CROSSWORD CYBERSECURITY

STRATEGY AND COLLABORATION: A BETTER WAY FORWARD FOR EFFECTIVE CYBERSECURITY

1.

INTRODUCTION

BY STUART JUBB, GROUP MANAGING DIRECTOR

There's a perfect storm facing the world of cybersecurity: escalating cyber attacks and rapid technological innovation leave companies stretched thin, trying to defend themselves against threats using existing technology, while simultaneously having to understand and secure new tools and services. Even with enhanced cybersecurity tools at their disposal, organisations are more exposed than ever.

Threat actors are organised and determined, so cybersecurity teams must match them to mount a defence. Hackers collaborate, so organisations must too. Yet, as our research makes clear, at present this is happening only to a limited extent. This is particularly true in terms of collaboration, which happens only informally, according to chief information security officers (CISOs) who we spoke to for this report. Increased and better collaboration is vital to a more cybersecure future.

Cybersecurity is a systemic issue that demands a strategic response. But too many organisations are still struggling to get the basics right and are too overwhelmed by day-to-day challenges to plan effectively for the future. That's the key finding from our survey of more than 200 senior cybersecurity professionals, backed up by in-depth interviews with academics and cybersecurity experts, as well as CISOs themselves.

Stuck in firefighting mode, CISOs are constantly chasing the next technology solution, which is never enough. New tools can help, but they need to be deployed as part of a robust strategy and reinforced with considered and deeply embedded processes and policies if they are to have a notable effect. Instead, cybersecurity teams find themselves stuck solving the same problems again and again. A new and more strategic approach that focuses on forward planning is required to tackle these real and concerning problems head-on. After all, a strategy that only lasts a matter of months really isn't a strategy at all.

This report explores what key issues look like to those who deal with them on a daily basis. It concludes with our considered recommendations on how they can best be tackled. As Group Managing Director of Crossword, I hope you find it valuable.

> "Threat actors are organised, determined and willing to collaborate.


"
CISOs are constantly chasing the next technology solution, which is never enough.

2.

THE SURVEY: A STRUGGLE TO DELIVER ON STRATEGY

Our research suggests CISOs are struggling with the range and sophistication of cybersecurity threats and the accelerating pace of technological change. The problem is global, systemic and must be addressed strategically. However, CISOs are stuck putting out daily fires. Almost half of respondents (44 per cent) say their organisation has only enough capacity to focus on immediate and medium-term threats and technology trends. There is no time for strategic planning.

Three-fifths (61 per cent) of those we interviewed described themselves as only "fairly confident" in their ability to manage their current exposure to cybersecurity threats. Furthermore, two-fifths (40 per cent) believe that their existing cyber strategy will be obsolete within two years and a further 37 per cent expect it to be irrelevant within three.

"We're facing repeat crises. They aren't always cybersec, but there's always a cybersec angle. Even Covid had a cybersecurity angle because we had to make sure remote working could happen safely."

While it is true that the speed of change in cybersecurity can sometimes require a change of approach, that is more of a tactical consideration. A strategy that won't last longer than two years is not really a strategy at all. Organisations should be looking five years ahead and strategies should be flexible enough to accommodate a degree of uncertainty.

The brittle nature of the strategies that our survey respondents are employing suggests a more fundamental problem.

"Understand your role. The CISO should be communicating outwards and upwards, and directing effort, not firefighting."

40%

believe their existing cyber strategy will be outdated in two years, and a further 37 per cent within three

The short-term threats that hog attention

Many short-term issues and challenges are overwhelming cybersecurity teams, with a high majority of respondents finding all areas of cybersecurity either a little, somewhat or very challenging.

Almost all (85 per cent) of respondents said they struggle to some extent with detecting or identifying the occurrence of a cybersecurity event or threat and the same proportion (85 per cent) struggle with third parties failing to disclose breaches in good time.

"People think cybersecurity is about buying technology, but there's still a massive problem with technical debt. We have machines that are too old for antivirus to be installed."

Third parties themselves are an issue. More than four-fifths of the executives we talked to (83 per cent) say they struggle to ensure their supply chain has a watertight ability to defend against threat actors and recover from

ADVICE

FOR INCOMING CISOS

The big concern for CISOs today is the lack of budget coming into 2022. It's difficult to say how much money is enough because CISOs told us they don't always have complete visibility of the risk, but every CISO is constantly arguing for more. There are signs of that improving because new risks – and ongoing global instability such as the war in Ukraine – have pushed cybersecurity higher up the agenda.

Governance remains an issue, however. In some places the CISO still reports to the CIO, which hinders communication with the board. And within the organisation there can be a perception that cybersecurity slows down innovation, so support from the board is vital.

CISOs have endured repeat crises over the past few years, such as the Colonial Pipeline attack, the JBS attack, SolarWinds and more. Even when it isn't a cybersecurity incident, there is often a cybersecurity angle. The rapid shift to remote working during the Covid-19 pandemic was a huge cybersecurity challenge and the war in Ukraine has put lots of organisations on cyber-attack alert. Current threats are so numerous and so fast-moving that executives just don't have time to plan. Add to that the rate of business change and the pace of new technology adoption and it's no surprise that they're constantly in reactive mode.

The risk of being collateral damage from attacks on others is something that a lot of organisations overlooked in the past, but supply-chain and third-party threats are on the agenda now. If the supplier of one tiny ingredient for the company's products gets attacked, then the product can't ship until the organisation knows everything is safe. The costs of something relatively small can be enormous.

Being a CISO can be rewarding. There's lots of visibility with senior leadership and balancing the roles of technology leader and business communicator is an engaging opportunity. But it's demanding, too. Many things may be in a mess when a new CISO arrives in post, so they must quickly identify what needs to improve and be able to communicate that to the business.

A major challenge is learning to take holidays and shut down for a while. Many CISOs burn out after a few years. A new CISO must build resilience into their team so it can function without them, and they must learn to delegate. They should focus on what they're good at and delegate what they aren't. Prioritise the leadership role and delegate the day-to-day. However, that is complicated by the fact that talent is so hard to find. Diversity and inclusion are a particular struggle because there just aren't enough good people out there.

There's camaraderie among CISOs. It's important to build a network, because a lot of information comes through informal channels, but it's also useful to have people to talk to who have dealt with the same issues and can share tips for dealing with them. Sometimes it simply helps to vent!

attacks. The scale of these struggles suggests that the current approach to cybersecurity needs a rethink.

Tasks that are considered "basic", such as patching, can also be harder than they appear. Organisations with significant legacy systems might find that patching takes a month or two. Meanwhile, our interviewees told us, putting in place a long-term cyber strategy takes two or three years, all while managing the day-to-day. It seems that the resources to make that happen are not available.

"The CISO needs to understand threats, risk, likelihood and assess improvements that could be made. Can you make a case for the costs?"

Chasing tomorrow's strategy while struggling to deliver on that of today

With so many short-term problems, it's no surprise that respondents say they can't focus on strategy. Delivering on the current strategy is difficult and planning the next is virtually impossible. A good strategy should be forward-looking, well-resourced and capable of withstanding changing circumstances. To deliver that, organisations must start thinking about the structure of their teams and the talent pool available to them. This is discussed in detail later.

What is holding them back, according to 31 per cent of respondents, is the skills gap – because without enough people with the right expertise to manage the load, security teams are overwhelmed, struggle to process alerts and sometimes miss crucial ones. Meanwhile, 28 per cent point to a lack of good threat intelligence and 27 per cent identified difficulties with securing digital identity as a key challenge, which makes it easier for hackers to gain access to data and systems by pretending to be someone else.

These are not challenges that will be fixed soon. The skills gap could be partially addressed by organisations putting more resources into training and upskilling their people. However, this is hard to do when the cybersecurity team has no spare capacity.

"We need to lower the barriers to entry and make it possible to get vocational training in cybersecurity and not just rely on university courses."

Threat intelligence is also a tough problem to solve. Law enforcement doesn't always share everything it knows, for operational reasons, and other organisations often keep threats confidential. Many CISOs find themselves relying on an informal information-sharing network.

Assessing strategic priorities

Asked which components of their cybersecurity strategy dominate now or will do so over the next 12 months, three-quarters (75 per cent) said software verification, which helps to ensure that the program is secure, while 69 per cent cited transition to the cloud. A similar number (67 per cent) said dealing with escalating ransomware attacks would be their focus.

"The best you can do is gain consensus in the organisation. Run lots of workshops to test threats, brainstorm the risks and potential outcomes."

Those short-term priorities were followed by cybersecurity mesh architecture (CSMA), which is a method for making cybersecurity products interoperable (65 per cent), and zero-trust and identity security

85%

of respondents said they struggle to some extent with detecting or identifying the occurrence of a cybersecurity event or threat

(62 per cent), which seek to deal with attackers posing as legitimate users by treating every action on the network as untrustworthy and investigating all. New technology tools mean that this can be done quickly, without inconveniencing legitimate users.

All of these technologies have a significant role to play in securing organisations for the future. However, as has been noted above, it would be a mistake to think that any or all of them could replace a robust cybersecurity strategy. These tools should form part of a well-constructed programme.

83%

say they struggle to ensure their supply chain has a watertight ability to defend against threat actors and recover from attacks

Key technology trends

When it comes to technology trends that our respondents expect to become a priority in the next 12 months, the most cited was the transition to the cloud and cloud cybersecurity (41 per cent), followed by CSMA (35 per cent) and growth in artificial intelligence and machine learning (31 per cent).

"In some regulated sectors, we have to keep at least a portion of our data on-premises. The regulators are catching up and realising that cloud services can sometimes be more secure."

Moving to the cloud undoubtedly brings new risks, not least of which is the growth of shadow IT. CISOs we interviewed said that employees are often tempted to download a cloud app on a personal device so they can access their work data, not realising that this increases risk for the whole organisation. When many employees are tempted to do this, the risk can be significant. Another cloud issue highlighted was the fact that it can be difficult to know precisely where your business-critical data is once you move to the cloud.

> "The best you can do is gain consensus in the organisation. Run lots of workshops to test threats, brainstorm the risks and potential outcomes.

"The challenge with critical national infrastructure is that nations are reliant on a constellation of technology they fundamentally can't protect from hostile state actors.

EXPLORING

THE BIGGER PICTURE

Academia has a significant role to play in the pipeline of innovation and science in cybersecurity. Academics can look at the bigger picture and put research effort into solutions to major problems, such as the explosion of data from the Internet of Things or how to secure critical national infrastructure.

Companies and governments are often too busy dealing with day-to-day issues to spend significant time on the big picture. On the other hand, academics must guard against naivety; from a distance it may be easy to think they have solutions to problems, but people who work at the cutting edge can often see issues with suggested approaches that those not in the direct line of fire would miss. That's why partnerships are so important.

Though academics do work with companies and governments, 90 per cent of research is initiated by them and sold on. A lot of work is focused on areas of commercial challenge, such as identity management and threat visualisation. Ransomware remains the biggest issue and often SMEs still aren't spending enough to defend against such attacks. It's important to teach CIOs and CTOs about the risks and how they can mitigate them.

The challenge with critical national infrastructure is that nations are reliant on a constellation of technology they fundamentally can't protect from hostile state actors. That doesn't mean they are doing badly, simply that the situation favours the attacker. Governments have a huge waterfront to protect from a highly motivated adversary. Researching vulnerabilities means that academics can help keep systems as secure as possible against malicious actors. However, much critical national infrastructure is run by private companies that answer to their shareholders. They aren't incentivised to tackle vulnerabilities that might affect others more – and that is a problem academia can't solve.

Academics are also very aware of their role in tackling the skills shortage. Universities can and are setting up courses. PhD candidates are working in industry on cutting-edge projects that will yield new research and often generate new intellectual property. Some PhD candidates are working on projects so secret that they can't even tell their supervisors what they are doing. However, one problem that academia has is that it can't offer salaries that experts in cybersecurity, artificial intelligence and data science can earn in industry, especially with big tech firms. That makes it difficult to attract people with more than theoretical experience of these threats. Academia must find ways to get expert practitioners involved.

The cybersecurity sector must attract a more diverse range of people, too. Companies need to lower the bar of entry so university courses aren't the only way in. But they might also look beyond technical people; cybersecurity needs cognitive psychologists, change managers, business experts and more. Cybersecurity touches every part of the public and private sector, so greater attention must be focused on it.

3.

CONCLUSION: BUILDING A STRATEGIC RESPONSE TO CYBERSECURITY PROBLEMS

The picture painted by our research shows CISOs are in urgent need of a strategic rethink that will allow them to recalibrate the daily firefighting attendant on a cybersecurity operation with managing the organisation's long-term requirements.

A good strategy starts with getting the basics right. If basic security tasks, such as patching, aren't being handled then everything else is pointless. A solid foundation is necessary on which everything else can be built. But that alone won't be enough because new fires will keep breaking out, so developing a robust long-term strategy that incorporates full supply-chain cybersecurity is crucial to creating a more secure future.

Focusing on information-sharing and collaboration

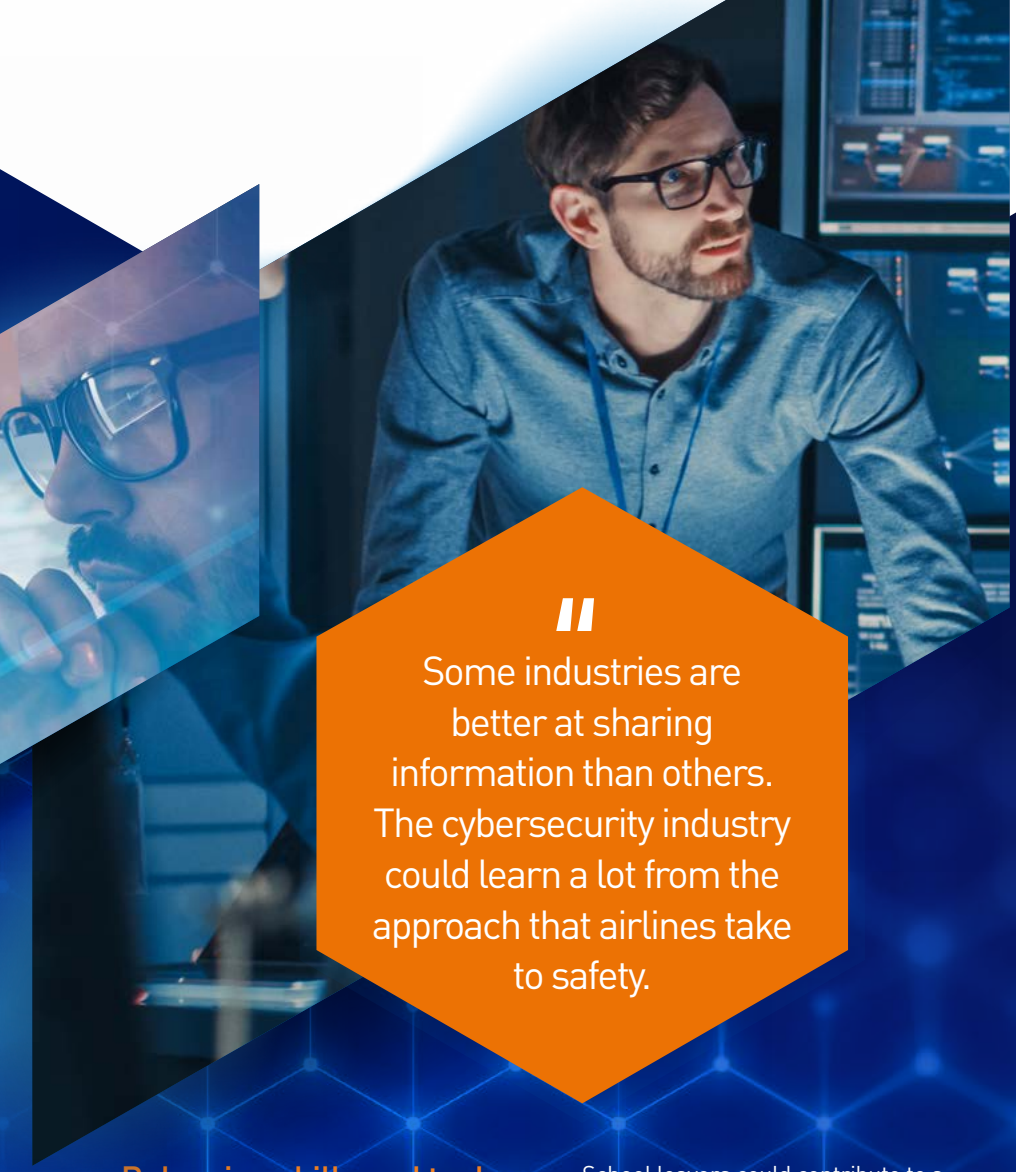
Laying the foundations for such a strategy begins with collaboration, including sharing sensitive information with peers and building a consensus on best practice.

If cybersecurity is an arms race, then CISOs must think like their adversaries. Threat actors are well organised and work together to accomplish their goals. To defend against them, cybersecurity experts must close ranks. They must be ready to work with peers, with other sectors and with academia and government. Companies should appoint a head of cyber collaboration to coordinate outreach.

Some industries are better at sharing information than others. The cybersecurity industry could learn a lot from the approach that airlines take to safety, for example. Information is shared in blame-free, anonymised incident reports. The stakes are arguably higher in aviation, but other industries are not far behind. As the Internet of Things embeds itself into everyday life, it becomes more likely that cybersecurity issues will also be public safety and trust issues.

Some CISOs see their jobs as making their organisation more secure than the next one. This is a short-sighted approach. Enhancing everyone's security makes life harder for threat actors everywhere. The head of cyber collaboration could gather information on incidents from partners and suppliers, while facilitating greater co-operation with their industry peers. The emerging trend for CSMA solutions, highlighted as a major one in our survey, is particularly relevant here because it is designed to reduce interoperability gaps between different security solutions and enable them to work better collectively.

Another area where the cybersecurity team might benefit from reorganisation is by appointing a strategy manager. The CISO is, of course, responsible for setting the strategy, but they will always be torn between firefighting and developing the longer-term response, between leading the cybersecurity team and communicating with the board and the business as a whole. It can be an overwhelming task, so a cybersecurity strategy manager could take the lead in ensuring that long-term plans are still being developed and carried out.



> Some industries are better at sharing information than others. The cybersecurity industry could learn a lot from the approach that airlines take to safety.

Balancing skills and tools

But who is going to make all of this happen? And how? The skills gap is real, but it is important to understand that skills shortages can be addressed by new approaches. Having the internal understanding and skillsets to manage cybersecurity risk to systems, assets, data and capabilities were highlighted as a significant problem by our respondents.

Organisations must take responsibility for upskilling their staff. Even so, it is not an issue that will be solved overnight, so CISOs must factor this skills shortage into their cybersecurity strategy and consider how they can make use of new approaches, such as automation and CSMA, to help tackle it while addressing the availability of new talent.

Budget needs to be put into training to help raise cyber skills levels across the board and the industry must find ways to lower barriers to entry. Certain gaps can be addressed with internal training or hiring people with specific skills.

School leavers could contribute to a cybersecurity team while spending the early years of their career being trained to a comparable level to degree-level candidates, for example. Furthermore, some skills – such as cybersecurity audit skills or penetration testing – are niche enough that many organisations will not require people on staff to fulfil those roles; that's where external consultants and third-party support can frequently help.

Hackers are often driven by curiosity, rather than malice, so the industry should look at ways to encourage more of them to "go straight" and work on cybersecurity. Similarly, cybersecurity experts could make greater use of "bug bounties" – paying hackers to report security weaknesses rather than selling them to criminals. These are long-term approaches, so in the medium term CISOs should factor in the skills they need today when building their cybersecurity strategy – and not be afraid of outsourcing when necessary.

Wider cybersecurity awareness is essential too and the industry should consider including cybersecurity training in executive courses, such as MBAs. Meanwhile, organisations should ensure that cybersecurity training is mandatory for all staff and put in place robust internal policies, such as regular drills.

Organisations must also have a proper discussion of risk at board level. Our interviewees told us that the board is often reluctant to tolerate any level of risk, but equally reluctant to spend what it takes to manage it. Perhaps the rising cost of cybersecurity insurance will push them to act, but cybersecurity teams are overstretched.

CISOs need support in the form of budget for technology solutions that will help reduce the load, such as artificial intelligence and machine learning. Many cybersecurity tools now employ automation to reduce the burden on cybersecurity teams by detecting and acting on security alerts without any human intervention. This means analysts don't need to deal with false positives, but it also means legitimate threats will be dealt with more quickly. Overall, CISOs need the funds and support to build a cross-business cybersecurity standard operating model covering their organisation and its supply chain that incorporates training, processes, policies, tools and frameworks.

Cybersecurity measures are not simply a business cost – they often provide excellent return on investment. Extending the use of CSMA solutions, for example, will create an integrated system that will even work between companies so that, according to Gartner, the financial impact of individual security incidents will be reduced by 90 per cent by 2024[1].

The way forward is clear and the time to act to get short-term issues under control and then begin planning long-term strategy is now. Every month of delay leaves businesses open to crippling cyber-attacks.

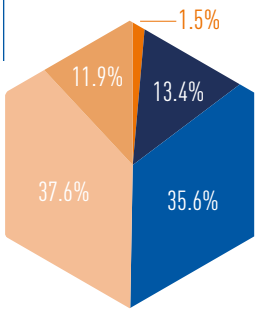
1 https://www.gartner.com/en/newsroom/press-releases/2021-10-18-gartner-identifies-the-top-strategic-technology-trends-for-2022

4.

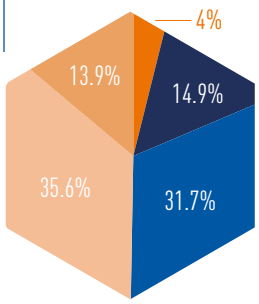
THE SURVEY:
A VIEW OF THE DATA

Q1. How challenging, if at all, are the following areas of cybersecurity risk management for your organisation?

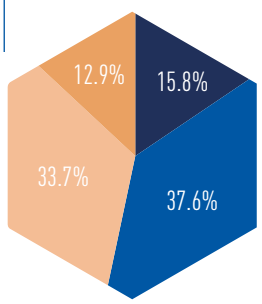
Managing vulnerabilities



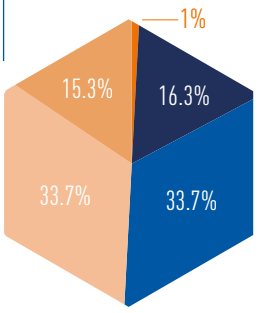
Managing regulatory and legislative compliance



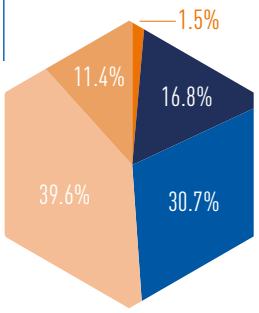
Implementing the appropriate safeguards to ensure delivery of critical infrastructure services



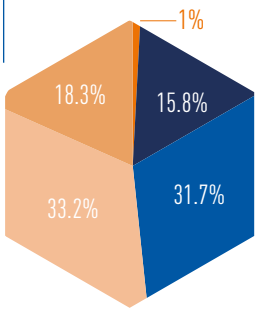
Recovering and restoring any capabilities or services that were impaired due to a cybersecurity event



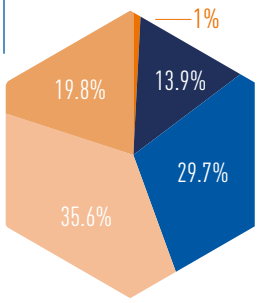
Developing internal understanding and skill sets to manage cybersecurity risk to systems, assets, data and capabilities



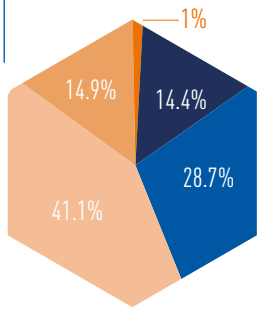
Ensuring that the entire supply chain is watertight in its ability to defend and recover against threat actors



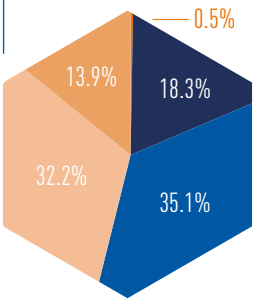
Ensuring that third parties disclose that they have suffered a breach in good time



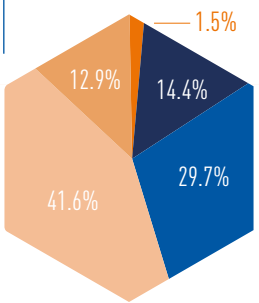
Detecting or identifying the occurrence of a cybersecurity event or threat



Responding to or taking action against a detected cybersecurity event



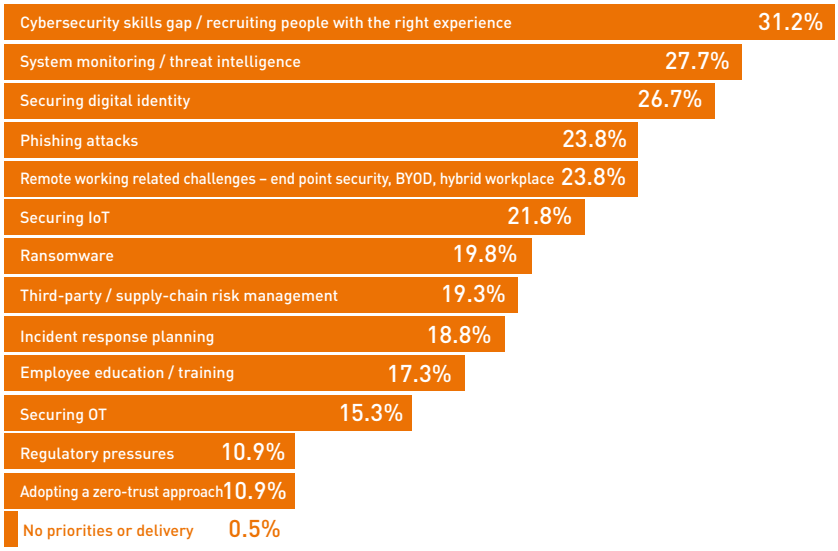
Understanding and anticipating new or potential future strategies used by threat actors



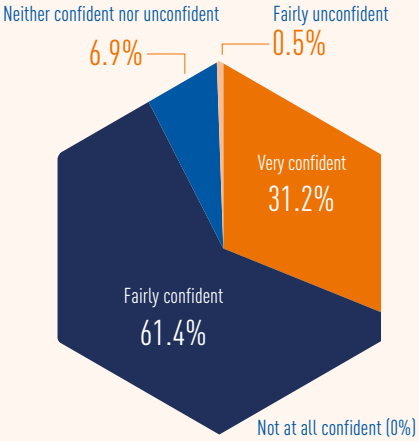
KEY

- Very challenging
- Somewhat challenging
- A little challenging
- Not at all challenging (i.e. non-existent as a challenge)
- Not applicable to my organisation

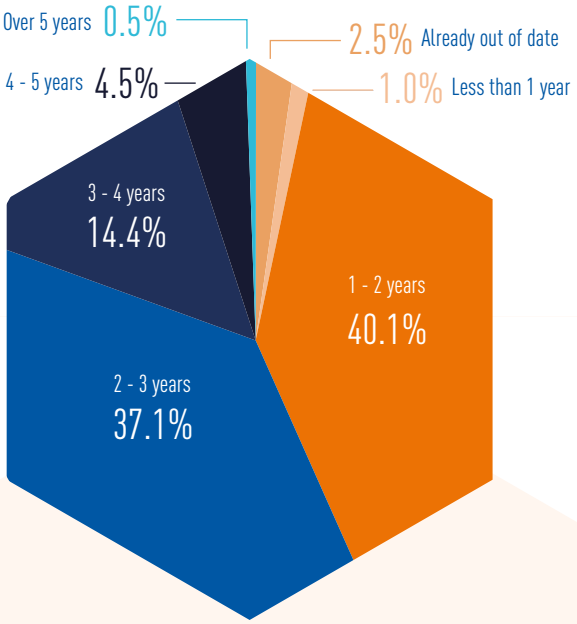
Q2. What would you consider as your role's top strategic priorities, if any, in delivering your organisation's Information Security / Cybersecurity over the next 12 months?



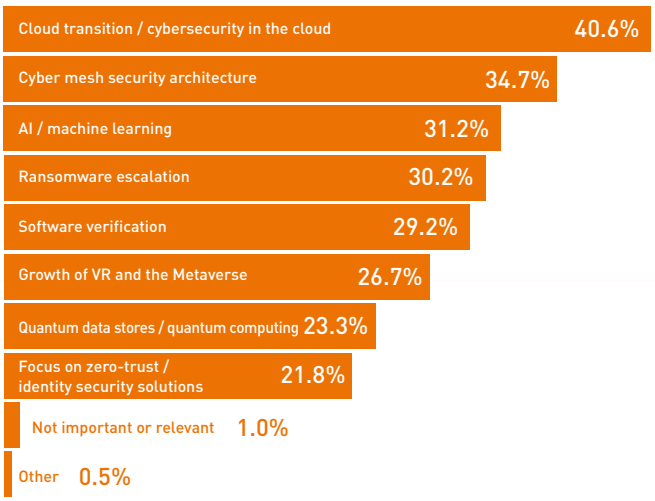
Q3. Overall, when you think about your ability to manage your organisation's current cybersecurity threat exposure, which of the following best represents your confidence level?



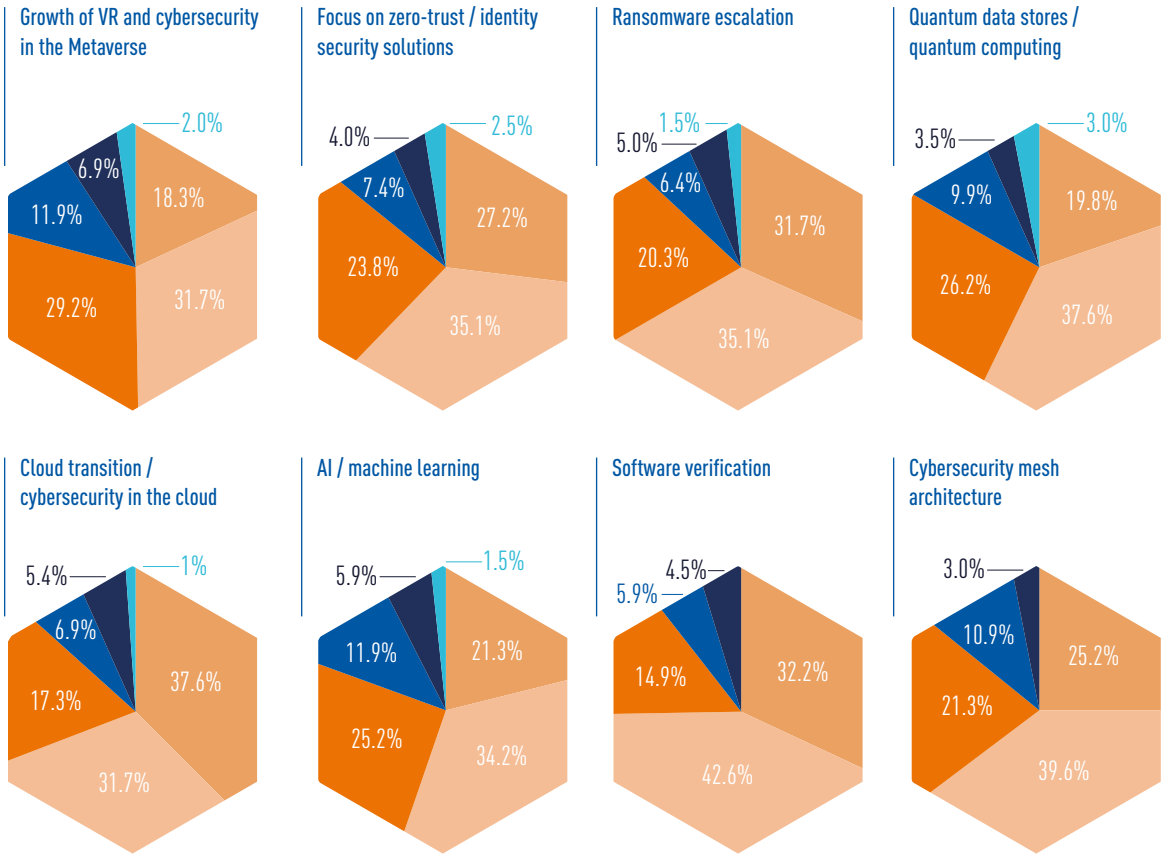
Q4. In what time period, if at all, do you believe the cybersecurity strategy that currently exists in your organisation will cease to be relevant?



Q5. Thinking about your current role in cybersecurity or IT, which cybersecurity topics or technology trends would you consider to be the most important or relevant to your role over the next 12 months?



Q6. For each topic, please indicate a timeframe for when you believe it will become a key part of your organisation's cybersecurity strategy.



KEY

- Right now, it's urgent
- In the next 12 months
- In the next 3 years
- In the next 5 years
- It's not key
- Never, it's not relevant

Q7. In your role, which of the following statements best describes your own capacity to focus on future cybersecurity threats and new technology trends within your organisation?

5.
ACKNOWLEDGEMENTS

We'd like to thank the following members of our executive team, advisory board and academic research professors for their valuable insight:

THE EXECUTIVE

TOM ILUBE CBE
CEO

STUART JUBB
GROUP MANAGING DIRECTOR

SEAN ARROWSMITH
GROUP SALES DIRECTOR

JAKE HOLLOWAY
CHIEF PRODUCT OFFICER

MARY DOWD
CHIEF FINANCIAL OFFICER

THE BOARD

ROBERT COLES
INDEPENDENT NON-EXECUTIVE DIRECTOR

THE ADVISORY BOARD

ALISON DYER
CHAIR OF THE ADVISORY BOARD

NAINA BHATTACHARYA
ADVISORY BOARD MEMBER

PROFESSORS

PROFESSOR TIM WATSON
PROGRAMME DIRECTOR, DEFENCE & SECURITY, THE ALAN TURING INSTITUTE

MUTTUKRISHNAN RAJARAJAN (RAJ)
PROFESSOR OF SECURITY ENGINEERING AT CITY, UNIVERSITY OF LONDON

About Crossword Cybersecurity plc

Crossword offers a range of cybersecurity solutions to help companies **understand and reduce cybersecurity risk**. We do this through a **combination of people and technology**, in the form of SaaS and software products, consulting and managed services. Crossword's areas of emphasis are **cybersecurity strategy and risk, supply-chain cyber, threat detection and response**, and **digital identity,** and the aim is to build up a portfolio of cybersecurity products and services with recurring revenue models in these four areas. We work closely with UK universities and our products and services are often powered by academic research-driven insights.
In the area of **cybersecurity strategy and risk** our consulting services include cyber maturity assessments, industry certifications and virtual chief information security officer (vCISO) managed services. Our end-to-end **supply-chain cyber** standard operating model (SCC SOM) is supported by our best-selling SaaS platform, Rizikon Assurance, along with cost-effective cyber audits, security testing services and complete managed services for supply-chain cyber risk management. **Threat detection and response** services include our Nightingale AI-based network monitoring, Nixer, to protect against application layer DDoS attacks, our Trillion and Arc breached credentials tracking platforms, and incident response. Our work in **digital identity** is based on the World Wide Web Consortium W3C verifiable credentials standard and our current solution, Identiproof, enables secure digital verification of individuals to prevent fraud. Crossword serves medium and large clients including FTSE and S&P listed companies in various sectors, such as defence, insurance, investment and retail banks, private equity, education, technology and manufacturing, and has offices in the UK, Poland and Oman.

CROSSWORD
CYBERSECURITY

Crossword Cybersecurity plc

60 Gracechurch Street,
London EC3V 0HR

e: info@crosswordcybersecurity.com
twitter: @crosswordcyber
t: +44 (0) 203 953 8466