Insight Space

cyber insights programme

nccgroup

Paying off the cyber debt:

How are decision makers approaching cyber resilience in 2021?

Introduction

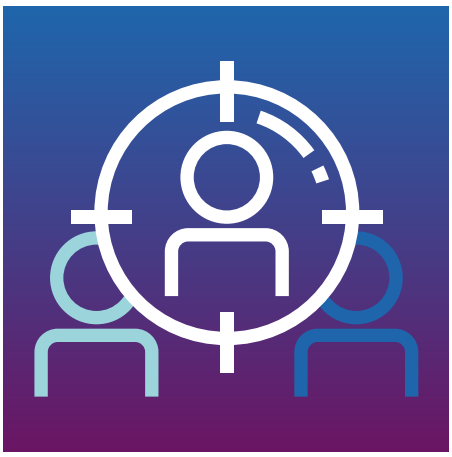
After more than 12 months since the first case of COVID-19 was reported to the World Health Organisation in December 2019, the coronavirus pandemic continues to challenge business leaders and cyber security decision makers around the world.

The speed and effectiveness with which many organisations have adapted to this challenge should be praised, with many discovering new efficiencies as a result. Inevitably, however, the circumstances have necessitated cost-cutting measures in a range of business areas, and cyber security is no exception: recruitment plans have been disrupted, creating internal skills shortages, while some decision makers have experienced stricter limits to their spending on cyber resilience projects.

Unfortunately, these measures have consequences for cyber resilience: organisations that made budget cuts, redundancies within cyber or delayed or cancelled cyber projects last year saw an increase in attacks. And, while nearly half of respondents to our recent survey felt that their organisation was 'very resilient' this time last year, just 38% have the same confidence in 2021. With the longer-term effects of the pandemic on organisations' security postures yet to be fully realised, it is crucial that organisations begin paying off this cyber debt to build resilience against the new threat landscape in 2021.

To understand how organisations planned to approach this in the next 12 months, we spoke to 290 cyber security decision makers from public and private sector organisations about the challenges and priorities facing them this year. The results highlighted four key areas of focus: people, investment, strategy and orchestration.

People: your largest untapped resource for cyber resilience?



From unknowingly clicking on a suspicious link in an email to insider threats from disgruntled staff members, it's no secret that employees can expose organisations to cyber risks. But the impact of the pandemic has thrown their role into sharp focus, highlighting employees' increasingly important contribution to maintaining cyber resilience.

When asked about challenges with human resource in 2020, 40% of respondents admitted that they had frozen recruitment in cyber, with 29% reporting that they had made staff redundancies. Worryingly, one in five had furloughed staff responsible for cyber resilience programs.

40%

40% of cyber leaders froze recruitment in cyber in 2020

EXPERT INSIGHT

"The pandemic - and specifically the lockdowns - has changed people's work patterns and behaviours significantly, which makes it harder for security leaders to manage people risk. Anomalies will increase significantly, particularly at the start, and it is important to recognise this and understand what it means for how activities of concern are spotted.

"Just as importantly, people are under very different stresses and often struggling to have a clear boundary between work and home life so engaging with someone that has given cause for concern must be done with even greater care than usual."

Stephen Bailey
Head of Cyber and Privacy Consulting

Filling the skills gap

The majority of decision makers acknowledged that operating without dedicated cyber personnel was an issue: two-thirds said that internal skills shortages represented one of their main security challenges for the next 6 months, while 31% claimed that 'more heads in the team' would make the biggest improvement to their cyber security preparedness.

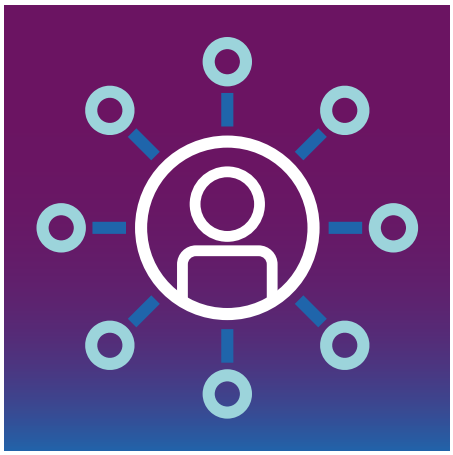
Encouragingly, decision makers are already planning to take action to mitigate risk in this area: of those that planned to increase the amount of cyber work that they outsourced in the next 12 months, 51% said that a lack of internal skills and capabilities was the top reason for doing so, followed by issues around staff recruitment and retention (50%) and internal redundancies (38%).

Respondents also demonstrated a willingness to upskill their existing staff members at all levels: 36% claimed that cyber security awareness training was the element of their cyber resilience work that they were most likely to outsource in the next 12 months, while 39% listed education of security owners on cyber best practice as the area their organisation would most benefit from.

EXPERT INSIGHT

"The human factor binds all the other elements of cyber resilience together. The types of individuals that succeed are details-orientated, have a high regard for problem solving, and work with transparency and autonomy. An appreciation for effective implementation of technology management is similarly important. There will often be trade-offs which need to be made, but ensuring you have the right people and promoting a safety-first culture, which has its foundations in measurement and management, is crucial to ensuring success."

Ollie Whitehouse
Chief Technical Officer



51%

51% will outsource to fill an internal skills gap in 2021

CASE STUDY

Response and rapid remediation for a charity organisation

After falling victim to a ransomware attack, a UK based charity enlisted NCC Group to investigate the incident, reassert control of the estate and stand up critical services. Like many other charities, the organisation had a severe lack of resources when it came to cyber security, and its small IT team was primarily focused on patching vulnerabilities as and when they occurred.

This shortage of skills and resources, combined with ongoing digital transformation projects, meant the charity did not have the time to perform necessary security upgrades or invest in further protections. After conducting a full investigation into the root cause of the attack, NCC Group's experts worked with the charity to remediate its vulnerabilities and protect the organisation from future attacks, saving considerable time and resources in the process.

Addressing the insider threat

In the past 12 months, the pandemic has forced most organisations to move some or all of their business operations online, and this was true for our cyber decision makers: 50% reported an increase in their use of remote working in 2020. And, while this operational shift has presented new efficiencies, our research suggests that it could also present security challenges: 66% of organisations that increased their use of remote working during 2020 saw an increase in phishing and malware attacks.

Notably, 39% of all respondents reported that accidental, malicious or inadvertent insider threats posed by current or former employees, contractors or partners had increased in the last 6 months. 51% believed that an increase in remote working was the main cause of this heightened threat, 39% blamed a lack of detection capability and 29% suggested that appropriate controls were not in place. This presents difficult questions for business leaders around how to effectively monitor security when their staff are out of the office.

Transitioning employees back to the office in the next 6 months was flagged as one of the top three challenges for decision makers, but the data suggests that organisations must act now to mitigate the insider threat.

39%

saw an increase in insider threats

Investment: how much is enough?

Quantifying risk has been a challenge for the cyber security industry for some time, and this issue has been exacerbated by the negative financial impact of COVID-19. Several organisations have had to deploy cost-cutting measures across the board, forcing cyber decision makers to work harder than ever to secure and justify investment.

Winning the internal battle

More than a quarter (27%) of organisations told us that they had experienced budget cuts that affected their spending on cyber resilience in 2020. With organisations continuing to enforce cost-efficiencies as they recover revenues lost to the pandemic, securing budget to support security initiatives was the second-biggest challenge facing our respondents in the next 6 months, with 68% referencing this as an issue. This situation appears even harder for those who had cyber budgets cut in 2020, with 60% expecting to see further reductions in 2021.

To overcome this hurdle, our research indicates that some decision makers will have to convince senior stakeholders of the importance of investing in cyber security. Of those who claimed that cyber is not a high priority in their organisation, 23% said that they don't have the buy-in of senior management, while 19% noted that investment was focused in other areas. Across all respondents, just under a quarter (23%) agreed that stakeholder buy-in would make the biggest improvement to their organisation's cyber security preparedness.

Overall, there was some optimism around budgets: 66% said they expected the total amount spent on cyber security by their organisation to increase in 2021, with just 7% predicting that spend would decrease.

Securing budget to support security initiatives is the second-biggest challenge facing cyber decision makers this year

EXPERT INSIGHT

"Whilst it is encouraging that organisations expect their budgets to increase, true cyber resilience can only be achieved if senior stakeholders are fully bought in. Without that understanding and commitment from the board, it can be difficult for decision makers to drive the strategy forward and make any tangible improvements. In these circumstances, having a focused improvement plan is imperative."

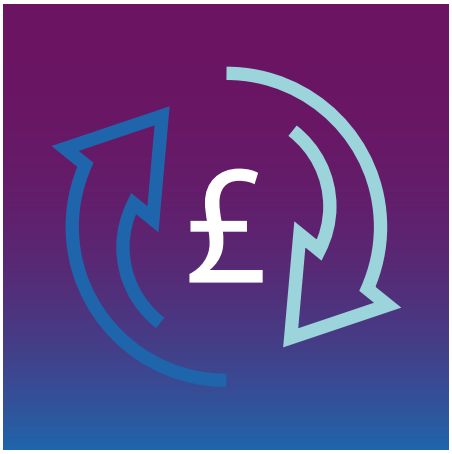
Gareth Pritchard
Associate Director at NCC Group

Making the case

The data suggests that there is room for improvement around validating the effectiveness of cyber security, which could help decision makers build an effective business case for investment in cyber when budgets are tight. To evidence this point, more than 90% of respondents admitted that they struggle to accurately assess or quantify the cost vs benefit of cyber security measures.

However, just 31% agreed that they'd benefit from benchmarking and validation of cyber security work done to date, revealing that many decision makers are missing an opportunity to identify priority areas, target their investment more effectively and measure improvements over time. By quantifying the effectiveness of their existing cyber security measures, organisations could better demonstrate their need for investment in cyber, something that many respondents appear to be struggling with. With organisations likely to continue scrutinising spend in all areas, recognition of the value of benchmarking and validation tools could increase significantly in the next 6-12 months.

Interestingly, of those who planned to outsource elements of their cyber security in the next 12 months, 43% said that this was being driven by return on investment. This suggests that organisations recognise the importance of validating cyber security spend, but it also suggests that businesses are not confident that they have the skills or resources to do so in-house.



90%

90% struggle to quantify the ROI of their cyber security measures

EXPERT INSIGHT

"As the cyber threat landscape evolves, having an up-to-date view of your organisation's cyber resilience against that of your industry peers and evidencing the efficacy of cyber security investments is critical. Making informed decisions without access to the right tools to provide insights across a range of cyber security metrics and datasets is challenging. So, whether you're establishing how far you've come since your last assessment or building a business case for targeted investment, benchmarking your resilience against recognised frameworks such as NIST should be factored into your cyber strategy."

Dominic Carroll
Product Manager and Service Architect

Strategy: built to last?

Threats in all areas have increased in the last six months, but the long-term impacts of COVID-19 on cyber resilience remain to be seen. In fact, 70% of respondents told us that understanding the threat landscape after the pandemic would be a challenge for them, making it the biggest challenge for cyber decision makers in 2021.

With this in mind, it is crucial that organisations proactively act to protect themselves in the short, medium and long-term and mitigate against current and emerging risks.

CASE STUDY

Protecting against threats to the global commodities sector

During routine monitoring for a global commodities organisation, NCC Group's Security Operations Centre (SOC) identified that unusual activity involving PowerShell, a scripting language that provides access to a machine's inner core, was taking place. Responding promptly, NCC Group's SOC analysts triaged the incident as high priority and alerted the organisation while beginning a more detailed investigation. After establishing that the incident was an attempted data exfiltration attack, NCC Group isolated the infected machine, containing the attack and eliminating the risk of wider propagation.

Had the NCC Group SOC analysts not acted as decisively as they did, there is a very real chance that the malicious actor could have established a persistent and undetected flow of classified information out of the corporate network. NCC Group's subsequent analysis and attribution also allowed the customer to adjust its defensive posture, leaving it in a better position to repel similar attacks in the future.

Assessing current posture

When asked about their ability to deal with the current threat landscape, almost 90% of organisations were confident that they could report a breach to authorities within 72 hours as per GDPR regulations, identify the root cause and fix it to prevent it from happening again.

However, the data suggests that there is more to be done, as only 38% of businesses consistently rated their organisation as 'very resilient.' Again, there is evidence that internal skills shortages are holding organisations back, with 71% of decision makers reporting that they are 'not confident' about improving or evolving their organisation's cyber security preparedness.

In terms of agility, decision makers estimated that they could detect and respond to an attack within 29 days, with more organisations taking over 1 day to respond to an attack (42%) than in 2020 (31%). Those with more employees were notably faster to respond to threats, with organisations of over 5,000 responding almost twice as quickly as those with 1,000 to 2,499 staff members.

38%

Just 38% of organisations believe that they are 'very resilient'

Securing digital transformation projects

Many organisations have turned to cloud-based software to support their shift to remote working, and four in ten of our respondents said that they increased their use of cloud and accessible software in 2020.

Encouragingly, decision makers had measures in place to manage the risk: 96% said that there was clear ownership for the security of cloud products in the organisation, while nearly half (48%) reviewed their security at least once a month.

However, 71% told us that the increased rollout of cloud infrastructure and services posed a challenge to the cyber security of their organisation, indicating that there are still some uncertainties around securing digital transformation projects among decision makers. As the threat landscape after COVID-19 becomes clearer, this data suggests that cloud could quickly become a key area of concern if its resilience is not assessed and improved within organisations.

4/10

Four in ten increased their use of cloud and accessible software in 2020

EXPERT INSIGHT

"The global pandemic has, in many ways, proven the value of successful digital transformation. It has also shown that true digital transformation has challenged many business and operational models, revealing new potential. By implementing a collaborative approach to SecOps and establishing a hybrid model that combines organisational focus, cloud-native solutions and third-party expertise, organisations will be better equipped to address an expanding attack surface, enhance productivity and boost overall resilience."

Nigel Gibbons
Associate Director and Senior Adviser

CASE STUDY

Moving to the cloud with confidence

When a major professional services client sought assistance in migrating its Security Operations Centre (SOC), which included two data centres, to the cloud, NCC Group's cloud experts were deployed to ensure that the migration happened successfully. The client, which had 250,000 users on its network, was reporting incompatibility problems with its incumbent SOC and was struggling to see and respond appropriately to security events.

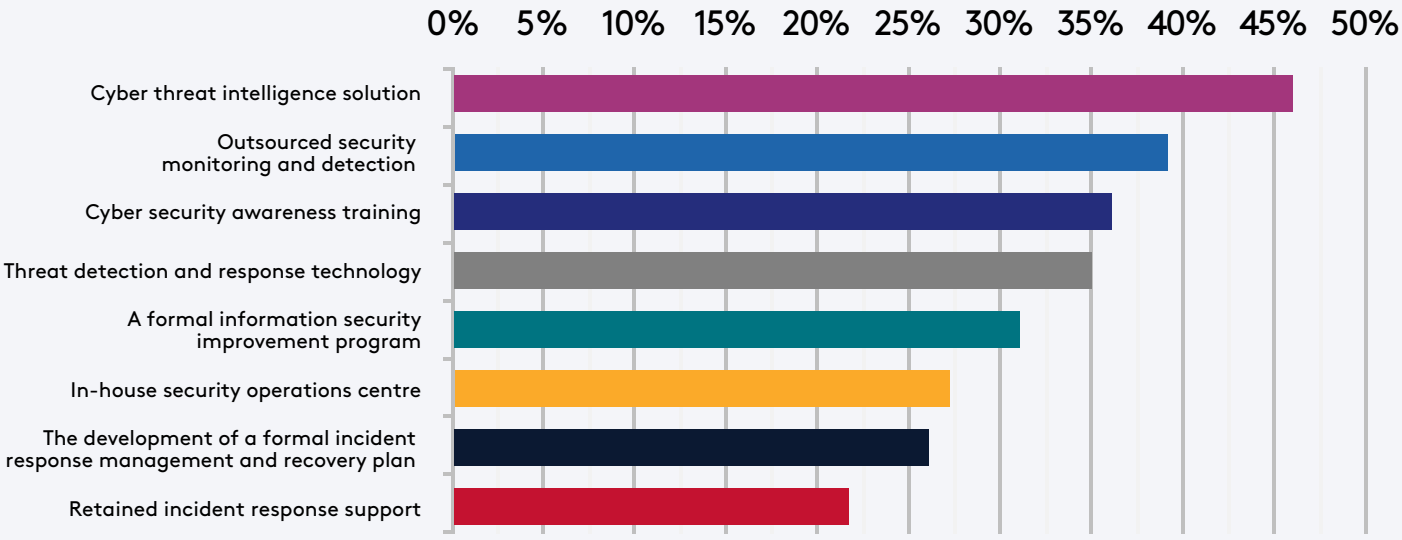
Over a four-month engagement, 12 NCC Group experts provided a full integration of on-premises SOC teams into the cloud. After threat modelling, harmonising standard operating procedures and creating incident response plans, the migration was conducted successfully, yielding noticeable security improvements, improved response rates to potential vulnerabilities and significantly boosting visibility of potential breaches.

Investing to strengthen resilience

The priority investment areas selected by our sample gives some indication of how organisations will look to strengthen their cyber resilience in 2021, with 'making security improvements' (76%), 'cyber threat intelligence solutions' (67%) and 'improved compliance, such as data or PCI programmes' (64%) making up the top three. 'Speed of threat detection' was the type of support that 46% of organisations agreed would benefit them the most.

Interestingly, respondents will turn to third-parties to help them achieve progress in these areas: 66% said that they would outsource more cyber resilience work in 2021, with threat intelligence (46%), security monitoring and detection (39%), cyber security awareness training (36%) and threat detection and response (35%) the elements most likely to be trusted to parties outside of the organisation.

Which elements of your cyber resilience work are you likely to outsource in the next 12 months?



Orchestration: do you have visibility over your IT estate?

Mapping and managing your IT estate is crucial to achieving cyber resilience, but gaining visibility of your inventory can be difficult. As a result of the pandemic, it's likely that IT estates have changed significantly and quickly through the addition of new cloud-based software, suppliers and other factors, but many organisations could be unaware of how these changes have altered their attack surface. With this in mind, regular monitoring and patching of your own estate and that of critical third parties will be crucial for decision makers in 2021.

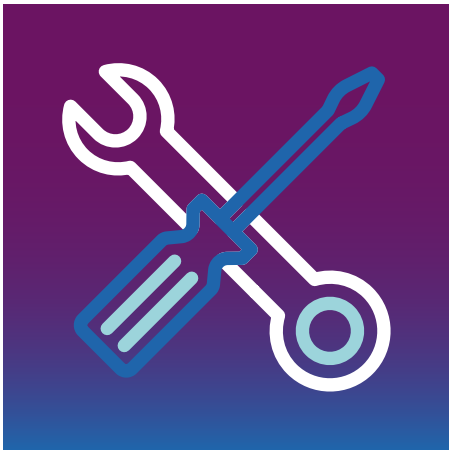
Shoring up defences

When asked how often they scanned their perimeter, including firewalls and browser isolation systems, 49% said they did so frequently. However, there was room for improvement with 37% only doing so occasionally.

As a vital part of security orchestration, effective patch management can help organisations to reduce their cyber risk by removing or securing unsupported legacy systems that should no longer have access to the internet. However, patching at pace and scale presents a number of challenges, making it difficult for IT managers to achieve total security coverage.

For example, 74% of respondents said that more than 50% of the connected devices on their IT estate are regularly patched, with just 21% claiming that all of their devices are regularly patched. This indicates that many are potentially leaving vast areas of their estates vulnerable to attack.

Threat actors can exploit vulnerabilities in unpatched systems and devices within hours, so applying security updates quickly and efficiently is essential: 20% of organisations said it takes them less than 2 days to patch, with 10% patching in less than a day. However, 49% said it took them a week or more, presenting a considerable window of opportunity to threat actors.



20%

Just 20% take less than 2 days to patch systems and devices

EXPERT INSIGHT

"To ensure that the wider estate is managed effectively, it will require continuous monitoring to ensure that any changes are spotted, and the inventory updated. One key element of the monitoring is the recording of any changes to your organisation's processes and the state of the systems themselves to ensure they are being kept up to date. Then, this will enable the organisation to perform the next aspect of what is widely called cyber hygiene: patch management."

Tim Rawlins
Senior Adviser

EXPERT INSIGHT

"Not all risks can be eliminated, so there are likely to be many vulnerabilities on your estate at any one time. From an operational resilience point of view, it is more valuable to consider the accuracy of the estate inventory and the time it takes to reduce the vulnerabilities, than the total number of vulnerabilities itself.

"This level of responsiveness reflects on the knowledge of the threats facing the organisation and its suppliers, the measures you need to have in place to protect it and your ability to respond and recover to any attack. So, consider the key metrics your CIO is offering you to see if they really are an accurate reflection of the overall risk to the organisation."

Tim Rawlins
Senior Adviser

Improving your cyber resilience in uncertain times

With COVID-19 continuing to affect countries all over the world, it's likely that understanding the threat landscape after the pandemic will remain a key challenge for organisations in the years to come.

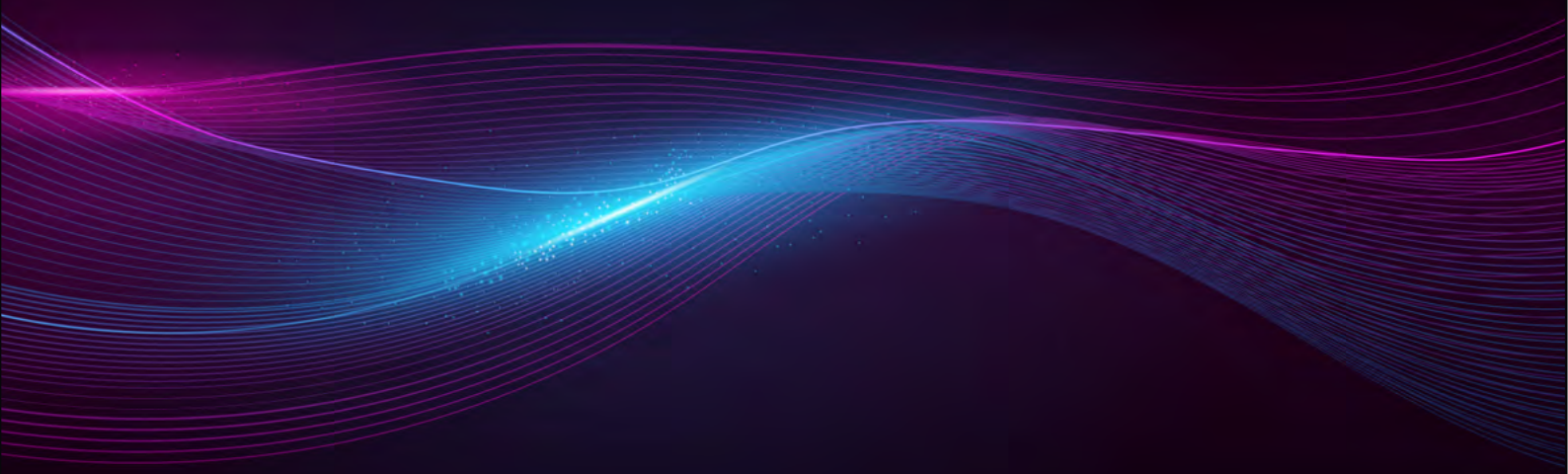
We discussed this in more detail on our recent Big Three Webinar. With the help of NCC Group's experts and Mark Ward, independent fraud, risk and security consultant, we answered the 'Big Three' questions about quantifying and paying off cyber debt post-pandemic.

Listen here ▸

Insight Space

cyber insights programme

nccgroup



About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

+44 (0)161 209 5111
response@nccgroup.com
www.nccgroup.com