Security

SCC

secure

Managing the security impact of COVID-19

security.
managing the security impact of COVID-19.

COVID-19

Managing the security impact

For years the IT industry has talked about the 'new way of working' as organisations adopt the latest productivity tools. But few could predict how quickly the remote working revolution would take place, amid the COVID-19 coronavirus pandemic.

Amongst key challenges caused by COVID-19 are:

- **Enablement of home working for entire organisations**
- **The diversion of projects and priorities**
- **The need to maintain business-as-usual operations whilst protecting employees, partners and customers**

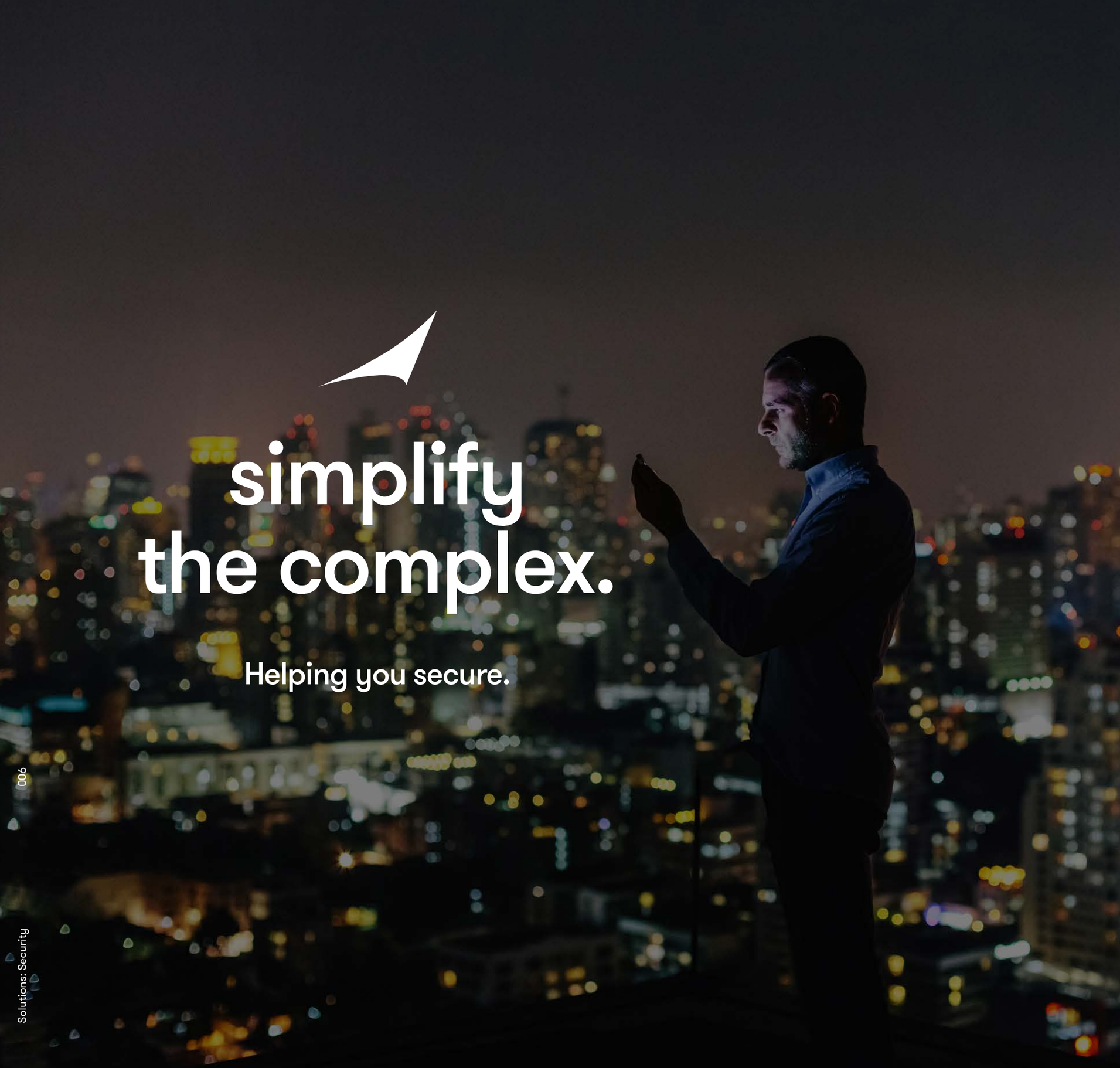
This is evident in the results of SCC's most recent IT Insights Report, a series commissioned by SCC to gain valuable insight into the UK IT market, in which we surveyed 550 IT decision-makers from 11 different sectors about the impact of COVID-19 on IT security. The number of decision-makers highlighting lack of staff training or awareness on IT security as the biggest security challenge increased by 36%, overtaking data security on personal devices.

These are unprecedented times, with the 'new normal' bringing endless challenges but also new opportunities to do things better, sooner. Some of these improvements will take place over time, as organisations play catch up with proper governance and adoption of new technologies, deployed quickly in response to COVID-19. Others are more urgent – in particular the protection of IT systems from would-be hackers who seek to take advantage of vulnerabilities caused by the pandemic with millions of new targets.

For every single homeworker, it is vital organisations provide education on how to remote work securely to protect their employees and the businesses against cyber threats. Similarly, organisations need robust security visibility – two things that few had time to implement at the beginning of COVID-19. IT teams have worked tirelessly under immense pressure to keep businesses protected in the short term, but now is the time to ensure long-term cyber and information security and enable your business to thrive again. The COVID-19 pandemic has triggered a rethinking of investment priorities for organisations around the globe, forcing IT decision-makers to make critical decisions about whether to reallocate funds from longstanding IT security projects. This shift in focus is reflected in SCC's IT Insights Report, with end user device security (78% increase), identity and access management (16% increase) and cyber security (9% increase) all becoming higher priorities in the IT budget post-COVID-19.

SCC has led the charge on cyber security for years, with a detailed understanding of how to significantly increase security around people, processes and technologies, whether office-based or working remotely. Our solutions help businesses identify security gaps, develop appropriate safeguards to limit or contain the impact of a breach, and proactively manage on-going risk to keep you protected.

These are the basics of IT security and secure remote working but now more than ever it's critical to prioritise what you must do to stay secure during the COVID-19 outbreak and beyond.



Managing the security impact

It is also clear IT decision makers expect the business effects of COVID-19 be felt for years to come, where there has been a shift in perception of the biggest security threats they are now most concerned about, with ransomware (up 32%), resource theft (up 52%) and dependency on cloud services (up 24%) expected to be larger IT security threats in five years' time, as cyber criminals look to capitalise on the rapid pace at which businesses had to adapt to a fast-evolving landscape brought about by COVID-19.

The scale of the IT security challenges ahead is emphasised in a new Gartner report, '7 Security Areas to Focus on During COVID-19', exploring key IT security threats, including incident response plans and protocols that might become obsolete or need to be adjusted, given that most of the security and risk team is now operating in completely different environments and mind sets. This is particularly pertinent as SCC's IT Insights Report reveals 22% of organisations do not currently have an incident response IT security function, whilst 9% of these are now considering a future provision by outsourcing – almost double the number that said the same thing before COVID-19.

Gartner also suggest businesses reinforce the need for remote workers to remain vigilant to socially engineered attacks, warning of the potential dangers of employees having more distractions than usual, whether it's having kids at home, worrying about family or concerns about their own health. Simply operating in a different environment might make employers less vigilant about IT security at a time when cybercriminals are proactively seeking to exploit such vulnerabilities, supporting SCC's findings of a growing concern around lack of staff training or awareness as a key IT security threat.

Gartner discusses the importance of testing and security patches, expanded security monitoring, evaluation of impacts to the security supply chain with security service vendors, accounting for cyber security systems, and continued compliance with information and privacy laws, as more information is collected relating directly to the COVID-19 pandemic. All told, it is no easy task for IT departments to ensure security remains robust whilst coping with the repercussions of a major global event, the likes of which we may never see again. But one thing is for certain: the new way of working has well and truly arrived and with great opportunity comes great risk, particularly in the case of IT security.

Current state of play

What IT decision makers are saying

Threats

It's interesting that, post-COVID-19, 12% of IT decision-makers now say skills gaps of IT security staff is the biggest challenge, with entire workforces having to work remotely, increasing vulnerability. At the start of the year, internal staff were considered more of a threat to cyber security (40%) than external threats (29%), whilst the biggest single threat was hackers, at 27%.

Demonstrating the importance of IT security, 87% of IT decision-makers said their organisation's leadership team is committed to the adoption of security across the IT estate. It's heartening that this remained the same post-COVID-19, despite the necessity to enable widespread homeworking for, in many cases, thousands of people at short notice. One way of making this task easier would be to remove security controls, but with 87% still reporting board level commitment to IT security, it's clear that the majority of businesses understand the on-going, increasing requirement for robust IT security.

Focus

IT security has topped the agenda of IT departments for a number of years, with information security now as important as any other business function. The volume, regularity and sophistication of cyber-attacks is increasing at the same rapid pace that technologies advance. For every new technology there is a renewed risk and security is often the number one concern and barrier to organisations adopting the latest IT services and solutions.

It's often said that the biggest risk to any organisation's IT security is its people, with human error, lack of training or not enough awareness of the latest techniques used by cyber criminals leaving all businesses exposed to the possibility of a breach. SCC's IT Insights report for IT security confirms this, with skills gaps of IT security staff the biggest IT security challenge according to 8% of decision-makers ahead of the COVID-19 pandemic. Security of enterprise data on employees' personal devices was the largest risk reported, at 12%, meaning net 20% of respondents highlighted people or personal devices as the most significant risk to IT security.

Priorities

In terms of priorities, 20% of IT security budgets were spent on cyber security before COVID-19. 17% of budget went on cloud security. End user device security appeared to be the lowest priority, with just 3% of the IT security budget allocation. This has grown significantly since the pandemic, now at 7%, highlighting a shift in focus to the end user as businesses look to make working easier but still secure.

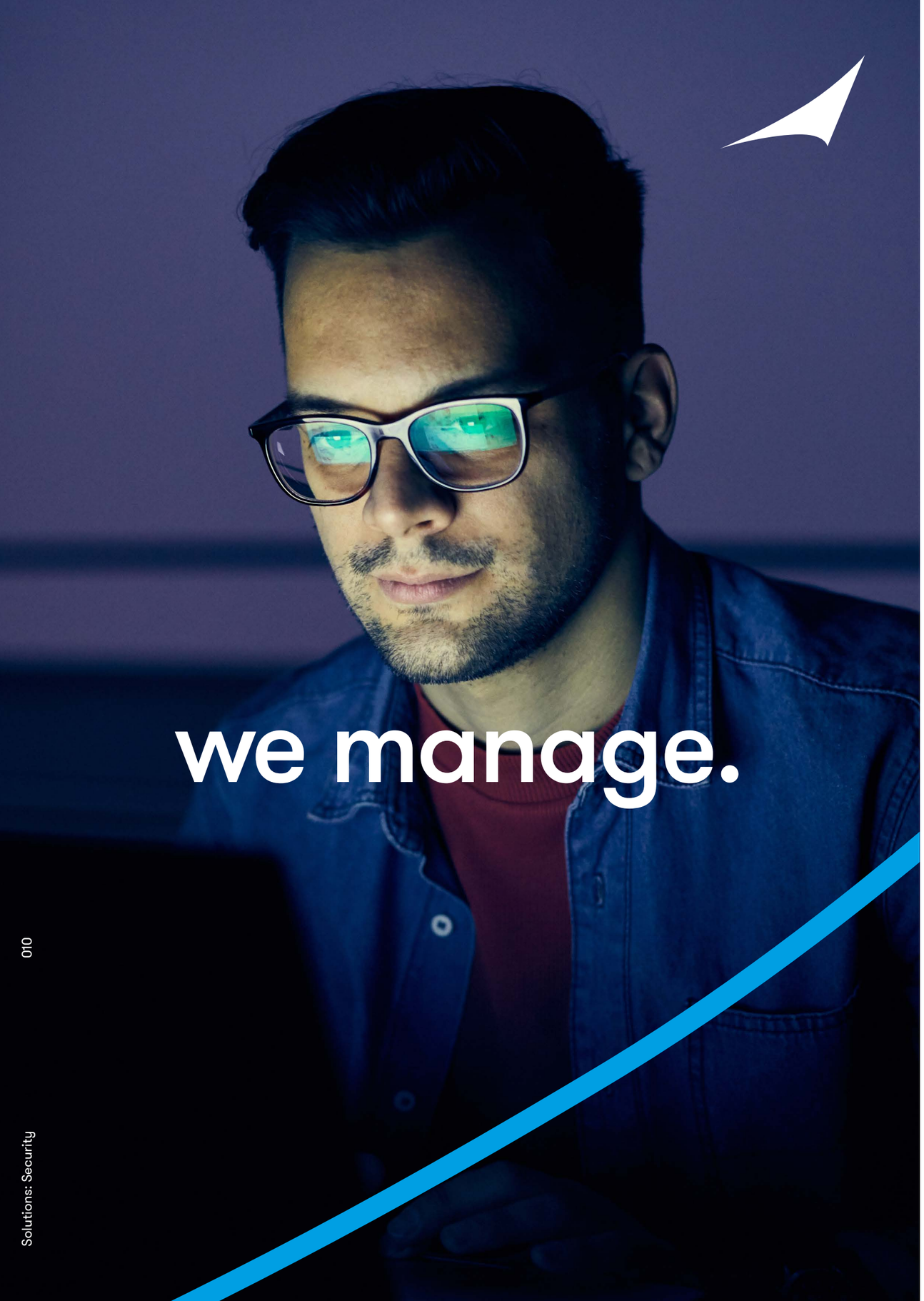
Before the pandemic hit, we asked which IT security functions were delivered in-house, outsourced or not currently provided, and whether there were plans to provision each of the functions in the future. Our insights reveal the majority of IT security functions are delivered in-house, but cloud security is more frequently outsourced. We would expect an increase in outsourced IT security functions post-COVID-19, as businesses look to experienced partners to cope with the enhanced threat.

Risks and Impact

We also asked for predictions about what IT decision-makers believed would be the main IT security risk in five years' time. Before the pandemic, the biggest forecast threats were dependence on 5G services (24%), dependence on cloud services (16%) and human factors (16%). The lowest forecast threats were both resource theft, ransomware (10%) crypto mining (7%). Asked the same question during the COVID-19 pandemic, there was significant shift in future IT security concerns, with resource theft increasing in ransomware, up to 13% and crypto mining, to 11%.

Dependency on cloud services, a main threat before COVID-19, was seen as an even bigger threat, up to 21%, further indicating that one of the outcomes of the pandemic will be a greater focus and priority on end user services. As businesses look to improve ease of access by delivering cloud services across the board, new security concerns arise around theft or malware.

Security of your people, processes and technologies should be high priority. The economy is currently under extreme pressure and any security breaches may now have an even bigger impact than pre-COVID-19, economically and reputationally.



COVID-19 impact on in-house and outsourced services

Pre-COVID in-house and outsourced mix

Firewall Management
In-house 46.1%
Outsourced 32.5%
Hybrid 21.4%

SIEM
In-house 48.7%
Outsourced 28.6%
Hybrid 22.7%

Incident Response
In-house 45.5%
Outsourced 29.9%
Hybrid 24.6%

Threat Intelligence & Management
In-house 44.2%
Outsourced 29.2%
Hybrid 26.6%

Cloud Security
In-house 39%
Outsourced 40.3%
Hybrid 20.7%

Privileged Account Management
In-house 46.8%
Outsourced 27.9%
Hybrid 25.3%

Governance, Risk & Compliance
In-house 42.9%
Outsourced 31.8%
Hybrid 25.3%

Email Security Management
In-house 50%
Outsourced 28.6%
Hybrid 21.4%

DDoS Management
In-house 37%
Outsourced 36.4%
Hybrid 26.6%

Businesses will need to be even more cyber resilient with focus on security features, capabilities and service rollouts that are critical to their operations. It has become paramount to create and test incident response, business continuity, disaster recovery, talent succession and also vendor succession. Essential to the rising COVID-19 security threats to an organisation's infrastructure is the monitoring of user activity to detect incidents before they result in operational risk.

A balanced approach to your in-house and outsourced mix across your organisation's IT estate will need to be revised to accommodate more effective risk trade-offs in light of the pandemic.

Our approach

SCC's Security Approach begins with an effective security program to understand the maturity of your organisation through to implementation of the right tools and security controls for provision of continuous monitoring and incident response. Our aim is to mitigate legal, financial and reputational risk.

Gartner's recent publication, '7 Security Areas to Focus on During COVID-19', discusses the principal concerns for IT security teams looking to ensure their organisation doesn't fall foul of increased cyber-attacks as a direct result of the pandemic, as we all get used to working in completely different environments and would-be cyber criminals look to capitalise on the new way of working.

Gartner: 7 security areas to focus on during COVID-19

- Reinforce the need for remote workers to remain vigilant to socially engineered attacks.
- Ensure that the organisation's incident response protocols reflect the altered operating conditions and are tested early.
- Ensure security monitoring capabilities are tuned to have visibility of the expanded operating environment.
- Ensure that all remote access capabilities are tested and secure and endpoints used by workers are patched.
- Engage with security services vendors to evaluate impacts to the security supply chain.
- Don't forget employee information and privacy.
- Account for cyber physical systems security challenges.

SCC Security approach

DISCOVER	DESIGN	SUPPLY	IMPLEMENT	MANAGE	OPTIMISE
• Cyber Risk Assessment • Cloud Security Assessment • Compliance Services • Vulnerability Assessment • Penetration Testing • Active Phishing Simulation Service • Information Security Awareness Training	• Security Solution Design • Security Standards and Guidelines • Technical Assurance • Security Policies Formulation	• Next Generation Firewalls • Network Access Controls • Identity and Access Management • Multi-Factor Authentication • Privileged Access Management (PAM) • Cloud Security • Application Security • Mobile Device Management • Anti Malware • Anti Ransomware • Anti Virus		• Managed SIEM Service • Firewall Management • Threat Intelligence • EndPoint Management • Active Directory Management • Secure Data Protection • Cloud+ Secure • Cloud Hosting	• Continuous Service Improvement • Security Hardening • Customer Success Program

CUSTOMER CHALLENGES

Our approach

Our security solutions fit within your business strategies and are designed to help you improve and strengthen your security posture across your entire organisation – ideal for responding to unforeseen incidents such as the COVID-19 pandemic

SCC has seen a significant increase in attempted resource theft, such as malware and ransomware, in UK markets since the beginning of the COVID-19 pandemic.

Our approach to IT security is designed to protect organisations across all areas and the whole information and cyber security lifecyle, by understanding both specific threat levels and our customer's current maturity before building solutions to match requirements, suitable now and into the future. Our approach is relevant pre- and post-COVID-19, with IT security crucial to all organisations and the coronavirus situation helping many to see threats that have always existed but have not always been a priority.

For example, with businesses across the globe expanding remote working and VPN access as a result of COVID-19, the requirement for multi-factor authentication has been brought into sharper focus, and barriers to adoption of the most basic security protocols have been removed. There is also a much louder conversation about IT security culture and learning within organisations, with the social element of the office space lost to homeworking and IT security teams relying on individuals to stay alert and act as the first line of defence against malicious cyber-attacks.

SCC's approach is to work in partnership with our customers to identify their threat level and walk them all the way through the journey, from start to end, with an understanding that IT security is an on-going, ever evolving journey. To SCC, COVID-19 is merely the latest significant event that has changed the current threat landscape for all businesses. Next year, there will be a new threat and once again organisations will need to adapt in order to remain secure.

A typical approach might be to take an off-the-shelf SIEM solution as part of an existing enterprise agreement. The reality is that no real value can be derived from a platform not integrated as part of the wider business or IT security strategy and allocated to an existing resource with no capacity to manage the solution appropriately. This is why SCC looks at the whole lifecycle and works to ensure full effectiveness across the organisation.

Our IT security solutions fit within business strategies, often opening up new opportunities for better ways of working, quickly and at scale – ideal for responding to unforeseen incidents such as the COVID-19 pandemic.

We help organisations take a proactive approach to managing risk and automating key processes to keep their business protected. Never reactive our solutions match each of the seven security focus areas during COVID-19 and beyond as identified by Gartner.

#StrongerTogether

How we're helping our customers through this crisis.

SCC helps NHS Foundation Trust focus on front line services

SCC continued to support a NHS Foundation Trust throughout the coronavirus crisis, enabling the continuation of operations for cancer patients. The Trust had an urgent requirement to immediately mobilise 600 priority NHS staff to work at home, with a total user base of 12,000 users.

The Trust were looking for implementation of a Fortinet firewall solution, to support their existing Cisco environment. SCC delivered within five days and provided subsequent further firewalls for another site along with additional tokens, management devices and engineering support, as we continue to support the NHS focus on delivering front line services at a difficult and challenging time.

The customer's Head of IT Infrastructure said: "Your help is directly enabling us to avoid cancelling operations for cancer patients, so I can't adequately put into words how great your help has been."

SCC delivers in record time for NHS Trust

SCC helped a NHS Trust accelerate an 'always-on' VPN project that had been running internally for 12 weeks. Faced with the difficult challenge of enabling remote working and collaboration for its staff and Trust Board in a short space of time, amid the on-going COVID-19 response measures in the UK, SCC got the project up-and-running within four days.

Within two days, we also enabled videoconferencing services, ensuring the Trust Board could meet virtually, saving over 650 miles of rural commute in addition to enabling business continuity.

SCC ensures business continuity and safety

A retail centre management company is benefitting from business continuity and employee safety throughout the COVID-19 crisis, thanks in part to SCC's home working solution.

SCC has delivered a secure VPN solution, as well as video and audio conferencing via WebEx and Jabber soft clients, to ensure employees can communicate from different locations and make use of their reception consoles and contact centre technology. Without this, the customer wouldn't have been able to carry out critical business activity during this unprecedented time.

How we're helping our customers through this crisis.

We deliver proactive security monitoring as cyber security threat rises

A major UK-based holdings company for leading insurance brands has a small IT team responsible for securing around 800 devices, generating thousands of logs and alerts every day. Targeted by up to 1,000 cyber-attacks each day, the company faces significant risk of financial and reputational damage in the event of a breach.

In partnership with SCC, the company use our SIEM service to get a real-time overview of network and security events and maintain a proactive approach to cyber security. The managed service ensures SCC is automatically alerted to significant incidents, giving its customer early warning of potential threats. Each potential incident is reviewed by security analysts and appropriate actions raised to SCC and customer, ensuring the business remains safe without carrying the burden.

The SCC service has been deployed across a hybrid environment that includes hosted private cloud infrastructure, on-premise systems and software-as-a-service systems, generating up to 1,000 system events per second and 10,000 network flows per minute. That includes user behaviour monitoring of around 500 individual accounts, monitoring Microsoft Server, Active Directory, Symantec End Point Security, Mimecast Mail Filtering and Cisco, with expansion into O365 and wireless networks underway. Customer Intelligence is provided through summary reports and dashboards, enabling a real-time view of the landscape.

We help leading university develop IT security strategy

SCC has partnered with one of the UK's leading universities on a number of initiatives to help them understand where they are in terms of their IT infrastructure and develop solutions and strategies to help them deliver academic excellence to their student population and improve their staff efficiency and wellbeing. The university, one of the largest in the UK, with a student population in the tens of thousands, prides itself on being a global institution, recruiting students from all over the world, with international students from China and Malaysia making up a quarter of its total student base of 47,000.

The university looked to Cyber Essentials Plus as a mechanism to satisfy the requirement to retain key industry tie-ups and funding. SCC worked closely with the university to understand the requirements of Cyber Essentials and provided a range of consultancy to review and assess the current position. We then made a number of suggestions as to how the university could come in line with the requirements, including additional security in the university's Office 365, environment together with network segmentation.

Helping County Council build roadmap to improve security

SCC supported a County Council by providing a Security and Threat Assessment (SATA) to help them define their current risk profile against cyber threats and deliver a roadmap of recommendations, including process and technology requirements to identify gaps in the infrastructure. The council was undergoing a review of its people, process and technology security requirements to ensure its needs continue to be met as the context in which it operates evolves, from a security and threat standpoint.

SCC carried out the SATA as an initial step to help the council baseline its current position, associated internal and external threat profile, and recommendations to appropriately mitigate risks surrounding cyber security. It's wide approach to security, covering not only the technical controls but the management of security from IT through to the board, gave the council a clear view of its current state, and the tools needed to build a new capability.

SATA is a standardised but flexible security assessment rooted in the NIST Cyber Security Framework, with mappings through to ISO27001, the Cloud Security Alliance framework, Cyber Essentials and other compliance frameworks. It enabled the council to appraise and review its security capability, footprint and level of maturity across the enterprise.

Output from the assessment is aligned to both management and technical audiences. It provides strategic advice to enable management to address the council's priorities in the context of evolving security threats alongside detailed analysis to enable technical staff to understand the detailed operational and technical risks. SCC is now working closely with the council to discuss elements of the report to address security requirements.

why choose us?

Supporting you in protecting against cyberattacks during and post COVID-19

Our security solutions help businesses identify security gaps, develop appropriate safeguards, and proactively manage on-going risk to keep you and your brand protected.

We work collaboratively, getting to know your people and processes to build a complete picture of requirements. Our experienced team of security experts work with you to meet your requirements, from cloud to managed security. And we continually invest in our capabilities.

Our international reach and strong global partnerships keep us relevant and allow us to take a vendor independent approach to your security requirements, acting as a thought leader to work in partnership with your business to deliver the best outcome against available resource and budget. Contact us and see how we have helped organisations in your sector deliver robust IT security. For every proposed product design, we map out and provide immediate feedback.

Find out more

Hopefully this guide has given you a flavour of what we have to offer. Why not get to know us a little better?

Connect with us.

linkedin.com/company/scc

twitter.com/scc_uk

instagram.com/scc_uk

facebook.com/specialistcomputercentres

vimeo.com/sccuk

Email: online@scc.com
Visit: scc.com

Email us

If you would like to book an appointment to discuss any requirements please email: online@scc.com

Talk to us

If you have any queries about our services, would like to speak to someone in more detail, or simply want to book a meeting, you can always speak with us directly via your normal point of contact or call the SCC Main Reception on: 0121 766 7000

Go online

Check out our website for full and up-to-date information about all our services. scc.com

SCC
James House, Warwick Road
Birmingham. B11 2LE

online@scc.com
scc.com