Cyber Security: Community Insights 2020
Lessons and predictions for the future

December 2020

www.crimson.co.uk

CYJAX

crimson®

The Cyber Security landscape has changed: What did we learn in 2020?

In recent years IT departments have witnessed a decline in Cyber-attacks, organisations were getting to grips with threats and fighting back.

However, the mass relocation of workers quickly increased the probability of attack exponentially as IT departments battled to secure networks, equipment and more. Suddenly our defences were down, IT departments were under pressure to make quick decisions, and the world relied on our technology superheroes to 'Zoom' in and save the day.

Consequently, IT budgets are at breaking point, and the level of investment is unsustainable. However, remote working is set to continue, 43 percent of IT leaders expect more than half of their employees to work from home after the pandemic, according to the 2020 CIO Survey by Harvey Nash.

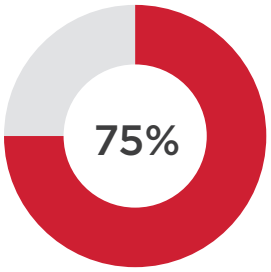
'We're in this together' has been our 2020 mantra, we have had to adapt to survive. This report presents the opinions and experiences of IT departments from across the United Kingdom to understand more about the future of Cyber Security.

Early reports suggest that around 40 percent of organisations experienced a rise in Cyber-attacks during the first peak of COVID-19 and that Cyber Security is now a top investment priority for digital leaders, we will put these initial figures to the test.

Our findings may validate your assumptions, and some of the results will almost definitely spark debate, are you equipped to tackle the latest threats?

Survey source data

This report features the results of a survey conducted by Crimson in partnership with Threat Intelligence specialists, Cyjax in October 2020, during the second wave of the Coronavirus pandemic. The IT leaders that participated in the survey work in a diverse range of sectors; **over 75 percent of respondents were from medium and enterprise-sized organisations.**



About Cyjax

Cyjax helps companies build effective threat intelligence solutions to tackle the ever-growing number of digital threats that organisations and people face today. Find out more about Cyjax at **www.cyjax.com**

About Crimson

Crimson is an IT recruitment and Microsoft IT solutions business that unites people, processes, and technology. The company is part of the £1BN global Harvey Nash Group. You can learn more about Crimson at **www.crimson.co.uk**

Contributors

Ian Thornton-Trump
Chief Information Security Officer at Cyjax Limited

Ian Thornton-Trump CD is an ITIL certified IT professional with 20 years of experience in IT security and information technology. Ian's insights have been published in various tier one publications; he is a valued contributor to the UK Cyber Defence Challenge. He also holds an executive position and lead architecture role in the Canadian Cyber Defence Challenge (Cyber Titian). In all these capacities, Ian helps mentor the next generation of Cyber Security professionals.

Andy Basham
Senior IT Recruitment Consultant at Crimson

Andy Basham is a senior IT Recruitment Consultant with strong technical knowledge gained from six years working in IT as an analyst, 1st/2nd Line Support, and Helpdesk Manager. For the last three years, Andy has hosted Architect Exchange, a networking forum for Architects. He recently commissioned a report assessing the impact of COVID-19 on UK IT departments. His impressive network and knowledge enable him to connect top IT and Cyber Security talent to organisations across the UK.

Section 1:
Accountability

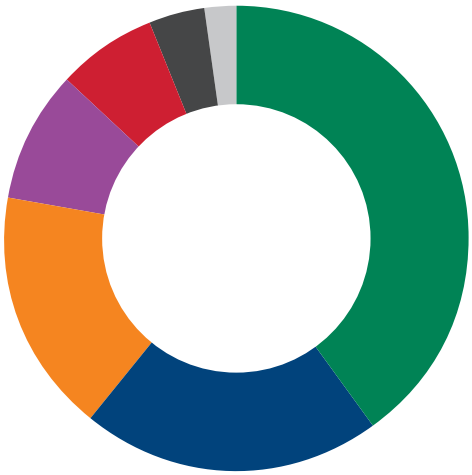
Chief Information Officers (CIOs) take ownership of Cyber Security Strategy.

C-level executives, especially CIOs, are being tasked with security responsibilities on top of other projects such as data science, data-driven operational improvements, and digital transformation.

Overall, 57 percent of survey respondents indicated that either CIOs or CISOs were responsible for delivering the Cyber Security strategy, this figure creeps up to over 70 percent for enterprise organisations.

Interestingly security responsibilities are relatively evenly distributed after C-levels among directors and managers.

Which C-level person is responsible for delivering the InfoSec/Cyber strategy in your organisation?



- 40% CIO
- 17% CISO
- 7% CTO
- 2% Not an individual person.
- 21% CEO / MD
- 9% IT Director
- 4% CFO

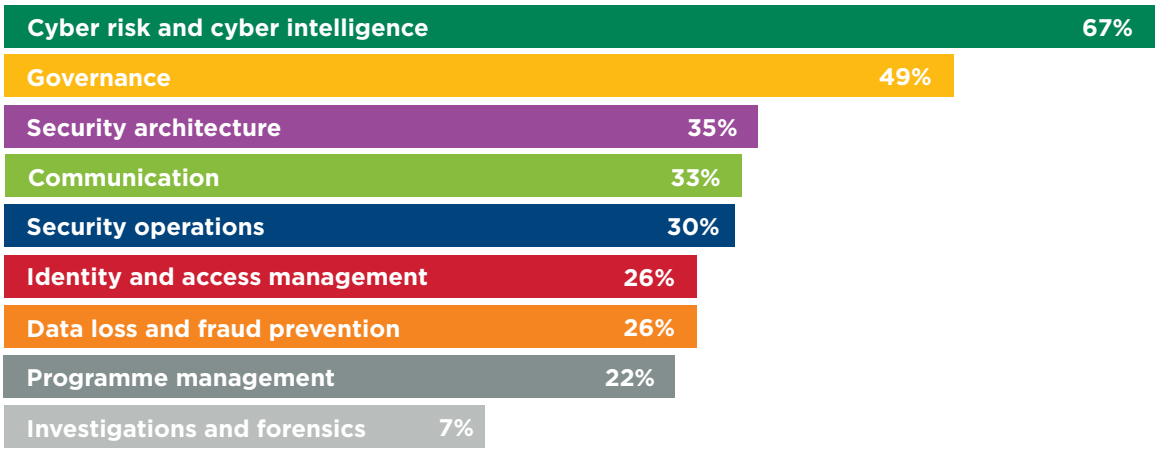
CISOs must remain current and operational at board level.

Keeping abreast of the current threats and risks (cyber risk and cyber intelligence) was identified as the most important aspect of a CISOs role. According to the CIO survey mentioned earlier, over 6 in 10 technology leaders report being more influential because of the crisis; however, globally, only around 60 percent of CIOs are board members. As security emerges as a top priority board membership may increase over the coming months.

"Activating and building security capability within the organisation is a primary function of leadership, although less than half of our respondents identified planning, buying, and rolling out new security hardware or software (security architecture). The delta between responsibility 'for' and action 'to do' has been a struggle for many organisations. When it comes to Cyber Security, authority needs to enable agility."

Ian Thornton-Trump,
CISO, Cyjax

CISOs must remain current and operational at board level.



What do you consider to be the three most important aspects of a CISO's role?

Cyber risk and cyber intelligence: Keeping abreast of developing security threats, and helping the board understand potential security problems that might arise from acquisitions or other business moves.

Governance: Making sure the right person or persons have the authority to make key decisions whilst ensuring security strategies are aligned with business objectives and consistent with regulations.

Security architecture: Planning, buying, and rolling out security hardware and software, and making sure IT and network infrastructure are designed with best-practice security measures.

Communication: Ensuring key business objectives and results are communicated effectively between the C-Suite and the security operation of the business.

Security operations: Real-time analysis of immediate threats, and triage when something goes wrong.

Identity and access management: Ensuring that only authorised people have access to restricted data and systems.

Data loss and fraud prevention: Making sure internal staff don't misuse or steal data.

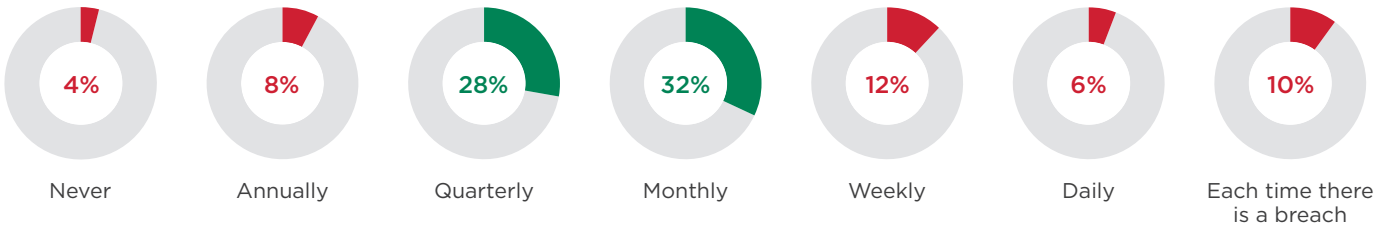
Programme management: Keeping ahead of security needs by implementing programs or projects that mitigate risks — regular system patches, for instance.

Investigations and forensics: Determining what went wrong in a breach, dealing with those responsible if they're internal, and planning to avoid repeats of the same crisis.

Cyber Security is on the board's risk register.

60 percent of respondents communicate with senior managers and board members on a monthly or quarterly basis, a step in the right direction to secure board and C-level support for security improvements.

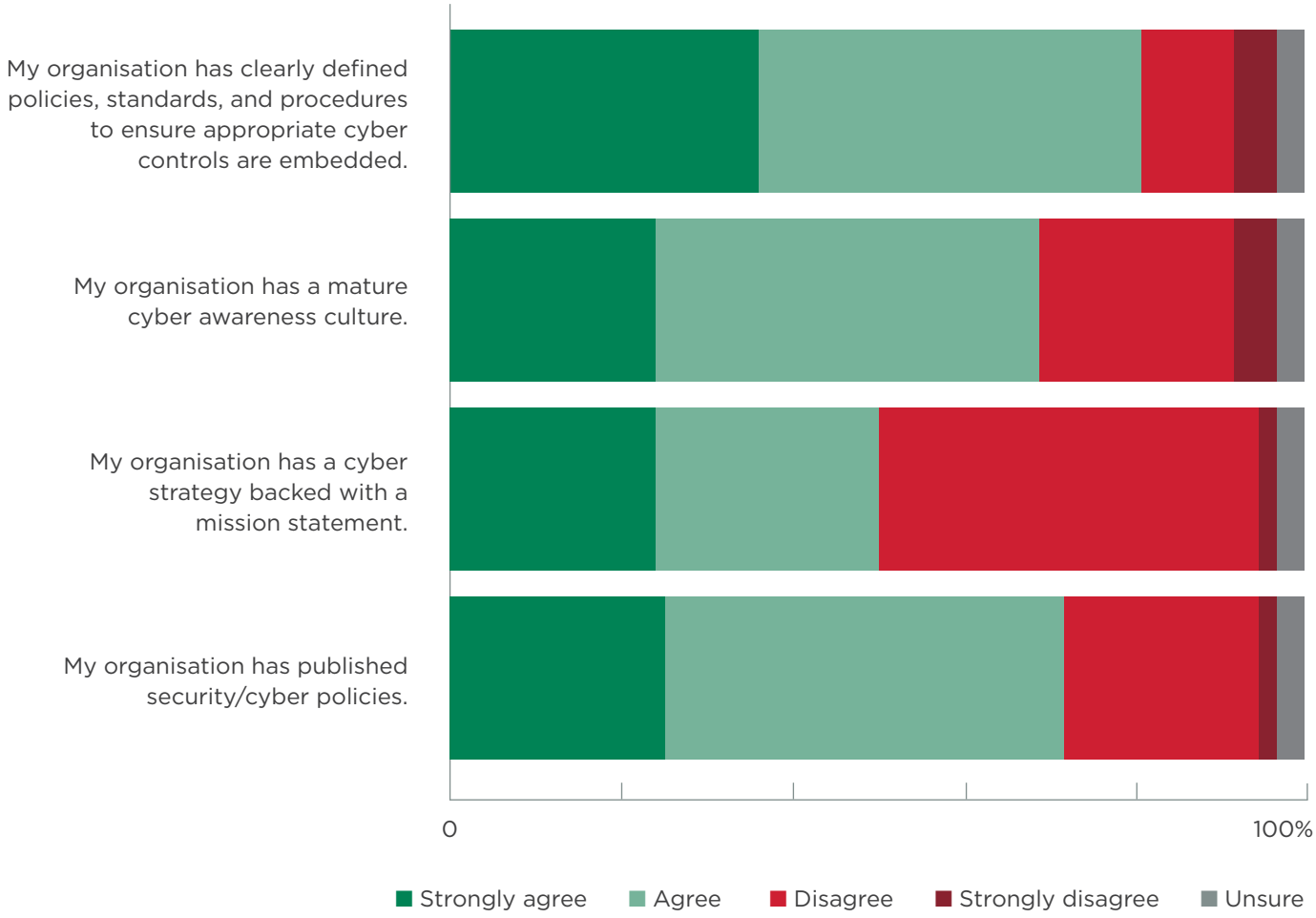
How often are senior managers/the board updated on Cyber Security in your organisation?



Section 2:
Cyber Security Culture

Almost 70 percent of tech leaders believe they have a mature cyber awareness culture.

These figures tell us that many IT leaders feel they have built solid Cyber Security foundations. Developing and sustaining a 'security culture' is no mean feat.



"The sudden increase in threats from Covid-19 related scams and the media coverage of large-scale Ransomware/Blackmail victims such as Garmin has dramatically enhanced awareness of the overall online threat. Given regulations such as the GDPR, it is concerning that over 20 percent of the organisations have not published policies relating to data and organisational security."

Ian Thornton-Trump,
CISO, Cyjax

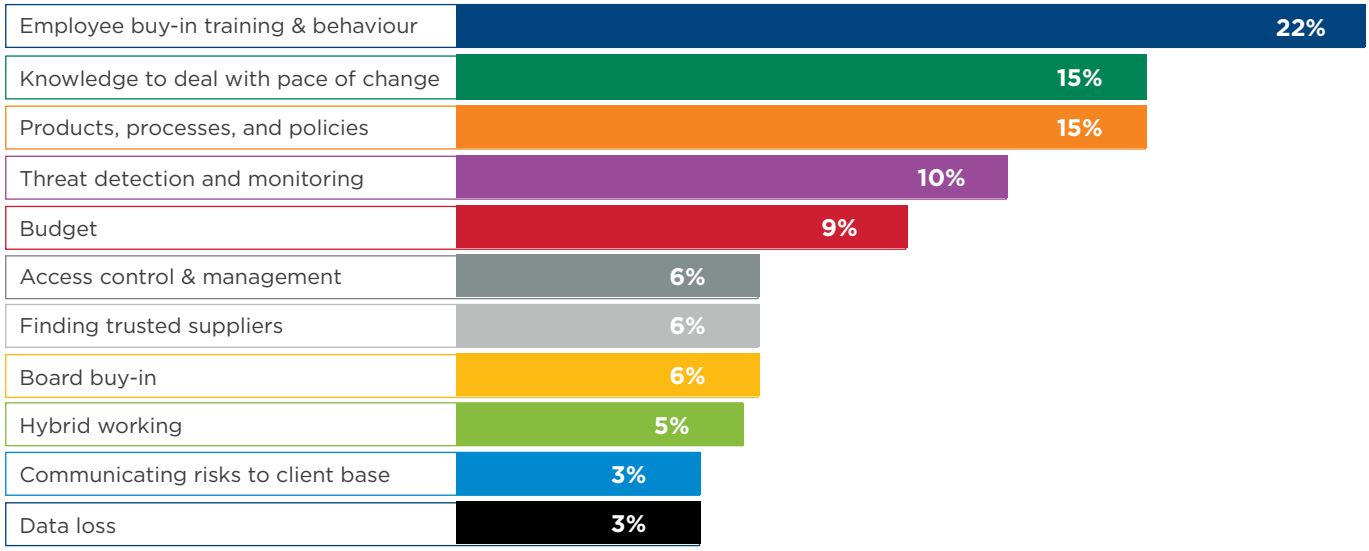
"Security awareness is one thing; security effectiveness is another. I think organisations are going to realise that they need to roll up their sleeves when it comes to tackling real-life cyber incidents as opposed to board rooms sessions."

Daniel Card,
CEO, Xservus

Employee training and behaviour is the biggest pain point for digital leaders.

Although 68 percent of the respondents believe their organisation has a mature cyber awareness culture, ‘Employee buy-in training & behaviour’ was revealed as the top pain point.

What are the top three challenges/pain points for your organisation in relation to Cyber Security?



“Maturity is frequently under attack by change in both the organisation’s technology and cybercriminal tactics. The digital transformation forced upon organisations by COVID-19 has disrupted the ‘security maturity’ of many organisations whose secure perimeter has, in many cases, evaporated. ‘Mature’ cyber awareness culture needs to be replaced by a ‘dynamic’ cyber awareness culture driven by threat intelligence to mitigate the new threats. The once a year click through PowerPoint presentation is never going to cut it.”

Ian Thornton-Trump,
CISO, Cyjax

“Staff need to be aware of the basic attack attempts but also more sophisticated attempts where attackers build rapport with the staff that have access to the crucial assets. I call these people your high-risk staff. People who have access to the crucial assets and data and are at the greatest risk of being targeted.”

Lisa Forte,
Partner, Red Goat Cyber Security.

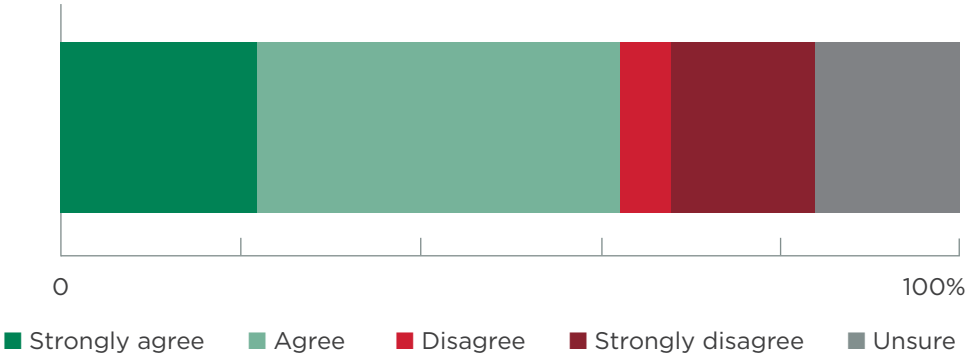
Section 3:
Risks and threats

Threats have more than doubled over the last 12 months.

Ignoring some self-serving information security vendor reports that claim 100 percent increases in threats, the year-on-year losses due to cybercrime from Europol, UK Action Fraud and IC3 in the USA all indicate substantial increases in loss and frequency of attacks.

62 percent of survey respondents believe threats have increased or substantially increased in 2020, 20 percent more than the CIO Survey, published in September, which suggested threats had increased by around 42 percent during the first wave of the pandemic. Worryingly 16 percent didn't know if threats had increased, perhaps because there were no metrics in place to track this. There is also a certain degree of shame associated with admitting a breach.

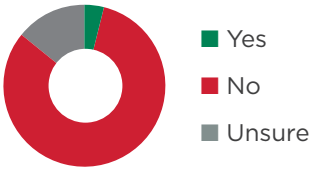
Have threats to your organisation increased in 2020?



Your supply chain, is it untouched?

The ambiguous definition of an organisation's supply chain is problematic. How the compromise is validated and what sort of visibility the organisation has into the compromise is also questionable. It is impressive to see over 80 percent of respondents categorically answering "No".

Has your organisation been compromised via the supply chain in the last 12 months?



"If the supply chain compromise was extended to include, information from public data breaches, lost and stolen devices due to shipping error, as well as identifying sensitive data stored by third parties in publicly accessible S3 buckets; that number may be significantly different. As for public data breaches, Marriott and EasyJet were two of the largest breaches in 2020."

Ian Thornton-Trump,
CISO, Cyjax

"Sending out a Supplier Risk questionnaire is time-consuming and in my experience yields limited results. However, the risks are real, with case studies such as NotPetya, and many others, this is something that always needs to be high on priority lists for organisations. You are only one supplier away from a breach."

Stuart Peck, Director of Cyber Security Strategy, ZeroDayLab Limited

Phishing, Social Engineering and Malware are amongst the most common attacks.

More than two-thirds of the attacks experienced were Phishing, or Social Engineering related. Spear Phishing and Malware were also reported as the most prolific attacks in the CIO Survey, which reinforces the need for training and educating employees.

Has the organisation experienced any of the following over the last 12 months? (successful or unsuccessful)

- Phishing/Social engineering
- Virus/Malware (Ransomware)
- Data Loss
- Service Interruption
- DOS/DDOS

"We can't forget the attack surface of exposed Remote Access services and perimeter risks. We've seen a range of RCE's in security products and outside of phishing, RDP attacks are still massively prevalent for ransomware actors to use a vector."

Daniel Card,
CEO, Xservus

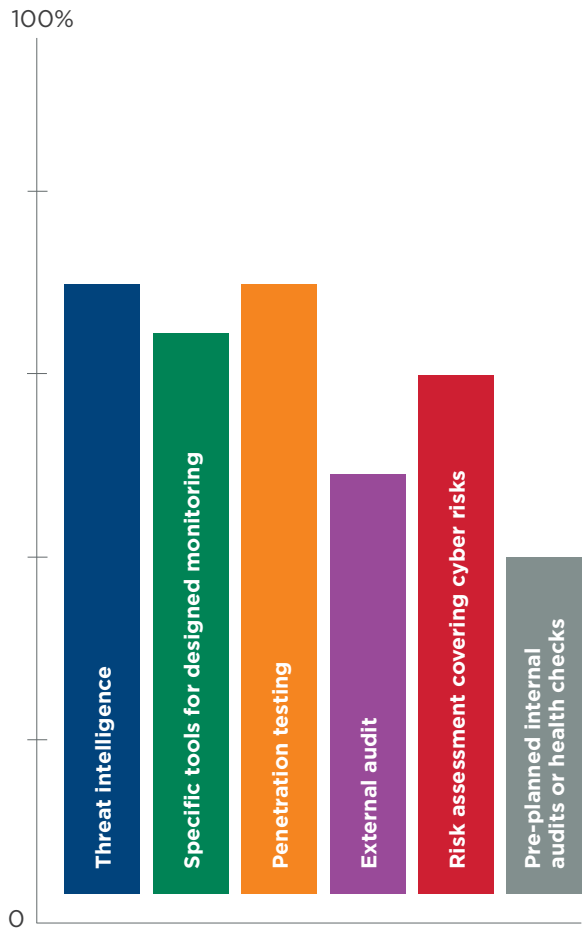
Nearly two thirds of organisations have monitoring tools in place.

Threat intelligence and penetration testing were amongst the most popular tools to identify risks.

"The only way for an organisation to survive is to understand the risks, avoid them if possible, and if not at least identify the cracks in the organisation that malicious actors may exploit. Detective controls for IoC 's are an excellent way for the security organisation to deliver assurances."

Ian Thornton-Trump,
CISO, Cyjax

How does the organisation identify risks?



End-point security in all our shopping baskets.

Assuming Anti-virus spend is a renewal of the existing solutions as opposed to a new deployment. Overall investment in security appears to be and remains end-point-focused.

Email filtering didn't make it into the top five despite well-known statistical data that suggests the majority of destructive cyber-attacks arrive via email. Undoubtedly the best security investments are those that prevent the most likely attack from reaching users.

Name three cyber products/services that your organisation purchased in the last 12 months...

"Pen Testing the organisation is an excellent investment because it identifies a baseline and a program of work to address the critical issues. This can lead to quick wins which can be achieved with the existing security solutions or network/server environment."

Ian Thornton-Trump,
CISO, Cyjax

THE BIG 5

End Point Detection and Response

Traditional Anti-Virus

Pen Testing

Firewall

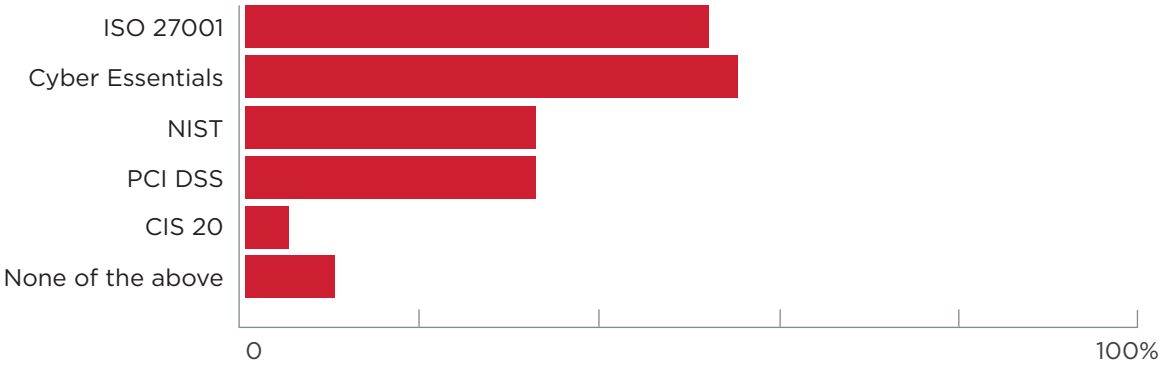
SIEM

Section 4:
Regulatory Compliance

Mitigating risks with regulatory compliance.

The survey uncovered some great news; most respondents have a security framework to measure their security controls. ISO 27001 and Cyber Security essentials are equally as popular.

Does your organisation use any regulatory compliance standard to mitigate cyber risk?



Data Protection: who is responsible?

Whilst everyone subject to GDPR must have a DPO function within their organisation, our survey found that more than two-thirds have a designated person to perform that role.

Do you have a Data Protection Officer? If no, are you planning to hire one over the next 12 months?

"A DPO is not a requirement under the GDPR, but there is still a requirement to protect data. Ambiguous ownership of data protection can be risky. If the ICO investigate organisations where there has been a data breach, and there is no clear ownership of privacy responsibilities organisations can often have difficulty evidencing their approach."

Ian Thornton-Trump,
CISO, Cyjax

Section 5:
Outsourcing

Around 4 in 10 businesses outsource aspects of Cyber Security; this proportion is lower among charities and higher in public sector organisations. Over 75 percent of our survey respondents are looking to third parties to perform security audits and pen testing. Research by the Department of Media, Culture and Sport (DCMS) confirms the sector is plagued by skills gaps, including penetration testing, forensic analysis, security architecture, incident response and a range of technical skills such as threat assessment.

Outside of pen testing and audits over 20 percent of respondents are outsourcing other security functions, 35 percent are using a third party to provide threat intelligence feeds, and this is likely to increase in the months ahead.

Which areas of your InfoSec or Cyber capabilities are outsourced?

THE TOP 3...

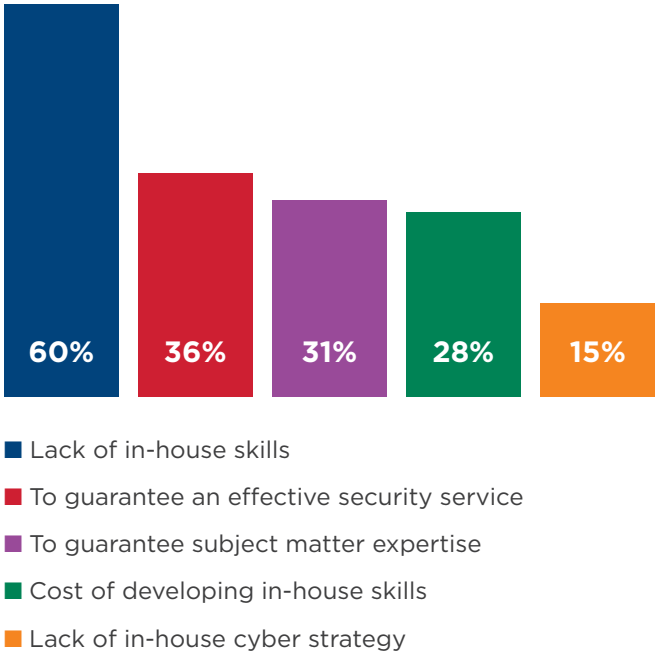
Why outsource when you can insource?

Of those that outsourced security functions, just over 60 percent are struggling to find the talent and skills they need in-house. Evidence that supports the narrative of a cyber skills shortage, but nearly 68 percent of respondents are looking for guarantees that Cyber Security advice is both accurate and effective. DCMS research also suggests that companies outsource to manage high workloads and to ensure against bias opinion in elements such as a security audit.

"Utilising specialist contractors can help businesses ensure agility which is essential in an unstable environment."

Andy Basham,
Senior Recruitment Consultant, Crimson

What are your primary reasons for outsourcing elements of Cyber Security?



Section 6:
Resourcing

Skills shortages/gaps, and budget influence recruitment strategy.

Despite an increase in attacks and Cyber Security's prioritisation, more than two-thirds of survey respondents have no plans to hire cyber professionals in the next 12 months; this could be conducive to stretched IT budgets.

However, earlier this year DCMS published figures on skills gaps and skills shortages. DCMS reported that two-thirds of firms had faced problems with technical Cyber Security skills gaps, either among existing staff or among job applicants.

The report also found that 22 percent of applicants lacked soft skills and over half of the businesses surveyed found generalist cyber roles hard to fill, with the percentage increasing for more senior positions.

In-demand roles include security engineers, security analysts, security architects, security managers and security consultants.

The sectors that commonly recruit include finance and insurance, information and communications, and professional services sectors.

We need to explore diversity.

Finally, a report by DCMS found that the Cyber Security workforce is not diverse and not in line with other digital sectors.

15% **workforce are female** (vs. 28% of the broader digital sector)

16% **ethnic minority backgrounds** (vs. 17% of the digital sector)

Diverse teams produce better results; there are some simple tactics you can use to help you diversify your workforce. Remove gender bias from job descriptions, request blind CVs from recruiters and make sure your interview panel come from a range of backgrounds. Diversity needs to be built into the culture of the business if someone in your company does not have ownership over the diversity journey consider working with a Diversity and Inclusion consultant.

"Without people you're dead. If you operate within the philosophy that the three pillars of security are people, process, and technology, never remove people from first position in that statement. They are not the weakest link in an organisation, they are the strongest."

Mike Thompson,
Information Security Manager, Zen Internet

Does your organisation plan to recruit Cyber professionals in the next 12 months?

Meanwhile, IT leaders are confident they know what they're looking for. Over 80 percent of our survey respondents said they have no problem writing job descriptions for Cyber Security jobs. The 'Cyber Security skills in the UK labour market 2020' report by DCMS, suggested differently, "Some cyber team heads found it difficult to align the job descriptions they were writing to particular qualifications. Some also felt that existing roles frameworks did not map well to qualifications."

"In a market where skills shortages exist, passive candidates (those that are not actively seeking a new role) is often where a recruitment company can help; our contacts enable us to spread the word amongst the cyber community. The new normal (flexible working/ homeworking) will create greater competition amongst employers. We work with employers who want to attract the best candidates by showcasing their brand."

Andy Basham,
Senior Recruitment Consultant, Crimson

Section 7:

The future of Cyber Security

Cyber Security climbs the priority ladder by 44%.

During the pandemic, many businesses have enabled employees to work from home, which has increased the attack surface. Many organisations needed to open VPN, RDP & OWA and did so without MFA, Access Control, and robust cyber hygiene policies. Opening these services to the whole internet without adequate security monitoring and controls may result in significant financial and operational impact. Threat actors are actively targeting poorly maintained infrastructure, which internally had many layers of security controls as protection but is now exposed.

It is therefore not surprising that IT departments have chosen to increase their focus on security.

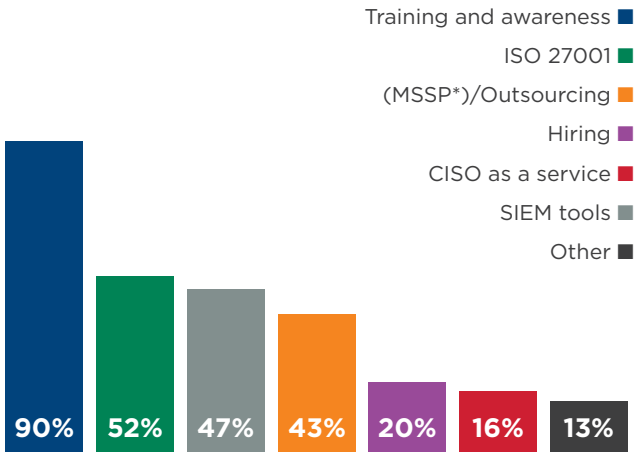
In a more remote world (since March 2020), how much would you say your organisation has increased its priority around Cyber?

2021 and beyond

What strategies will we be using to bolster our Cyber Security strategy?

There is an overwhelming response to training and awareness despite two-thirds of respondents claiming they have a mature Cyber Security strategy. However, as the pace of change increases, many organisations will be looking to improve and adapt their training programmes.

Which of these form part of your future Cyber Security strategy?



*Managed security service provider

"I can see two very distinct and divided camps when it comes to proactive and reactive approaches to security controls. In the proactive camp are those that identified a focus on adoption or support of an 'ISO 27001' Information Security Controls Framework. In the other camp, are nearly half of respondents that would like to improve or adopt SIEM technology - a very reactive approach to organisational security. Risk models will vary by sector, what mitigations are chosen to deploy will differ as well. It is interesting to see the two different camps revealed in the data."

Ian Thornton-Trump,
CISO, Cyjax

Cyber Security Leader Viewpoints

"Organisations are trending towards greater investment in security controls and visibility of Cyber Security at high organisational levels. I sensed a certain level of apprehension to security improvement from the results. However, security tools and outsourced services seem to be a focus, good news for vendors and third parties. It was disappointing to see organisations failing to invest in building, training, and hiring in-house security resources. Perhaps this organisational reluctance is based on uncertainty and COVID-19. Working from home has had a profound impact on Cyber Security tools, training and security resources, geographic constraints on resource availability are at least, for the time being curtailed - we can access more talent."

Ian Thornton-Trump,
Survey partner and contributor, CISO at Cyjax.

"I was pleasantly surprised to see the maturity of thinking around collective responses as we see peers gravitate towards the role of Threat Intelligence to make informed posture changes for organisations, and the use of standard frameworks such as ISO27001 to set out their best practice.

Seeing such high-volume use of Cyber Essentials Plus is also heartening, as it means that active Cyber Security thinking is starting to percolate across sectors.

There is still much to do across the industry. Still, as a 'state of the union,' it would appear that the value of Cyber Security in this 'Internet Age' is starting to be understood and enacted at Board levels. Increasing trust in services is vital to preserving the customer relationship and maintaining a healthy business."

Barry Richardson,
Head of Cyber Security, NHS Blood and Transplant.

"I was pleased to see the honesty of the responses to this survey. It is a great overall reflection of the industry. I was disappointed to see the low levels of diversity, but progress has been made, and we need to celebrate that. I have seen more spear phishing and an increase in long term attacks where the target staff member is befriended over time. Gone are the days of tick-box training that covers off the basic concepts. We need to go further and develop the level of confidence and independence of staff to spot and report nefarious contact. Using intelligence to inform defensive investment decisions will be crucial for 2021."

Lisa Forte,
Partner, Red Goat Cyber Security.

crimson®

CRIMSON
The Hive,
Kings Court, The Crescent,
Birmingham Business Park,
Birmingham, West Midlands
B37 7YE

T: 01675 466 477

Microsoft Partner

Gold Cloud Business Applications
Gold Cloud Productivity
Silver Data Analytics
Silver Datacenter
Silver Cloud Platform

www.crimson.co.uk