Are people your largest untapped resource for cyber resilience?

Insight Space

cyber insights programme

Welcome to the NCC Group Insight Space

From unknowingly downloading a suspicious file in an email to insider threats from disgruntled staff members, it's clear that people can expose organisations to cyber risks. But the impact of the pandemic has thrown employees under the microscope, highlighting their increasingly vital contribution to an organisation's cyber resilience.

According to our research of 290 cyber security decision makers, 40% of organisations froze recruitment in cyber, 29% made staff redundant and one in five furloughed people responsible for resilience programs in 2020. However, those that did so experienced more cyber attacks in the last 12 months, suggesting a link between the strength of your people and the resilience of your organisation.

Meanwhile, the operational shift to remote working in the last 12 months has presented specific people challenges for organisations: 39% experienced an increase in insider threats, with 51% blaming increased remote working. This suggests that business leaders can't afford to wait until employees return to the office to mitigate this increased threat.

With that in mind, this issue of Insight Space focuses on how you can manage your people risk. Here, you'll find technical and executive insights, case studies and practical advice to help you to increase your cyber resilience during and after COVID-19.

"The operational challenges that organisations have faced in the last 12 months have resulted in a cyber security debt that must now be paid off. While it is encouraging to see that organisations recognise that they must make up lost ground by investing in cyber, it is crucial that these budgets are used in the right areas.

"People are one of the biggest untapped resources for cyber resilience, so decision makers should prioritise this area by investing in their teams as cost-effectively as possible. By addressing internal skills shortages and reducing the risk of insider threats, organisations can build a secure platform for growth and maintain cyber resilience in this difficult period."

- Ian Thomas,
  Managing Director at NCC Group

Contents

Addressing the insider threat

Filling the skills gap

Additional insights

Insight Space

cyber insights programme

nccgroup

Addressing the insider threat

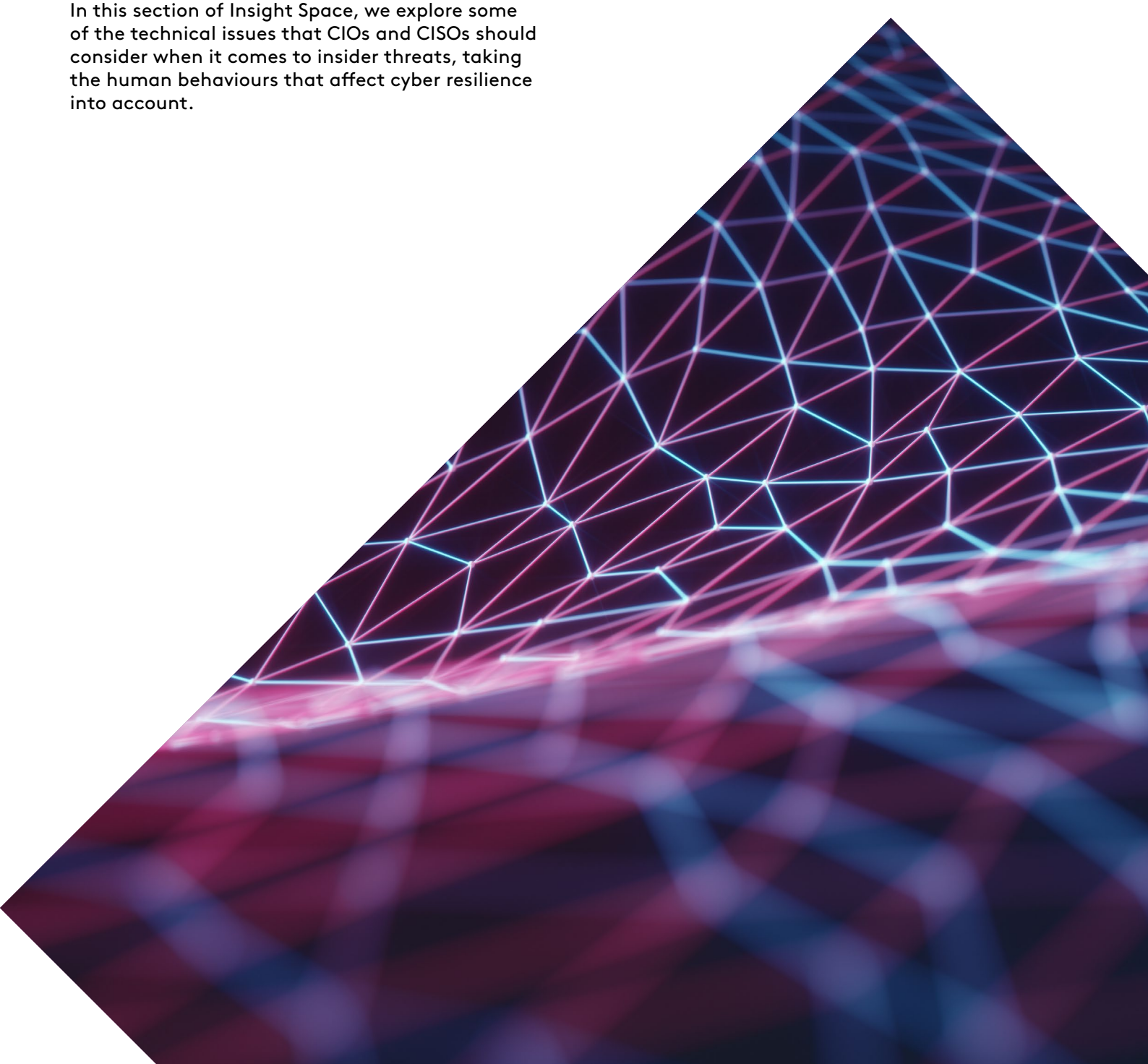
Addressing the insider threat

In the past 12 months, the pandemic has forced most organisations to move some or all of their business operations online.

This operational shift has presented new efficiencies, but it has also presented security challenges: insider threats posed by current or former employees, contractors or partners have all increased in the last six months. Transitioning employees back to the office will be a priority for many, but this increase suggests that organisations must act now to mitigate the insider threat.

In this section of Insight Space, we explore some of the technical issues that CIOs and CISOs should consider when it comes to insider threats, taking the human behaviours that affect cyber resilience into account.

We also reflect on those issues from an executive's perspective, giving you practical advice to reduce your organisation's risk of insider threats while working remotely.



Insight Space

cyber insights programme

nccgroup

Technical Viewpoint

The insider threat: understanding the human behaviours that impact cyber resilience

Ollie Whitehouse

Introduction

When a cyber attack happens, it can be easy to point the finger at users who may have been the trigger or inadvertently involved in a breach, but playing the blame game is both toxic and often counterproductive. Instead, it's important to dig into the human factors and behaviours that lead to a cyber security incident.

Often, the underlying cause can actually be a combination of human, business process and technical factors. Research into human factors and the insider threat continues to be an emerging and evolving field of study in cyber science. Within this research, it is recognised that despite the often-held misconception that systems would be far more secure without users, people can indeed be the strongest link, especially when you educate them about their role in keeping the organisation secure.

Taking into account the behaviours of people

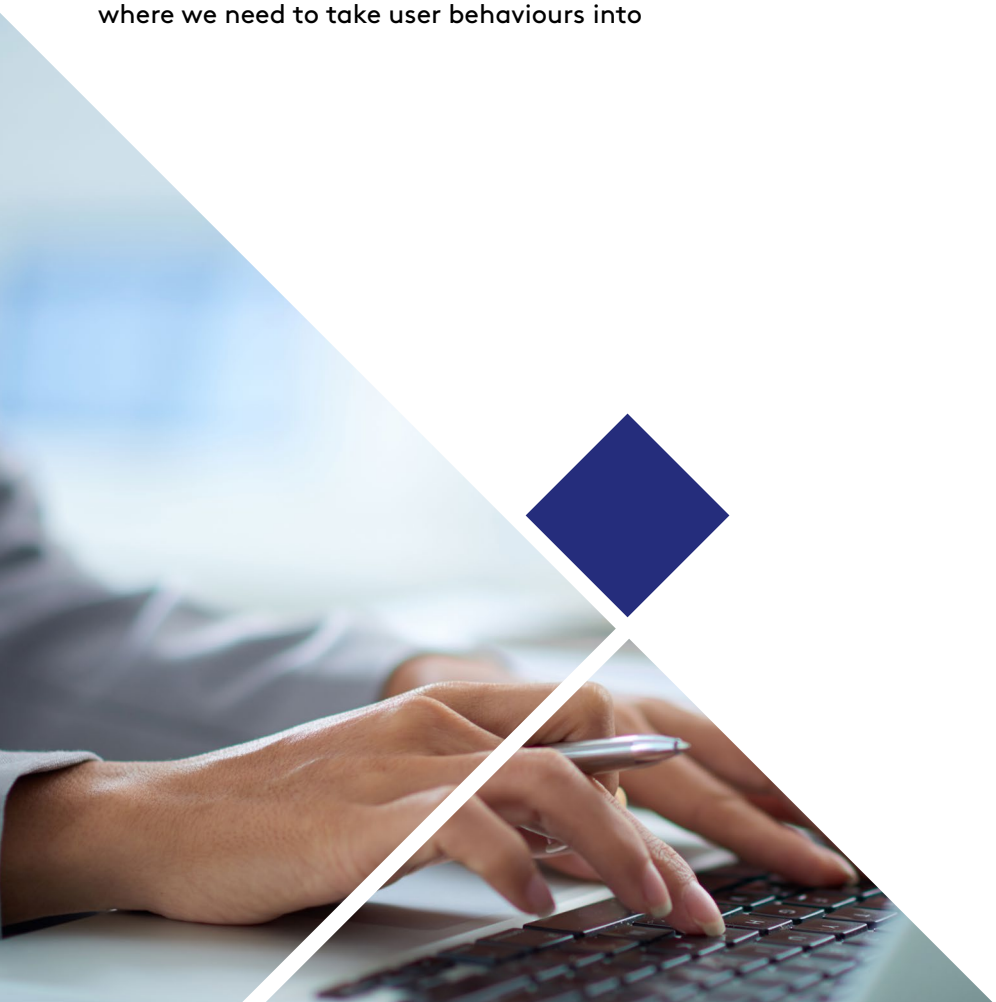
With the proliferation and evolution of phishing emails, it's becoming harder for users to spot a malicious link or attachment, especially when they come from a convincing contact or colleague.

Read any serious phishing research and the statistics will show that with any user population of any reasonable size, the chances are that more than 10% will fall victim to phishing attacks.

This is one example where user behaviours need to be taken into account. If your security strategy relies on the fact that people won't click on links or open attachments, despite this being crucial in roles such as recruitment – then you quickly see how critical it is to have a viable resilience strategy. This strategy should be airtight and ensure that if and when a user becomes a security weakness, you can prevent, detect or otherwise mitigate malicious activity.

Similarly, various research shows that if you put too much temptation in front of someone, the risk that they will take advantage for personal, ideological or other gain increases. This is another example where we need to take user behaviours into account. If your security strategy solely relies on the integrity and stability of your staff, you can see how this might quickly unravel in the real world, and the possibility of a truly malicious insider compromising your organisation.

Finally, when thinking about cyber security and information technology professionals, it's important to understand our own biases for solutions. The University of Bristol's Decisions and Disruptions game, which was developed to analyse the decision-making behaviours of various stakeholders across a business, proves that a technology-focused bias exists. Results from the game showed that cyber personnel and leadership are technology-driven, whereas those in IT were the only group to materially consider human factors and intelligence gathering, both of which are just as crucial as technology when it comes to formulating robust security strategies.



User-centric security design

Users are not cyber security experts for the most part and asking them to make decisions which oscillate between everything is fine and everything is on fire by simply clicking one of two choices next to each other is going to raise the table stakes accordingly.

This is where a user-centric security design can prove effective. Put simply, this is where the flow of the process, user experience, tools and day-to-day operations are considered.

While there are various considerations, the key ones to prioritise include:

- How onerous are security controls on the practices and processes of various business functions? If too onerous, they will be worked around and undermine security no matter how secure.
  - The Royal Holloway University of London's Information Security Group delves into this more in their paper 'Inclusive Security: Digital Security Meets Web Science'.
- How fit for purpose are the business processes? Overly complex processes during periods of high cognitive load can often fail.
- How intuitive or easy is it to make mistakes which result in security consequences? For many, this could be the user experience, which has been explored in more depth in the following publications:
  - The UX of Things: Exploring UX Principles to Inform Security and Privacy Design in the Smart Home
  - Usability Research in Support of Cyber-Security

Practical examples of user-centric security design vary, but a couple of examples include:

- Virtual desktop infrastructure (VDI) – cloud or on premise – which can be used for various discrete use cases, such as web browsing, email or privileged user function. This approach has a number of benefits:
  - The user experience is familiar and can be akin to native applications
  - Allows compartmentalisation which provides resilience and detection opportunities
  - Provides the organisation the ability to apply variable policies and controls
  - Can be ephemeral precluding persistence by threat actors
- Privileged access management (PAM) provides real-time and auditable access to systems and applications in an automated manner:
  - Easy-to-use from a user perspective
  - Prevents a build-up of long-term high privileged access on particular users
  - Provides an audit tail which provides detection opportunities

With more employees working from home than ever, this approach will be even more helpful in bringing the user's machine into an environment where maximum resilience benefits can be provided without impacting functionality or the user experience.

Monitor host, application and user behaviours

Managing the risk from the insider threat has its basis in strong identity and access management (IAM), coupled with behavioural monitoring to identify suspicious or outright malicious behaviour.

However, this root of identity and access management and monitoring shouldn't solely be about the people of a system. With many more machine-to-machine interactions and thus application-to-application interactions, it is equally critical to consider these as part of the overall solution.

This widening of the scope is why we have seen the original acronym of user behaviour analytics (UBA) expanded to user and entity behaviour analytics (UEBA). Or more simply put, the application of statistical modelling on a set of properties to detect those activities that might be suspicious or malicious – often described as analytics or machine learning.

For this type of strategy to be effective, there are several factors to keep in mind:

- Telemetry coverage and context: this is our eyes on the problem. If we can't see it happening and don't have context, it's near impossible to detect systematically.
- Analytics with various horizons: this is our brain for deciding what is abnormal. For this to be effective, we need various time horizons on the models. Some will be minutes, while others are months. This approach ensures that we can detect both the long and slow attacks, as well as the smash and grab breaches.
- Alerting and context: this is what drives our response to allow us to quickly contain and remediate issues.

This monitoring then occurs across the full stack:

- Hosts: examining which hosts are communicating to which, on what protocols and by how much.
- Applications: looking at which applications are communicating to which, what other processes are they spawning, how much data are they sending and receiving over the network and where to.
- People: assessing which people access which applications or data sets at what times of day, in what quantities and what they are doing.

This visibility allows organisations to detect what is anomalous and what should be classed as abnormal behaviour. This is the crux of UBA and UEBA – that is:

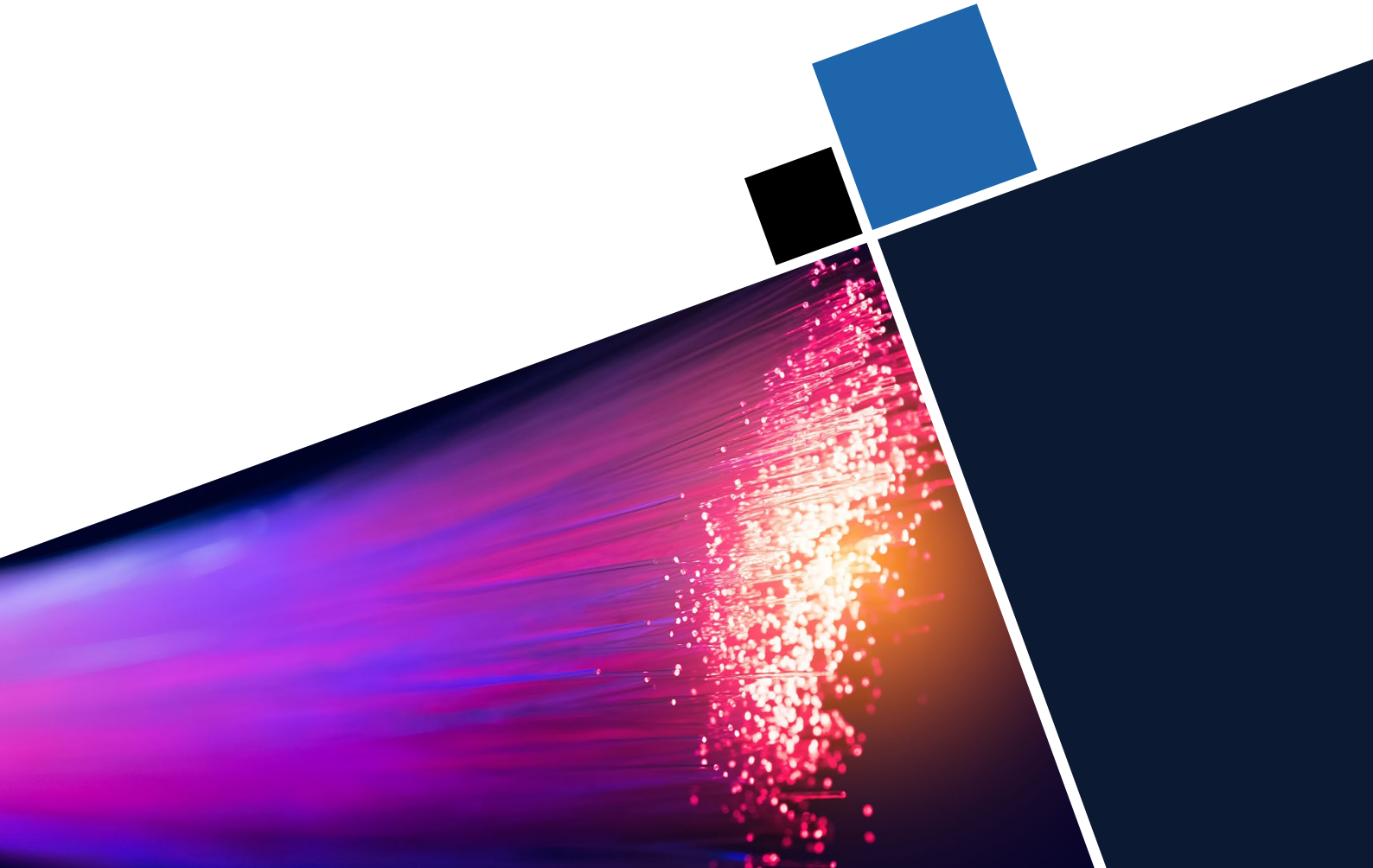
- Strong identity of host and user
- Comprehensive telemetry coverage across network, host, application and user behaviour
- Analytics working various time spans and horizons using technologies (depending on use case and coverage), such as Apache Kafka, Microsoft Sentinel or Splunk

However, the complexity involved in building, maintaining and responding is still beyond the sustainable ability of many organisations in reality. This is why managed detection and response (MDR) services are such a valuable offering in the cyber resilience space.

Conclusions

The insider threat takes many forms – from the truly malicious to the otherwise honest yet complicit through no fault of their own. As the world moves to a post-pandemic model of working, organisations should consider how they think about the insider threat across their people, processes and technology.

Most importantly though, organisations should ensure that the burden is not put on the user. Creating a culture of openness and awareness as opposed to one of blame is crucial. Getting the balance right between this and technology can be difficult, but it is how one can achieve true resilience.



Insight Space

cyber insights programme

nccgroup

Executive Analysis

Three actions to reduce insider threats while working remotely

Stephen Bailey

The shift to remote working during lockdown has presented specific security challenges for organisations: 39% of respondents to our survey of 290 cyber security decision makers reported that insider threats have increased in the last six months, and 51% believed that an increase in remote working was the main cause for this.

Whether they are malicious or accidental, insider threats can take various forms including disruption to systems, theft of intellectual property and fraud. However, all insider threats can expose organisations to cyber risk, so it's vital that you take action to address them.

In a separate paper, our chief technical officer, Ollie Whitehouse, explores some of the technical issues around insider threats that your CIO or CISO should consider. In this briefing, we reflect on those issues from an executive's perspective, giving you practical advice to reduce your organisation's risk of insider threats while working remotely.

OPTIMISE YOUR CONTROLS

According to our research, 29% of decision makers agreed that a lack of appropriate controls had contributed to their increase in insider threats. This can partly be explained by the fact that organisations have been forced to establish new remote working infrastructures quickly, without always understanding the risks of doing so. In many cases, these infrastructures will have included exceptions to pre-lockdown security controls such as greater leniency when granting access to files and the disabling of multi-factor authentication. However, these exceptions could all make it easier for insiders to compromise sensitive information while appearing legitimate.

With this in mind, organisations should ensure that they have a strong Identity and Access Management (IAM) framework in place across their remote working set-up. IAM covers the policies, processes and systems that govern the roles and access privileges of individual network users. Ideally, this should include clear policies around who can access certain systems, data or functionalities and why, and the circumstances in which those privileges could change according to the business's need.

Among other things, IAM should also mandate users to establish their identity before authenticating that identity with multiple factors including passwords, two-factor authentication or biometrics. However, it's important that your IAM controls aren't so strict that they deny users the privileges they need to carry out their day job. In these circumstances, people will often develop workarounds, heightening the risk of accidental insider threats and wasting time and resources required to investigate them.

To mitigate against this, ensure that someone is actively checking incident logs to bucket insider incidents into accidental and malicious categories. If you're regularly seeing accidental security alerts, speak to your people and your IT team to ensure that your controls are fit-for-purpose and consider adjusting them accordingly. When they are optimised in this way and combined with the concept of least privilege, which only provides users with the minimum levels of access and permissions needed to do their job, IAM controls can be a powerful defence against insider threats.

IMPROVE YOUR DETECTION CAPABILITIES

Often, there is no obvious pattern to indicate that an insider threat attack is imminent or ongoing. However, 39% of decision makers that suffered an increase in insider attacks in the last six months blamed a lack of detection capabilities, indicating significant room for improvement in this area.

To detect insider incidents as early as possible, implement a logging or monitoring system to provide visibility of activity across the network and create clear benchmarks for what constitutes 'normal' vs 'anomalous' behaviour for each individual system. For this solution to be effective and to avoid missing suspicious activity, it's also important to appoint someone with responsibility for regularly checking alerts and output. Pop-ups that warn a user that their activity is being monitored when they try to access restricted areas can also be helpful deterrents against insider activity, and can be used as part of a detection solution.

As part of this detection of network traffic, monitor for indications of mass data exfiltration or large data transfers via removable media such as USB flash drives. This could indicate that an insider is transferring data from the organisation maliciously, so it's important that you can identify this quickly and easily. Fingerprinting data and analysing it as it passes the boundary of a company through Data Loss Prevention (DLP) solutions can be effective safeguards here.

TRAIN YOUR PEOPLE

Of the respondents that reported an increase in insider-related incidents in the last six months, a third believed that a lack of training or awareness within their organisation was behind this. As such, it is important that cyber security teams take a holistic view to defending against insider threats, focusing on training and awareness alongside technical controls and detection measures.

Firstly, ensure that your training programmes are updated to reflect people's new ways of working and that the content of the material includes real, current events and incidents that people can relate to. For example, we have seen a rise in phishing attacks that label ransomware with titles including COVID-19 in the last 12 months, so share examples of these attacks with your employees. This will increase the impact of the training and be more likely to bring about meaningful change in people's behaviours.

Next, ensure that your employees know what key indicators of a potential insider threat looks like and empower them to anonymously report suspicious activity to senior management. Organisations should also tailor their training to the specific threats to your organisation. We have seen many organisations use the same generic security awareness materials for all staff without updating them on a regular basis. However, the insider threat landscape has evolved through remote working, offering more opportunities to access and compromise vital assets, so this approach is ineffective.

With this in mind, you should tailor training according to users' roles. For example, someone responsible for monitoring incident logs should receive different training to an everyday user. Additionally, those with escalated privileges should be informed on best practice around the security of the assets that they can access so that they can spot any malicious activity towards those assets.

No training program will ever completely remove the likelihood of an employee clicking on a suspicious link. However, these measures will help employees to feel more engaged with the security of their organisation, flag suspicious activity earlier than they would have done and be less inclined to consider a malicious attack themselves, all lowering the risk of an insider attack.

CONCLUSION

It's important to have empathy when dealing with insider threats. Personal changes and challenges have accompanied the operational shift to remote working, leaving people juggling the demands of their partners, children and pets alongside their professional responsibilities.

This process has meant that traditional working hours and practices, well known by cyber defence teams, have become very different. For example, early starts to get on top of work before taking over the home schooling so partners can focus on their work for the rest of the day are now commonplace, as are new ways of sharing data, files and access via cloud-based software that businesses have integrated under lockdown.

Previously, all of these things could have been flagged as suspicious activity, but it's vital that you don't alienate employees by casting doubt on their behaviour while working remotely. Ultimately, this new way of working is here to stay, so it's vital to make it as easy as possible for people to follow security guidelines rather than asking them to change their new behaviours.

By optimising their controls, increasing their detection capabilities and upskilling their staff, organisations can go a long way to reducing their risk of insider threats while working from home.

Three actions to reduce insider threats while working remotely

1. **Optimise your controls:** implement strong Identity and Access Management (IAM) controls across your remote working infrastructure and assign someone to monitor and optimise them on a regular basis.

2. **Increase your detection capability:** use a logging or monitoring system to ensure visibility of your network traffic and identify anomalous behaviour.

3. **Train your people:** deliver bespoke security training for every level of your organisation and update your training materials to include real-world examples of insider threats.

Insight Space

cyber insights programme

nccgroup

Filling the skills gap

Filling the skills gap

Despite multiple initiatives to address the cyber security skills gap in the last decade, it remains a major problem for organisations.

The gap has been widened by cost-cutting measures during COVID-19, with many freezing recruitment in cyber, making security personnel redundant or furloughing people responsible for cyber resilience programs in the last 12 months. However, organisations that cut their people budgets reported an increase in every type of cyber attack in 2020, indicating that your people have a direct impact on the resilience of your organisation.

In this section of Insight Space, we offer you technical and executive analyses around how you can reduce the skills gap in your organisation.

We explore the technical skills that are needed to enhance cyber security, the importance of creating a culture of resilience and how cyber skills can be a business enabler. We also share practical actions to build your resilience quickly and effectively, focusing on recruitment, training and outsourcing.

Insight Space

cyber insights programme

nccgroup

Technical Viewpoint

Cyber resilience skills: please mind the gap

Ollie Whitehouse

The scale of the gap

Cyber security has evolved into a complex profession with various sub specialisms. The supply of talent to meet these needs has not generally kept pace with demand.

In response to this, there have been significant endeavours over the last ten years to drive talent into these roles.

These endeavours include skills frameworks, such as the Chartered Institute of Information Security (CIISec) Skills Framework, Australian Signals Directorate Cyber Skills Framework, European Cyber Skills Framework, and the Canadian Centre for Cyber Security Role-Based Framework.

A number of professional industry bodies have also been instrumental in driving talent forward, including the Chartered Institute of Information Security (CIISec), Australian Information Security Association and the National Cybersecurity Society.

As well as this, a range of engagement, training and upskilling initiatives have encouraged greater engagement with the profession from a younger age. This includes the UK Cyber Discovery programme, CyberFirst UK, the Youth Cyber Exploration Programme, Singapore, as well as the Cyber Assembly, Singapore.

A global glance

Despite these initiatives and measurable strides being made, the estimated skills gaps continue to be significant.

According to research from the UK government, 48% of businesses in the UK have a basic skills gap, 30% of businesses in the UK have an advanced skills gap, and 27% of businesses in the UK have a gap with regards to incident response.

Outside of the UK, 80% of German businesses surveyed in 2020 said they had a skills gap, and 15% said they would have cyber roles which would go unfulfilled. As well as this, (ISC)2 estimated 561,000 cyber security jobs in Europe would go unfilled, and in the USA there is currently a shortfall of 3.12 million cyber security professionals.

INTERNAL SKILLS MAINTENANCE IS NOT ALWAYS ECONOMICAL

Indeed, NCC Group's own research has shown that 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 they are not confident that they have the skills or resources to do so in-house.

NICHE SKILLS NEED NURTURE AND INVESTMENT

If we start to look at the very niche roles which exist in cyber, it is no surprise that people with the relevant skills are in short supply. Those that excel are often driven by a mixture of intellect and wider aptitude, commitment to lifelong learning and discovery, and have an intrinsic interest in the subject. But there is also the continued development and investment in maintaining and developing these expert practitioners that non-specialist organisations often wrestle with.

Good reverse engineers to analyse malware, great intrusion analysts and incident responders, amazing quantitative analysts who also understand cyber security, sublime DevSecOps people through to those information security risk managements who can tell you the most impactful 5% of things to do. The scarcity of these people, high expectations around personal development, and a market demand which outstrips supply presents unique challenges around talent attraction and retention.

A SPECTRUM OF CYBER SKILLS AND KNOWLEDGE

Technology dependence

As society becomes ever more technologically dependent, it has been recognised for up to nearly two decades that cyber skills need to permeate all professions – from medicine to law to engineering and everything else in between.

Cyber skills in organisational leaders

Similarly, the importance of security skills across organisational leadership is now recognised – from non-executive directors, the chief executive officer and chairperson, through to the operational board. This has led to various educational institutions offering MBAs in cyber security, including the likes of Rutgers.

Baseline skills for all

A baseline set of cyber skills in all facets is increasingly important, both competitively and operationally to allow organisations to function in an agile manner with confidence.

All employees in an organisation have a role to play in ensuring its cyber resilience. These employees are our eyes and ears, as well as the first and the last line of defence. A baseline needs to be set across an organisation to ensure that every single employee has the knowledge to keep this first line of defence up. However, for them to work effectively, culture is an important facet.

Culture of resilience

Organisations and their operations are complex systems. The book Drift into Failure talks about how organisations that empower people to speak up, challenge and have delegated authority are, in real-world terms, the most resilient from a safety perspective. This insight has significant application to the cyber resilience world.

CYBER SKILLS AND A BUSINESS ENABLER

NCC Group's research showed that 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 an increasingly global yet hostile world in which we navigate a state of 'unpeace', cyber skills are a business enabler. Cyber resilience allows organisations to move at pace with confidence and take advantage of the opportunities presented.

How so? Well, if you are an organisation that has experienced rapid digital transformation and haven't been held back by cyber resilience fears, it's clear that you are best placed to adopt new technologies to further your competitive edge in a cost-effective manner.

However, if you are an organisation drowning in a sea of technical debt and legacy systems, or wilting under the weight of unpatched vulnerabilities or suffering sleepless nights on whether a breach will be detected to and responded to effectively, one sees the very real-world impact of the skills and capacity shortage.

A cyber resilient business supported by skilled staff, be they internal or supplier-based, is a confident one. These businesses will often have a capability and agility edge over one which is just about hanging on. This is the true enabler that skills and capability bring to the organisation, its operations and its business.

KEY TAKEAWAYS

When it comes to cyber resilience, people are three things:

- The leaders and direction setters
- The first and last line of cyber resilience
- Our capability

However, for them to be effective and the organisation to be confident and resilient, the right culture must be created, where investment is directed towards providing training and developing of cyber skills. Only by doing so can organisations expect to operate in a manner which catches the advantage from technology in an ever-hostile world.

For this reason, some organisations may look to outsource key cyber security functions, especially those who struggle to attract and retain the very specialist skills needed.

Insight Space

cyber insights programme

nccgroup

Executive Analysis

Three actions to reduce your cyber security skills gap during COVID-19

Stephen Bailey

Despite multiple initiatives to address the cyber security skills gap in the last decade, it is still a major problem for organisations: according to our research of 290 cyber decision makers, internal skills shortages are one of their main security challenges for the next six months.

These shortages have been exacerbated by cost-cutting measures during COVID-19: 40% of respondents admitted that they had frozen recruitment in cyber in 2020, with 29% reporting that they had made security personnel redundant. One in five had furloughed people responsible for cyber resilience programs.

However, organisations that cut their people budgets reported an increase in every type of cyber attack in the last 12 months, suggesting that the strength of your people is directly related to the resilience of your organisation.

With this in mind, we outline three actions to reduce your cyber security skills gap and build resilience against the new threat landscape that has emerged during COVID-19.

TARGET YOUR RECRUITMENT

Nearly two-thirds of respondents claimed that 'more heads in the team' would make the biggest improvement to their cyber security preparedness. However, recruitment can be costly and time-consuming, so it's important that it is focused on quality rather than quantity. Practically, this means that you should identify the specific skills that your organisation would benefit from and target your recruitment to provide those skills.

Firstly, review your business strategy and create a security roadmap to determine the skill sets that you will need to execute that strategy. For example, if you are launching digital transformation projects, you will need people with specific expertise around moving to the cloud. If you are acquiring or merging with another organisation, you need someone who can assess the risks of that organisation and how it will affect your security posture.

If you don't know what your current security requirements are, consider assessments such as red teaming exercises or cloud security reviews that can identify your risks in specific areas. Benchmarking tools can also help you to establish your short, medium and long-term priority areas, enabling you to recruit strategically and cost-effectively within those areas.

Ultimately, cyber security is such a broad subject that it is impractical to recruit experts in every area. By focusing on the specialisms that are most relevant to your strategy and security roadmap, you can cut through the competitive cyber recruitment market and acquire the skills that will tangibly increase your resilience against cyber threats.

DEVELOP AND RETAIN YOUR TALENT

The competition for skills has driven cyber salaries sky high, so it's not surprising that they were some of the first to be cut when budgets tightened during COVID-19. However, half of our respondents admitted that they had issues with recruiting and retaining cyber expertise, indicating that they are not confident of doing so even when they can afford it.

People regularly leave to secure a higher salary elsewhere, creating a revolving door effect that makes it difficult for organisations to address their skills gaps. However, skilled individuals also leave because their employers fail to deliver a well-defined career path for them, presenting an opportunity for you to develop and retain your talent more effectively.

Start by reviewing exit interviews to establish why previous employees decided to leave: 71% of decision makers told us that they are 'not confident' about improving their organisation's security posture, so ensure that you offer tailored training and development initiatives that empower people to do their jobs effectively.

You should also consider an apprenticeship and training scheme to develop the skills that your organisation requires internally. By giving your senior employees responsibility for training those apprentices, you can give them a greater sense of purpose and career satisfaction, reducing the likelihood that they will be tempted away by other organisations.

It's likely that you will need to recruit specialists in some areas. However, by investing in your existing talent, you can reduce your skills gap without committing huge chunks of your budget. You can also make your organisation more attractive to new recruits as budgets recover from the impact of COVID-19.

OUTSOURCE EFFECTIVELY

Outsourcing is one of the most effective ways for an organisation to complement and strengthen its internal resources, and 66% of respondents told us that they intended to trust more aspects of their cyber resilience activities to third parties in the next 12 months.

With budgets stretched, outsourcing offers decision makers a quick and cost-efficient method to improve their cyber resilience until they can afford to recruit dedicated specialists. It also allows organisations to determine their resource requirements before making firm commitments to spending on recruitment, enabling them to allocate their budgets more effectively.

For example, respondents told us that cyber threat intelligence and security monitoring and detection were the two areas of cyber resilience that were most likely to be outsourced in the next 12 months. Both of these fields require dedicated teams of experienced specialists working around the clock to stay ahead of threat actors and new attack trends, so it would not always be practical for many businesses to recruit here.

Outsourcing can also give organisations the flexibility to address specific short-term security requirements that can't always be addressed internally. For example, more than a third of respondents planned to outsource cyber security awareness training, indicating that they recognise its importance but are not confident that they have the resources to deliver it in-house.

Against the new threat landscape, this 'try before you permanently buy' approach could be an effective way to determine which skills your organisation needs to recruit and which you can afford to outsource. By relieving under-resourced security teams, it can also reduce the skills gap in the short and long-terms.

CONCLUSION

Understanding the threat landscape after COVID-19 was named as the biggest challenge facing our respondents in the next six months. The specific threats are yet to be fully realised, but the data suggests that organisations with strong internal skills and resources will be more resilient against them than those that have cut their people budgets in the last 12 months.

Skilled cyber experts are in short supply compared to the demand. However, by targeting their recruitment, developing and retaining their talent and outsourcing effectively, cyber security leaders can begin to reduce their skills gap as budgets recover during COVID-19.

Three actions to reduce the skills gap during COVID-19

1. **Target your recruitment:** review your business strategy and create a security roadmap to determine your specific security requirements.

2. **Develop and retain your talent:** invest in your people to develop the skills you need internally.

3. **Outsource effectively:** complement and strengthen your internal resources by outsourcing aspects of cyber resilience projects that would be impractical to recruit for internally.

Insight Space

cyber insights programme

nccgroup

Additional insights

Insight Space

cyber insights programme

nccgroup

Is there a cyber debt left by COVID-19?

Ade Clewlow, Senior Advisor at NCC Group

With rapid digital transformation, financial pressures, and a mass shift to remote working, many organisations have struggled to maintain their previous levels of cyber resilience over the last year.

This has built up a cyber debt that is affecting a wide range of businesses. To truly understand its scale and impact, we spoke to 290 cyber security decision makers from across public and private sector organisations about the challenges that they've faced this year.

We found that budget cuts have significantly affected cyber spend over the last 12 months. Three out of 10 businesses experienced delays or a cancellation of their cyber resilience projects, while one in five had to furlough staff responsible for cyber resilience programmes.

This reduction in resources has already had an impact on business resilience. Of those that reported cuts to budget, 70% also stated that they'd seen an increase in cyber attacks, while two-thirds of businesses reported internal skills shortages and an increase in insider-related incidents.

These issues have been exacerbated by changing working habits over the last 12 months. 21% of organisations expect staff to use more of their own devices while working in 2021, which makes effective security monitoring far more difficult. Meanwhile, digital transformation and cloud solutions are here to stay, which can contribute to a build-up of cyber debt.

To examine the scale of today's cyber debt, and how it can be paid off, we discussed the below topic on our latest Big Three webinar. I was joined by cyber experts Mark Ward, Global Chief Information Security Officer at Interserve IT, Katharina Sommer, Head of Public Affairs at NCC Group, and Tim Anderson, Group Commercial Director – managed detection and response at NCC Group.

QUANTIFYING CYBER DEBT

Quantifying cyber debt is extremely complex. With changing working habits, it's hard for organisations to understand what the future could look like – and therefore, how their level of cyber debt might change.

However, it's important for organisations to understand their current risk profile and adapt their operations where necessary. Threat actors are seeking to take advantage of security weaknesses, while business leaders' focuses are on other operational concerns – which introduces a new element to existing threats.

Understanding any current vulnerabilities and areas for improvement is the first step towards quantifying cyber debt. A Cyber Security Review is a useful way of benchmarking your sector peers, and provides clear actions that can help your business begin addressing this cyber debt.

RESPONSIBILITY FOR CYBER DEBT

Many security decision makers are already aware of the importance of increased security investment. Our research found that two-thirds of organisations plan to increase cyber security budgets this year, and that the amount spent on outsourcing security expertise will increase.

For many organisations, showing a return on investment on security efforts remains a challenge. 90% of respondents highlighted that they struggle to quantify the cost versus benefit of cyber security. For IT security leaders, articulating security risk in terms of business priorities is key.

It's also important for all employees to take ownership of the issue of cyber debt. This can be achieved by ensuring that all staff are aware of what they can do to maintain cyber resilience. A safety-first culture, an effective technology strategy, and investment in both internal and outsourced skills can all make a significant difference.

RESTRUCTURING CYBER DEBT

To begin paying down this cyber debt, organisations must first understand their own risk profile and strategic priorities.

Once businesses understand the level of risk they face – and the level of risk they are willing to accept – it's possible to build a list of priorities as part of a security improvement plan. This type of plan maps out the short, medium and long-term strategic measures that can significantly improve your security posture.

While organisations may not be debt free in a matter of months, now is the perfect time for business leaders to address the issues that have built up over the last year, and begin paying off their cyber debt.

To find out more about how your business can quantify and address cyber debt, you can watch the full webinar, 'The Big Three: Is there a cyber debt left by COVID-19?', on-demand here.

Insight Space

cyber insights programme

nccgroup

Case Study

Filling the skills gap in a large FTSE 100 company to manage a major cloud deployment

NCC Group was enlisted by a large hospitality organisation that manages a number of brands to provide assurance, expertise and guidance on a cloud migration.

Over the course of a 12 month engagement, NCC Group provided a spectrum of services including data loss prevention, vendor analysis and supply chain management, as well as managing a virtual CISO role. NCC Group ensured that the environment was secure and fit for purpose, and a relationship with the client is still ongoing.

AT A GLANCE

Organisation
FTSE 100 hospitality organisation

Industry
Hospitality

Challenge
Providing assistance and assurance for a cloud migration

Solution
NCC Group provided a full suite of solutions including a virtual CISO, vendor analysis and data protection

Results
NCC Group ensured that the cloud environment was secure and fit for purpose, freeing up valuable resources for the organisation.

SUMMARY

The client was a large FTSE 100 hospitality organisation that manages a number of brands under its umbrella. The company is customer driven, with a sharp focus on efficiency. It has 5,500 corporate users and an additional 32,000 retail outlets globally. The exercise consisted of a three month engagement in which a total of four NCC Group experts acted as virtual CISOs for the organisation. This was extended to 12 months due to additional scope.

CHALLENGE

The client was midway through its journey to full Office 365 cloud migration when it realised it had insufficient resources on its team to manage the transition.

The client needed full assurance across the Microsoft Office 365 and Azure environments; its existing information security teams lacked confidence to sign off the programs of work due to their unfamiliarity with security tooling and how to integrate it into the existing security operations.

SOLUTION

A three month engagement quickly extended to 12 months, which involved Director-level support and a virtual CISO role managed by a total of four NCC Group experts. These four roles rotated throughout the year, enabling NCC Group to ensure that it always had the best people on the job, depending on the particular task. During the engagement NCC Group provided:

- Advice on fully built out cloud architecture
- Information security design and architecture across Microsoft Office 365 and Azure environments
- Policy and process development for Office 365 eDiscovery
- Vendor analysis and recommendations for endpoint – Windows Defender APT
- Privilege identity management – Azure identity protection and multifactor identification
- Data protection – scope included Microsoft Cloud Application Security (CAS)
- Data loss prevention – information rights management
- Message hygiene – the solution implemented moved from proof point to Office 365 Advanced Threat Protection (APT)
- Data lifecycle management and GDPR compliance, including architecture on a SharePoint based subject access request solution
- Supply chain management for online collaboration

RESULTS

The support provided by NCC Group ensured that the client's business criteria for managing the cloud were met, and that the environment is secure and fit for purpose.

The relationship with the client is ongoing, having evolved into strategic advisory services for Office 365 assessment and its integration into the existing security operations.

Insight Space

cyber insights programme

nccgroup

Annual threat monitor report

From the Research and Intelligence Fusion Team

FOX IT

part of nccgroup

2020 in review

Critical vulnerabilities caused global havoc during 2020. The most prominent was of course our organic society targeted by COVID-19, impacting everybody's lives in many different ways. Cyber security also had its share of major vulnerabilities affecting large numbers of people.

The year started with a vulnerability in Citrix systems commonly used for remote working. Shutting down those systems to prevent exploitation forced many people to commute to work instead of working from home, going so far as causing "Citrix traffic jams" in deeply digitised economies like the Netherlands. That scenario is almost unimaginable from the world's current locked down state a year later, where social distancing and remote working is a hard obligation instead of an optional perk.

Other high-profile vulnerabilities with significant worldwide impact followed throughout 2020, including RCE issues in F5 BIG-IP and MobileIron products and privilege escalation via Zerologon. We describe these and more in detail in this Threat Monitor, together with insightful analysis of timelines from publication and proof of concept to active exploitation in the wild.

The COVID-19 pandemic drove rapid adoption of remote working and a faster shift to cloud-based solutions. Threat actors were already aware of the benefits offered by cloud systems, such as the ease of blending in with legitimate activity described in our previous report and webinar on long-term covert operations performed by the Chimera APT targeting aviation and semiconductor sectors.

Additionally, Fox-IT's detection and response efforts discovered that overlooked Linux and Unix systems serve as avenues of attack which exploit the specific features for stealthy and persistent access.

Another trend that has persisted through 2020 and will likely continue further into the future is the explosive growth of ransomware. Its "business model" has proven extremely effective for cyber criminals, and is growing even more so as they adopt increasingly aggressive negotiation techniques. We discuss these alarming developments along with a blueprint of the modus operandi these extortionist groups follow.

Finally, as 2020 was drawing to its end, a massive but stealthy operation that had been ongoing most of the year exploded in a crescendo of investigations and incident response after the SolarWinds supply chain attack was discovered. This far reaching campaign will probably go down in history as one of the most notable cyber espionage operations to date, and will definitely continue to receive significant attention and deliver intriguing revelations well into 2021. Even though many organisations might not have been directly affected, this major incident is teaching everyone important lessons about the supply chain attack vector. Lessons that are becoming ever more relevant in our increasingly interconnected future.

ABOUT FOX-IT MDR™ SERVICES

Managed Detection and Response delivers 24/7 monitoring and detection from our European Security Operations Centre (SOC). MDR is a comprehensive approach that brings together insights, technology and employees within an integrated range of intelligence driven services with a strong focus on response.

Developed over the last two decades, its in-house solution CTM (Cyber Threat Management) platform builds on the expertise of cyber security experts. Tried and tested, it is based on a combination of extensive insight into current threats and innovative technology, supported by a global network of security experts.

Our alerts are not solely reliant on traditional signature based detection as we utilise our technical threat intelligence to produce detailed actionable insights. Expert investigation by our analyst team means that all alerts are triaged, while deep dive analysis of network packets and endpoint events is completed, removing false positives and escalating genuine threats.

Critical events monitor

The timeline highlights major incidents on the global threat landscape during 2020.

JANUARY

01 Travelex forced to take digital services offline after REvil breach.

14 Microsoft patches crypto vulnerability reported by NSA.

14 Evil Corp resumes ransomware activity after December '19 indictments.

19 Citrix releases fix for widely exploited CVE-2019-19781 in Citrix ADC and Gateway.

FEBRUARY

03 DoppelPaymer leaks victim data on darknet if ransom unpaid.

10 Chinese military personnel charged with hacking Equifax in 2017 by US Justice Department.

16 Iranian Fox Kitten group exploits VPN flaws worldwide during intrusions.

20 UK blames Russian GRU over 2019 Georgia defacements attacks.

MARCH

09 Compromised European power grid organization ENTSO-E restricted to office network.

13 Czech Republic hospital with COVID-19 testing laboratory hit forcing shutdown.

26 Navigator/FIN7 group delivers USB by post to install Griffon backdoor.

APRIL

13 EDP continues power supply services while conforming breach.

21 Researcher disclosed four IBM zero-days after refusal to patch.

22 Brute force attacks against RDP increased during COVID-19 lockdown.

23 BEC group schemes three UK private equity firms out of $1.3m.

MAY

01 MAZE group steals 11 million BCR credit cards in ransomware breach.

09 Disruption of systems at Iranian port linked to Israeli cyberattack.

19 EasyJet airline suffers breach exposing customer data.

28 NSA discloses critical Exim flaw exploited by Russian Sandworm group.

JUNE

09 Indian hack-for-hire group Dark Basin tied to BellTroX company.

19 Australia targeted in offensive campaign by alleged state actor.

23 Evil Corp group deploys new ransomware variant WastedLocker.

23 Team9/Bazar: new first stage malware used during Ryuk attacks.

The timeline highlights major incidents on the global threat landscape during 2020 (Cont).

JULY

15 Internal Twitter admin tool abused for cryptocurrency scam.

16 Iranian group Charming Kitten training videos exposes operations.

17 Emotet launches new mass spam campaign after five month hiatus.

30 EU imposes first ever sanctions against foreign cyber attackers.

AUGUST

06 Intel source code leaked under contested circumstances.

13 Russian APT28 Linux malware disclosed by NSA and FBI.

24 Norwegian parliamentary email accounts breached.

24 New Zealand stock exchange disrupted by DDOS extortionists.

SEPTEMBER

21 'DarkOverlord' hacker sentenced to five years in prison.

22 Windows XP and Windows server 2003 source code leaked.

24 Microsoft detects active attacks leveraging ZeroLogon vulnerability.

26 KuCoin cryptocurrency exchange hacked for $281 million.

OCTOBER

12 Microsoft orchestrates takedown of Trickbot botnet using court order.

19 US charges six Russian GRU members for Sandworm APT activity.

22 EU sanctions two Russian military officers over 2015 Bundestag hack.

29 FBI warns of imminent Ryuk ransomware threat against health care.

29 Prominent MAZE ransomware operation shuts down its operation.

NOVEMBER

13 COVID-19 vaccine researchers targeted by APT28, Lazarus and Cerium in worldwide campaigns.

20 Qakbot trojan partners with new Egregor ransomware service.

23 Mustang Panda APT impersonates Catholic news outlets to collect Vatican intel.

20 Europol and partners thwart €40 million credit card fraud scheme.

DECEMBER

13 New Turla 'Crutch' backdoor found on the internal network of an EU country's Ministry of Foreign Affairs.

09 EU medicines regulator EMA hacked, COVID-19 vaccine data stolen.

13 First report on SolarWinds Orion supply chain attack, access to FireEye red team attack tooling.

28 Finland parliament email breach, hackers access MPs' email accounts.

Network monitoring is a team sport, which is something not necessarily unknown. Yet it needed to be relearned this past year.

The sensors are hardware appliances processing customer traffic in their designated locations. Our SOC analysts triage and build cases on the detection rules crafted by the Fox-IT Security Research Team and others. Detecting incidents quickly makes the difference between a contained, closed case or a lingering client exposure.

The pandemic has tested this approach, forcing it to include more VPNs and teleconferencing connections than anyone bargained for and the inevitable waves of attempted attacks to boot. The cohesiveness of the team stayed undefeated in its relay race-type shifts covering 24 hours a day, 7 times a week, seeing dial-in times totalling over 80 hours per group call in some occasions. Fortunately, this situation could be addressed after a few weeks to retake the office grounds under strict conditions, again without causing any hiccups to the operational services.

Not only has the monitoring continued unabated, in fact it expanded. SIEM and endpoint monitoring solutions have been adopted and implemented to discover budding threats instantly and in more detail. Alongside our automated channels, this may also be done in manual threat hunting exercises that start from innocuous looking events, yet may turn out to be major issues and/or flaws.

Exemplary for such endeavours is when analysts decided to pick apart URL shortening service bit.ly amongst customer traffic. One GET request with minimal HTTP headers stood out as particularly obscure. Running it down led to the discovery of the “Powerup.ps1” file, which explores a target machine for privilege escalation opportunities. This was determined to be associated with the Powershell Empire post-exploitation framework. A likely exploit attempt constituted enough reason for the customer to wipe the host and for our hunt to continue chasing leads.

> During the first wave of COVID-19 infections in Europe, we observed adversarial scanning peaking against health care providers. Phishing attempts setting up medical information pages popped up. A particular message lure attempted to move bank customers to order anti-bacterial bank cards.
>
> On COVID-19

Automated backdoor deployment immediately after the compromise. The patching which is performed with some delay then becomes inconsequential. In the Citrix case, Fox-IT observed adversaries alter the configuration of flawed versions to maintain exclusive access.

On Novel Attack Techniques

Threats appear in different shapes and sizes. Frequently, they lapse for a while and seem to have disappeared, only to relaunch with campaigns of renewed maliciousness. Therefore, indexing them by their target allows for categorisations – increasing the understanding of a threat and its intentions and capabilities by whom or what it attacks. Such dynamics are chronicled in the Threat Monitor report, allowing for comparative trend analysis.

The questionable distinction of being the most targeted sector in 2020 has fallen to the public sector. Even though this sector only saw a small increase, it surpasses all others with an average of 26 incidents per public institution. This is in contrast to the overall organisational average of just short of 16 reported cases a year, which in itself is lower than the previous year averaging just over 20 cases. Much of this is explained by the strongly reduced number of cases within the consumer discretionary sector, which saw major upheaval in a few specific instances which have since stabilized. Overall, it's the five listed sectors below that are hit most incessantly **(Figure 1)**.

Attackers that know to switch up their way of working, increase their chances of success. Therefore, the frequency of various techniques encountered is registered to establish the distribution of attack types **(Figure 2)**.

If new vulnerabilities appear, we observe the rush to exploit those still exposed. Now that contest is not just between the adversary and its target anymore, but also among rival adversaries themselves.

The most impactful attacks can arise from a combination of known actions: an employee bringing in a coin-miner along with their online activity, external port scans followed by bruteforcing credentials, or known hacktools like Metasploit and Cobalt Strike attempting to chart a course to critical assets. Policy violations originating with user activity would fall to the 'other' category in the chart below, which shows a decline that may reflect the workforce often working remotely rather than more responsibly.

More alarming is the increasing malware deployment and lateral movement, often detected by webshell and malicious Powershell activity. The malware included spyware such as Agent Tesla, PremierOpinionD or backdoors as Lojack and Hiddapp RAT. Also DDOS bot scripts are triggered from within the network, establishing that the IOT botnet Mirai remains active. Lastly, a distinct decline for adware can be noted, which is due to the other increases in attack types combined with a lower risk classification.

Hunting often reveals the presence of outdated or insecure systems in the customer network. Typically, those findings originate from policy violations or Indicators of Compromise used for retroactive queries. Network monitoring needs to work in tandem with SIEM and Endpoint solutions to defeat encrypted traffic and enable early warning capabilities.

On Threat Hunting & Monitoring

FIGURE 1 Percentage of SOC incidents by sector

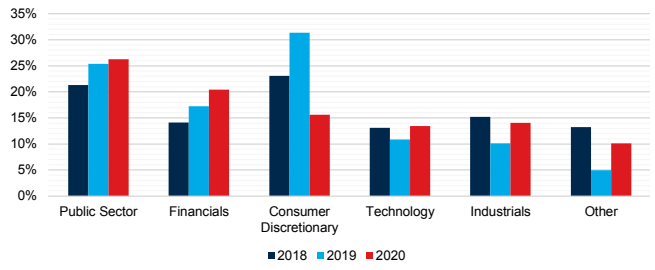
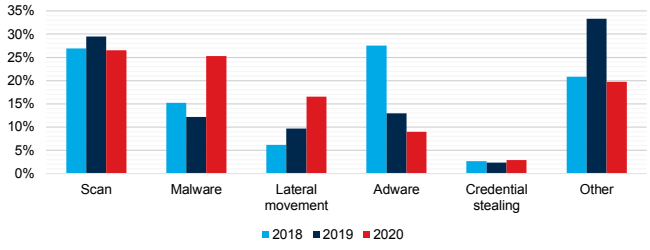


FIGURE 2 Distribution of attack types



FORENSICS & INCIDENT RESPONSE

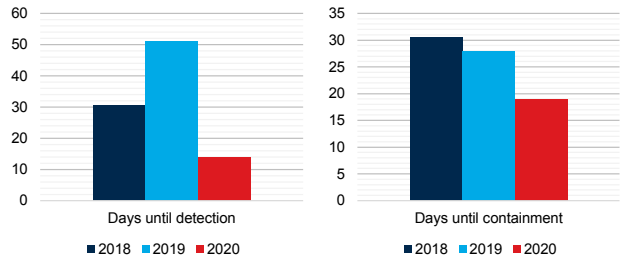
Where the SOC is much like the emergency call centre, the Fox-IT CERT operates more as an emergency service itself. The team is particularly focused on putting out digital wildfires and going on rescue missions under adverse conditions to save endangered systems and data. When incidents turn to crises and tempers flare, it becomes our job to save the organisation from itself at times. Putting the focus on the investigation scope, root cause and remediation options offers light at the end of the tunnel.

Yet this year, the additional burden of COVID-19 means supporting the victim remotely due to inescapable pandemic restrictions. Challenges in communication naturally occur when navigating this uncharted territory. Typically, finding a way forward is as straightforward as approaching a stakeholder at their desk and discussing the needs of the project. Now the path ahead proves more often to be a dead end or riddled with hurdles due to unresponsive staff members or misguided actions leading to more work to correct.

Starting points of forensic investigations need not always be cyber attacks. Consider, for instance, a hole in the wall the size of an average bicycle wheel. When break-ins happen, clearly visible damage to physical structures and missing valuable items raise immediate concerns as we've seen in two separate occasions over the past two years.

These clients, however, did not fail to realise that when access to networked systems - and the server room in particular - is gained by perpetrators, they may also invade the virtual domain of your organisation. Investigations of this type are straightforward. Upon determination of the timeframe in which the devices have been physically exposed, potential signs of misuse are collected and logs recording insertions of devices and log-on activity are examined. At both instances we were able to offer a silver lining and rule out further damage. In the case of the freshly 'air-gapped' office wall we were able to do so before the police or mason worker arrived.

FIGURE 3 Median time until detection & Median time until containment



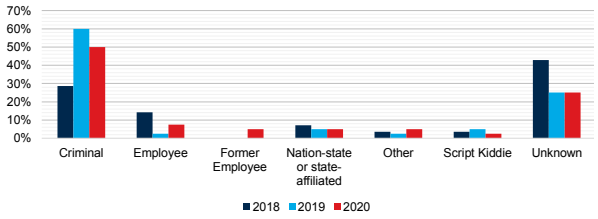
The trajectory to recovery starts when clients realise they have an incident on their hands, based on their own observations or with outside help. In 2020 this averages on two weeks,[1] which is significantly better than previous years where month(s) were the more appropriate length of measurement. Time to contain the intrusion is likewise trending downwards. The combination of knowing your infrastructure and us knowing what the attacker is likely after, wins the race. In multiple instances, the phone call summoning the team came only when suspected ransomware groups had already taken over their domain controller and were moments away from deploying the final payload.

The proliferation of ransomware is reflected in the degree of cybercrime cases we perform being one in two. As a rule, it is extremely difficult to undo the effects of the encryption. Yet in specific instances some sophisticated forms of data recovery - without involving backups - have proven feasible. Also business E-mail compromise is a continued favourite of the financially motivated hackers, particularly in combination with cloud services. In a substantial amount of cases the perpetrator remains unidentified due to priorities being placed elsewhere or traces not being recorded sufficiently.

[1] Calculation of the metrics for these diagrams is based on the median number of days, used as a measure that represents the distribution of the dataset most accurately.

Nation-states and their affiliates are often capable in covering their tracks, forcing a rather endless challenge of proving a negative onto the investigations following the Solarwinds backdoor, since what does having discovered the malicious software update without traces of a second-stage follow up mean? As new targets and techniques are still being uncovered among the security community, current outcomes leave some lingering doubts whether the absence of evidence is evidence of absence, or rather points to incomplete findings.
A firm recommendation in that regard is to enable logging on DNS resolvers - internally and extensively.

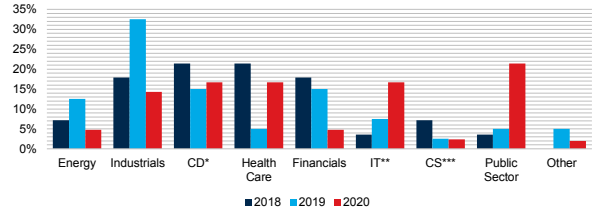
FIGURE 4 Attribution by adversary type



A more diffused picture than previous years emerges when looking at the target selection by sector. Consistent with the previously discussed SOC incidents the public sector is leading here, accounting for over 20% of cases. Remarkably, energy and financials dip under the five percentile range. Health care providers have been under incredible strain this past year, and unfortunately the security of their systems has been no exception to this. For this reason Fox-IT made custom insights on threat activity available to hospitals at an early stage last year, enabling improved detection and response.

In sum, health and endurance of both humans and computer systems have been thoroughly tested and damaged, and while neither will ever be without flaws, there are encouraging, vital signs pointing to growth and recovery.

FIGURE 5 Investigations by sector



SOLARWINDS: DATA EXFILTRATION AS STEALTHY AS THE INTRUSION IS WIDESPREAD

During the Solarwinds supply chain attack, the attacker came up with a new (and honestly quite impressive way) of exfiltrating data, leveraging cloud services that were already present in the target environment. The reason why this form of exfiltration is interesting to attackers and defenders alike, is because of its elegance and simplicity. Without needing to introduce custom or well-known red team tools that can achieve the same goal, the attacker confined their techniques to functionalities already present in the target network.

From what is known thus far, the attackers leverage a Windows client in their attacks. Some of the functionalities that are present in the on-premise Exchange environment like the 'New-MailboxExportRequest' and 'Get-MailboxExportRequest' are used to check the status of an ongoing export request command, and can also be leveraged to export contents of a primary mailbox or archive to a .pst file.

After a mailbox is exported, the attacker creates a password protected archive using 7-zip, and placed this archive on the OWA server that was present in the target environment. The attacker places the archive in a folder which was reachable externally. This way the attacker could retrieve the archive with a HTTP GET request.

Next to exporting the mailbox with the built-in functionalities of the on-premise Exchange server, the attacker leveraged another functionality, and this is where the Windows client becomes instrumental. Another command was used that enabled the attacker to synchronise the mailbox using the device ID of the Windows machine of the attacker using ActiveSync. This was done using the 'Set-CASMailbox' command.

Blue teams will have a very hard time in coming up with detection methods for every built-in functionality of a given service, potentially targeted by attackers for nefarious purposes.

Terms of use

Fox-IT tracks global cybercrime activity. We base our intelligence on tracking threat actors, darkweb research, forensic investigations, internationally deployed sensors and fraud monitoring services.

Going beyond botnet & malware information, we provide a global picture of trends, geographical activity, actors, their motivations and their evolving business models. We provide links to campaigns, tactics, procedures and individual IoCs to feed network security components. Customers become part of a global community, with live threat tracking, collaboration, and the largest criminal threat database, with over a decade of experience.

The data and charts contained within this report represents Fox-IT's own dataset collected within its malware lab. The data from this lab should be considered a sample including factors potentially skewing the analysis: our lab does not analyse every malware sample on the threat landscape, merely those assessed to represent a cross-section from a variety of sources. Our sources may be skewed towards certain types, families or regions which can introduce further bias. The report documents the dataset over a fixed period of time allowing for comparative analysis, whereas when referring to previous datasets a discrepancy with previous reports may seemingly occur due to inclusion of the updated dataset that may contain recent data impacting the statistical outcome.

Furthermore, the lists of data we use to identify targets for attacks can also be biased because they will naturally contain more data pertaining to Fox-IT customers than organisations not part of the MDR community. Although we augment customer supplied data (such as URLs for online banking and BINs) with autonomously collected data, the customer supplied data will always be more detailed and extensive. In short, these charts provide indications, and should be incorporated by interested parties as such. Customers are advised to incorporate and correlate multiple feeds with internal network telemetry.

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 14,000 customers 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 assess, develop and manage 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, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

To discuss how you can manage your people risk, speak to our team today.

+44 (0)161 209 5111

response@nccgroup.com

www.nccgroup.com