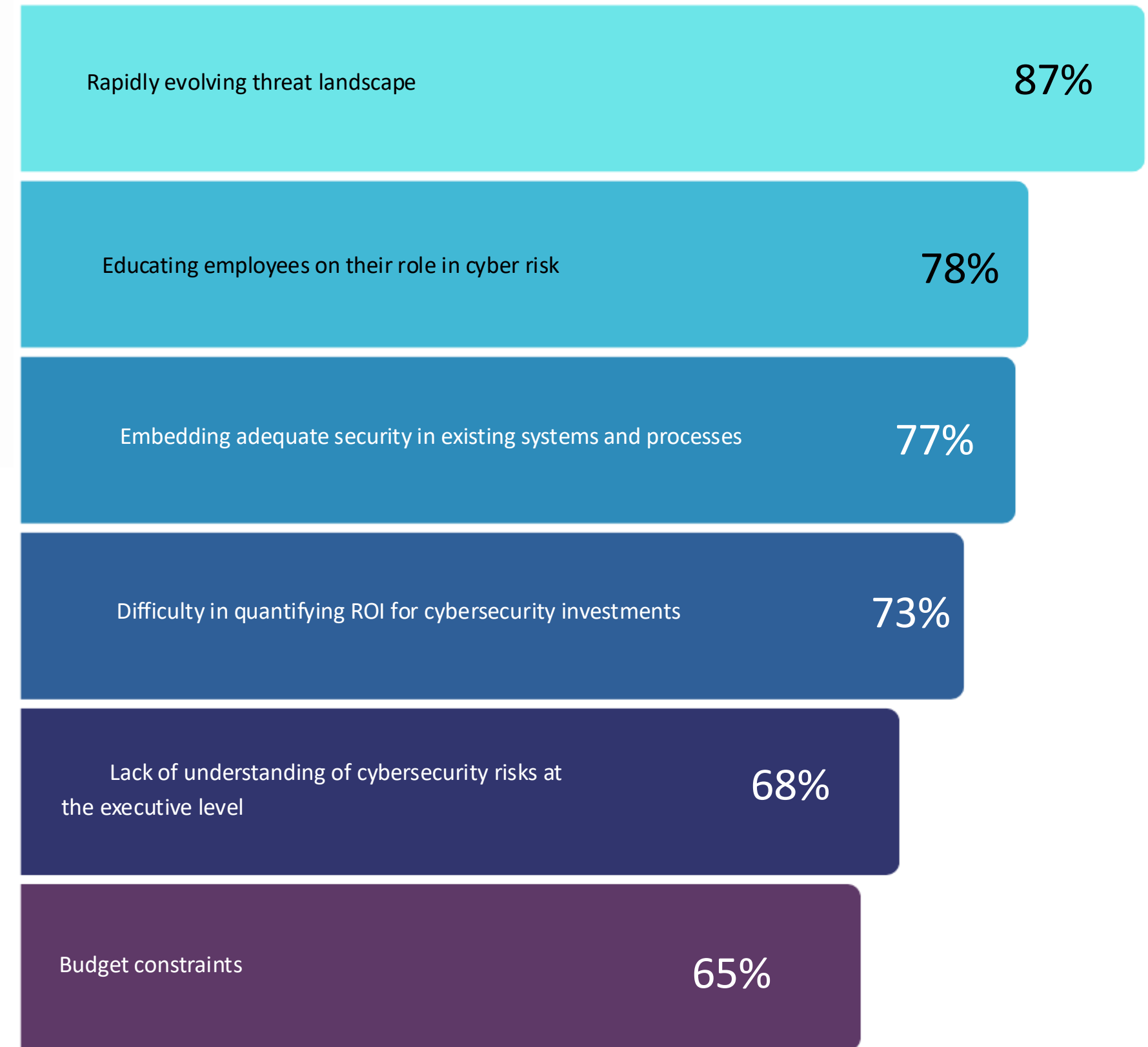




Seventy-three percent of organisations find **it difficult to calculate an ROI** on security investments. The **rapidly evolving threat landscape** leaves **eighty-seven percent of organisations constantly on the back foot, always trying to catch up.**

The threat landscape is evolving at an unprecedented rate, and although technologies such as AI have the potential to shore up cybersecurity defenses, finance functions say it is difficult to quantify an ROI. Budget constraints experienced by sixty-five percent of organisations and lack of awareness of the business risks in rest of the C-suite conspire to make it even more difficult to make a compelling business case for investment in preventative measures.

What are the barriers to implementing cybersecurity initiatives?



Larger organisations take cybersecurity more seriously but are no quicker at recovery.

The largest organisations, those with more than 10,000 employees, are more likely to rate their cybersecurity as excellent, (sixty percent versus twenty-five percent for smaller organisations). Larger organisations, are also much less inclined to outsource all or part of their cybersecurity. But this confidence may be misplaced.

In broad terms they are presumed to have 'deeper pockets' and have more complex business operations, making them more attractive to cyber criminals and more vulnerable to ransomware attacks. Larger enterprises also face greater challenges with respect to insider threats.

Despite the better cybersecurity rating, the gap between the ability of large and small organisations to recover quickly from a cybersecurity attack is slender. Sixty-six percent of organisations with more than 10,000 employees say they can recover quickly from a cyberattack versus the rest, fifty-nine percent. It seems that whether an organisation is large or small, the time taken to evaluate the damage, consider if threat actors are still active, close any vulnerabilities and restore systems and data is similarly time consuming.



Eighty-nine percent of organisations are **not confident in their organisation’s ability to recover quickly from a cyberattack.**

Data breaches are considered the most likely form of attack (eighty-one percent) closely followed by ransomware and phishing attacks. These attacks frequently have a long tail and can render systems inoperable for months. The survey also finds a surprising level of vulnerability to the less publicised risk of ‘insider’ attack, whether accidental or intentional. To help overcome this, cybersecurity should be made a concern well beyond the IT department. Staff with access to the network at all levels – from administrative to managerial – should be properly educated and trained in their responsibility for keeping it secure from cyberattacks. The required behaviours to prevent attacks and what is expected in the event of an incident, should be built into employees’ contracts of employment.



89%

Eighty-nine percent of organisations are not fully confident in their organisation’s ability to quickly recover from a cyber attack.


81%

Data breaches



71%

Ransomware



73%


Phishing attacks



37%

Insider threats





LACK OF CYBER-KNOWLEDGE WITHIN THE FINANCE FUNCTION IS LEAVING ORGANISATIONS VULNERABLE TO UNACCEPTABLE BREACHES IN THE INTERNAL CONTROL ENVIRONMENT.

“

The modern finance function is facing a credibility gap. On the one hand eighty-one percent see themselves as being responsible for managing the risks of cybersecurity and on the other hand more than half do not have a sufficient grasp of the complexity of cybersecurity issues to safeguard the integrity of the internal control environment.

Gary Simon

CEO FSN & Leader of the Modern Finance Forum

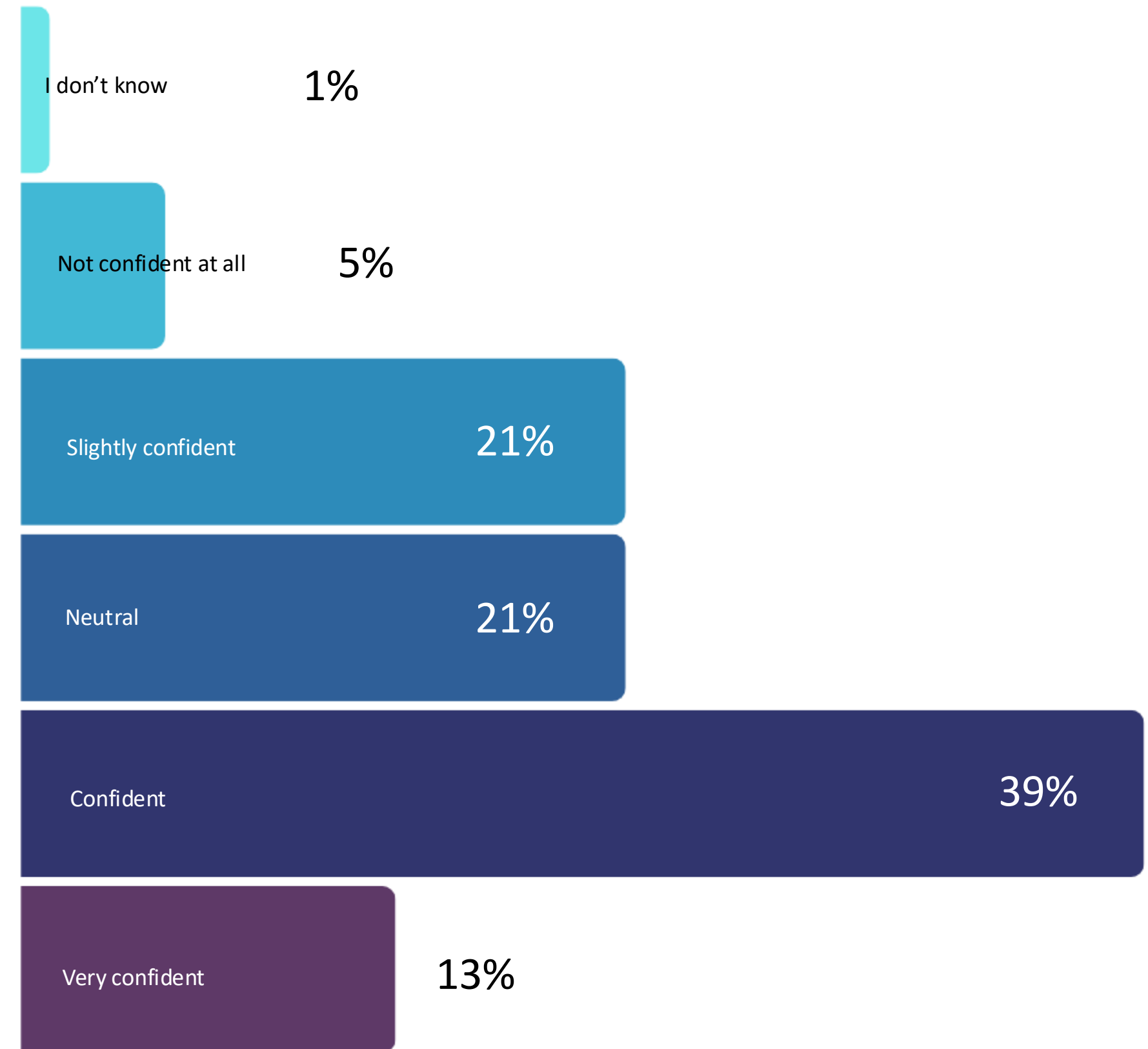


Just fifty-two percent of organisations are **confident** or **very confident** in their company's ability to secure, sensitive regulated data.

Despite the increasing prevalence and sophistication of cyber threats, only half of finance professionals express confidence in their organisation's ability to safeguard sensitive data, such as personal identifiable information (PII) and financial records, during a breach.

Only financial services and government organisations show a higher level (seventy-three percent) of confidence, with a similar percentage saying that they can recover quickly from a cyber attack, compared to just sixty percent across other industries.

How confident are you in your company's security measures for protecting your regulated, sensitive data in the event of a breach?





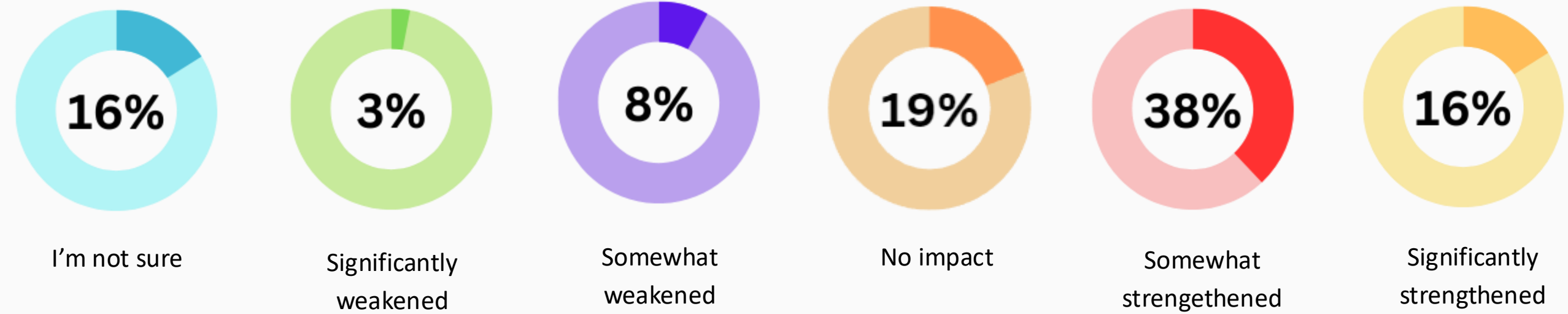
Fifty-four percent say moving applications to the cloud bolsters cybersecurity


Fifty-four percent of organisations consider that moving applications to the cloud has strengthened their cybersecurity. Just eleven percent consider that cloud deployment has weakened their cybersecurity.

In essence it is widely considered that cloud vendors make a better job of cybersecurity than organisations can on their own. This makes cloud very attractive, especially when the threat landscape is constantly evolving as well plugging the gap in the finance functions knowledge on cybersecurity.

However, sixteen percent are unclear on whether cloud hosting makes any difference to vulnerabilities and risks and 20% say it has had no impact at all.

How has your organisation's use of cloud solutions impacted your overall cybersecurity strategy?





Cyber resilience means being ready for anything. When the worst should happen, can you keep your business running?

“

“The world is on track to spend over \$200 billion on cybersecurity this year, almost entirely focused on stopping attacks. Yet almost daily we hear news of successful cyberattacks. Prevention alone is not enough. Attackers are still getting through. When a successful attack risks halting business operations, cyber resilience becomes the responsibility of CFOs and the entire executive team, not just CISOs and CIOs”

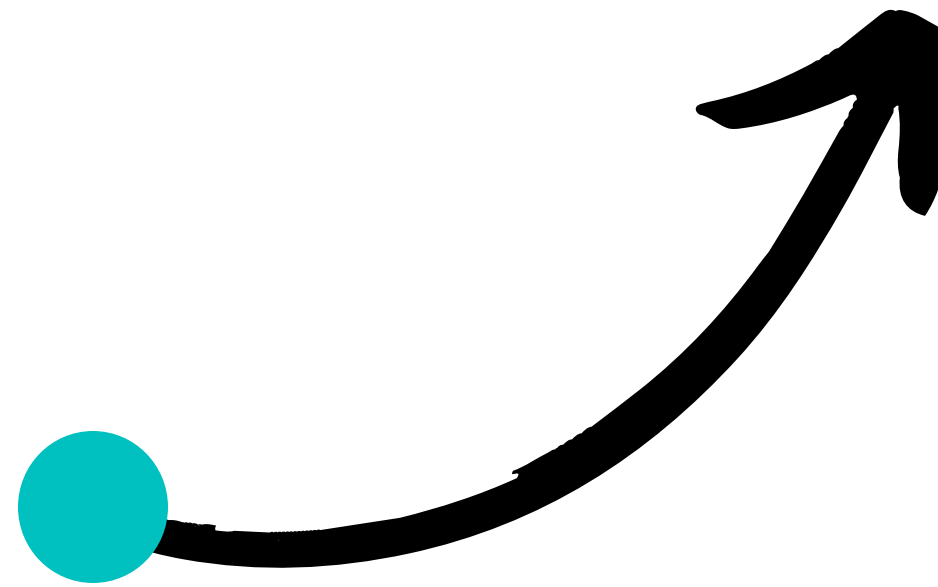
Zach Deming

Vice President of Product Marketing

Rubrik



Resilience means being ready for anything. Make your business unstoppable.



From datacentres to the cloud, keep your business running with cyber resilience before, during, and after a breach.

Rubrik's platform is built to give companies complete cyber resilience. By uniquely combining cyber recovery with cybersecurity capabilities, customers are equipped to uncover and minimise sensitive data risks before a cyberattack, find and quarantine malware during an attack, and determine a clean point of recovery after an attack. When a cyberattack happens, Rubrik customers can recover quickly and get their operations up and running.

Cyber resilience means being ready for anything. Become unstoppable against cyberattacks and operational failures with a platform that combines cyber recovery and cybersecurity.”

CONTACT US

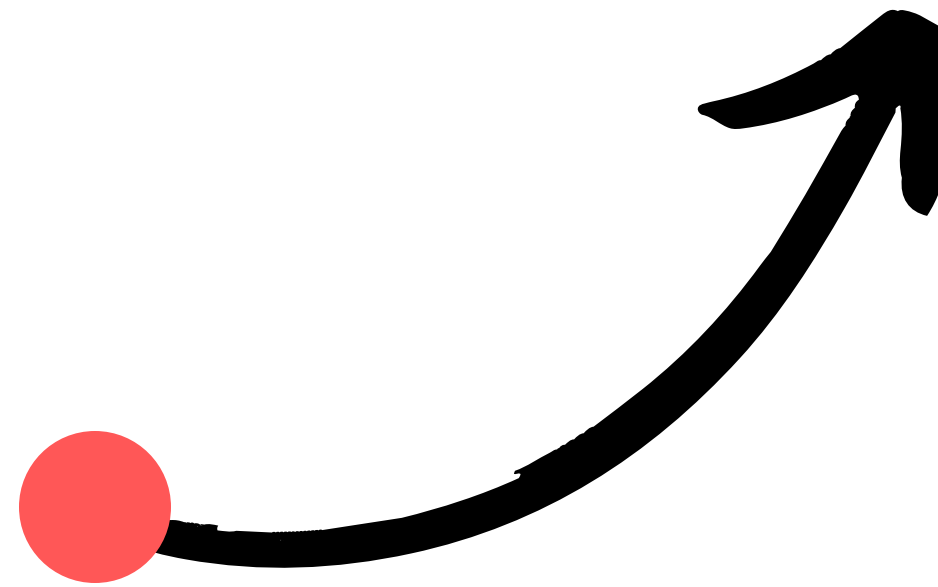
Learn more at www.rubrik.com

Follow Rubrik on [LinkedIn](#)



Looking to recruit high calibre finance professionals? Or are you a finance professional looking for a new role?

FSNTALENT can help



We offer unparalleled access to an extensive talent pool of more than 58,000 senior finance professionals across Europe, the USA, and Asia-PAC.

We believe that success lies in building strong relationships with clients and candidates. This is why we advocate a finance-led approach, which prioritises a common finance language, shared experiences, empathy, and professional knowledge.

Our deep knowledge of finance in industry, commerce, public practice, and management consultancy allows us to quickly understand every client's unique business needs and efficiently evaluate the potential of top candidates.

CONTACT US

For hirers please contact Gary Simon

gary.simon@fsntalent.com

+44 7770 310891

For candidates please contact Michelle Fabian

michelle.fabian@fsntalent.com

+447801815120

