Six Degrees

PLANNING FOR THE FUTURE OF CYBER SECURITY TODAY

How remote working changed the cyber landscape, and how to respond.

Beyond Cloud.

Planning For the Future of Cyber Security Today

How remote working changed the cyber landscape, and how to respond.

It would be an understatement to call the past year disruptive. Fundamental shifts in how we communicate, collaborate and share information have changed how we work. Cyber security will need to undergo a transformation in order to keep information safe while enabling the flexible and remote access required to succeed.

The term new normal has been bandied about with such regularity that it can seem cliche. But the importance of getting this transition right should not be understated. Businesses are establishing new methods of working now that will become entrenched norms. Cyber security is a critical component of making these changes without creating unacceptable risk. Getting ahead of the curve will deliver a competitive advantage while ensuring secure outcomes.

Planning long-term

Change is an opportunity. Accommodating remote workflows and collaboration has been a long-established challenge in cyber security. Although new developments have accelerated the need to find answers, it does not change the potential long-term benefit of making the right investments today.

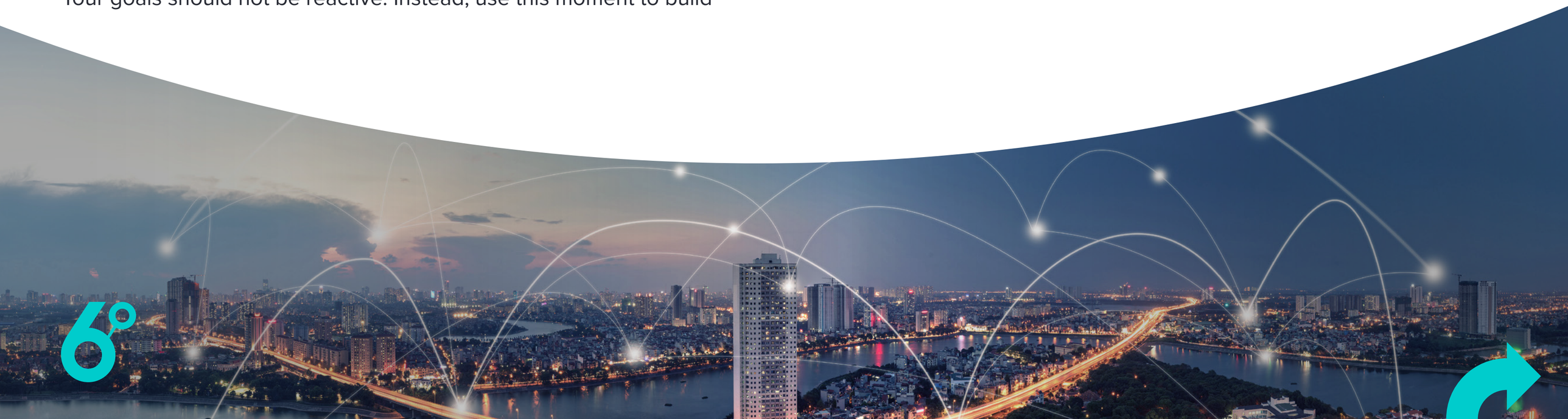
Effective cyber security is a gateway to commercial opportunities. Your ability to safely and flexibly engage with remote workflows is a prime example of how cyber enables business growth and success. Thinking about these outcomes is important when making any investment and communicating the value of cyber security within your organisation. Creating efficient systems and finding the right partners will help you deliver the security you need while still being able to focus on your actual business – which likely isn't cyber security.

Planning for the 'new normal' requires looking far beyond next year. Your goals should not be reactive. Instead, use this moment to build sustainable and flexible foundations able to adapt within an uncertain future. Remember, cyber security is not a destination, it's a process. By understanding your cyber journey you can build capacity for change into the heart of your security programme, do more with less, and keep your systems secure.

What this report will deliver

At Six Degrees, we provide a full range of managed cyber security services to some of the largest brands in the UK. Combining first-hand research and collated industry insights, this report will provide a snapshot of key trends impacting cyber security and the risk landscape. We will then use those insights to identify sustainable and long-term answers to pressing cyber security questions.

In order to support your business in the new economy, it's important to look at what's changed and what stayed the same. This report is about helping you do just that.



Cyber security and the risk landscape

In the run-up to 2020, we saw record breaking figures. The total financial cost of cybercrime in 2019 was more than $1 trillion. As of 2018, 1.2 billion people had been a victim of cybercrime. The critical importance of cyber security has not changed. But the risk vectors and methods of attack continue to evolve. We need to look at both in order to create an effective long-term strategy.

Changes to the workplace

Major changes to the workplace centre around remote access. To accommodate remote workers, businesses have needed to move new types of data online, rely more heavily on the cloud for business-critical applications, and provide flexible access to unsecure networks and devices.

1. **Remote working** – There are more people engaged in remote and flexible working than ever before.

47% of the UK workforce now works from home.

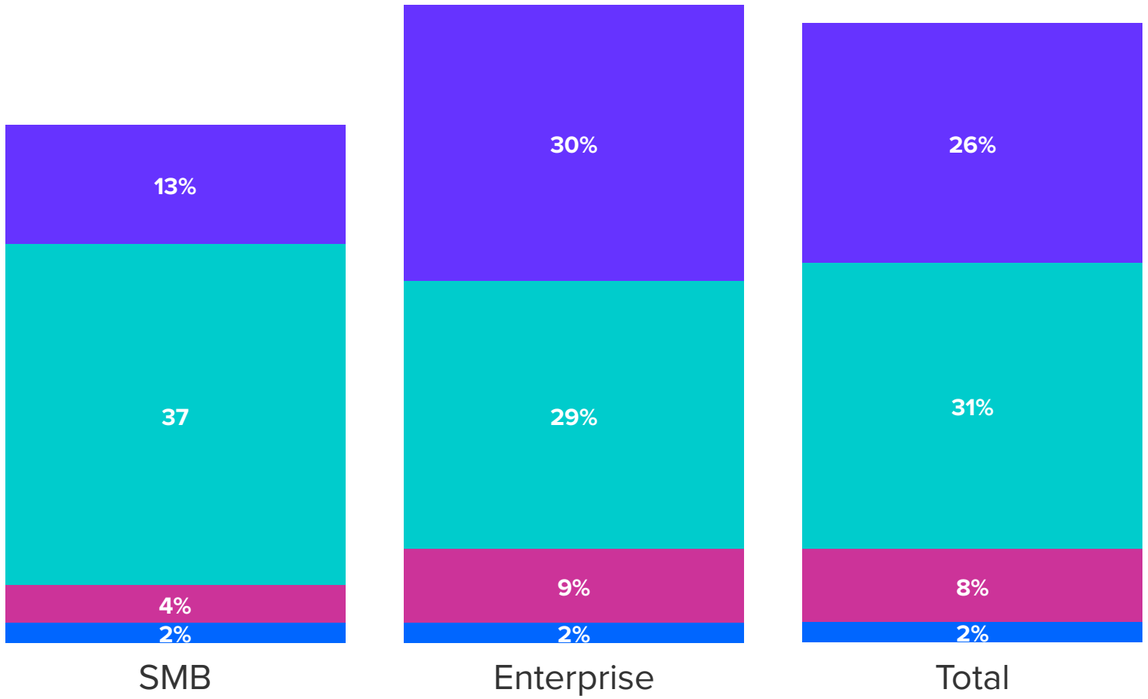
88% of people who worked remotely during lockdown would like to continue to do so.

86% of remote workers cite COVID-19 as the specific cause for changes to work habits.

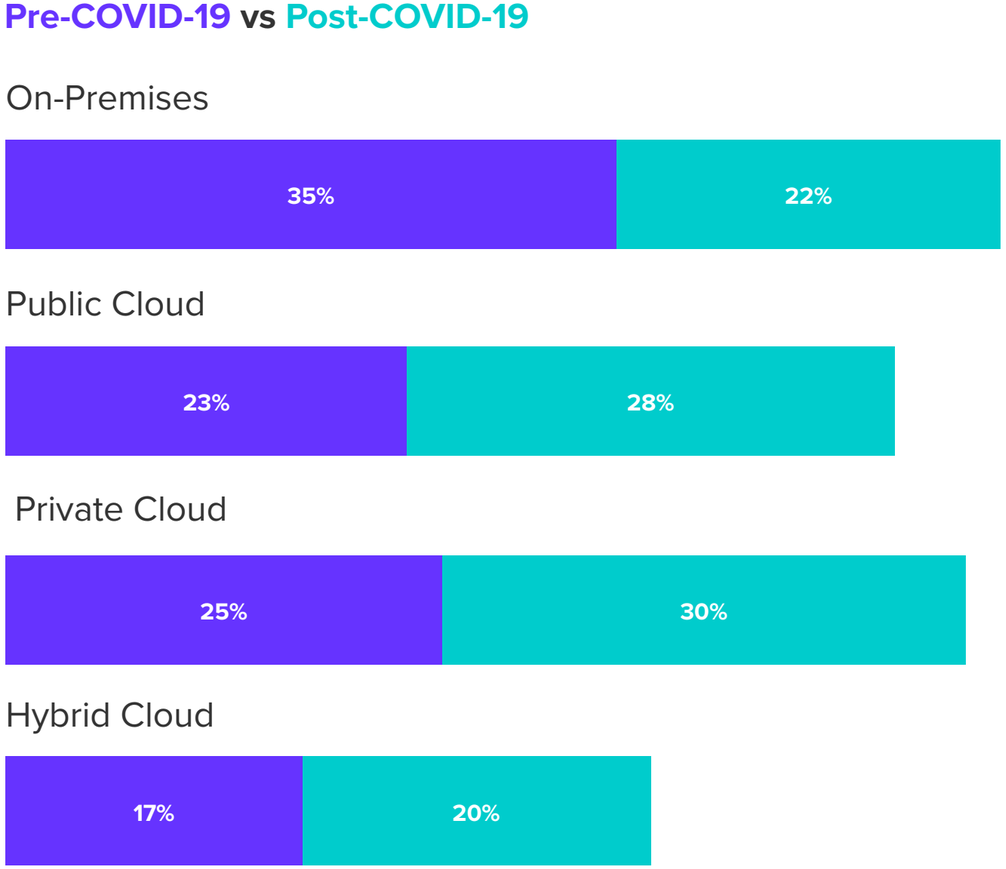
These numbers are likely to decrease long-term. However, public pressure to maintain flexible working will likely lead to a long-term change.

2. Accelerated adoption of the cloud – The cloud made remote working in response to COVID possible, and 87% of global IT decision-makers agree that 2020 has pushed organisations to accelerate cloud migrations. As you can see, not only has cloud usage increased, expectations that future workloads will move online has also increased.

Changed from planned cloud usage due to COVID-19



Projected shifts in workloads by 2025 before and after COVID-19



Gartner projects that technology spending will come under pressure. However, the public cloud service market is forecast to grow 6.3% in 2020 to total $257.9 billion, up from $242.7 billion in 2019.

Note: Desktop as a service (DaaS) is expected to have the most significant growth in 2020, increasing 95.4% to $1.2 billion. DaaS delivers access to virtual applications and desktop services through the cloud, and has been an essential part of supporting the surge in remote workers needing to access enterprise applications from multiple devices and locations securely.

3. More critical applications running online – Organisations have embraced the use of public clouds for new types of data. More than half of cloud decision-makers are moving sensitive corporate financial data or consumer data to the cloud. This creates security concerns and needs to be taken seriously.

Type of data that will move to cloud	Corporate financial data	Consumer data (PII/PHI)	Order/Sales data	IoT/Edge data	Non-sensitive data for analysis	Other non-sensitive data
All stays on-premises	21%	19%	12%	6%	5%	5%
Mostly stays on-premises	25%	18%	16%	13%	10%	11%
Mix of on-premises and in-cloud/SaaS	24%	30%	27%	20%	22%	22%
Mostly will move to cloud/SaaS	11%	13%	17%	20%	23%	21%
All will move to cloud/SaaS	15%	17%	23%	24%	37%	35%

Changes to the risk landscape

Credential theft, errors and social attacks are the three most common causes of security breaches. Employees working from home can be particularly vulnerable to these attacks. In these uncertain times, it makes sense to focus prevention efforts here.

There have also been changes to attack volumes and the types of attacks since the start of COVID. For example:

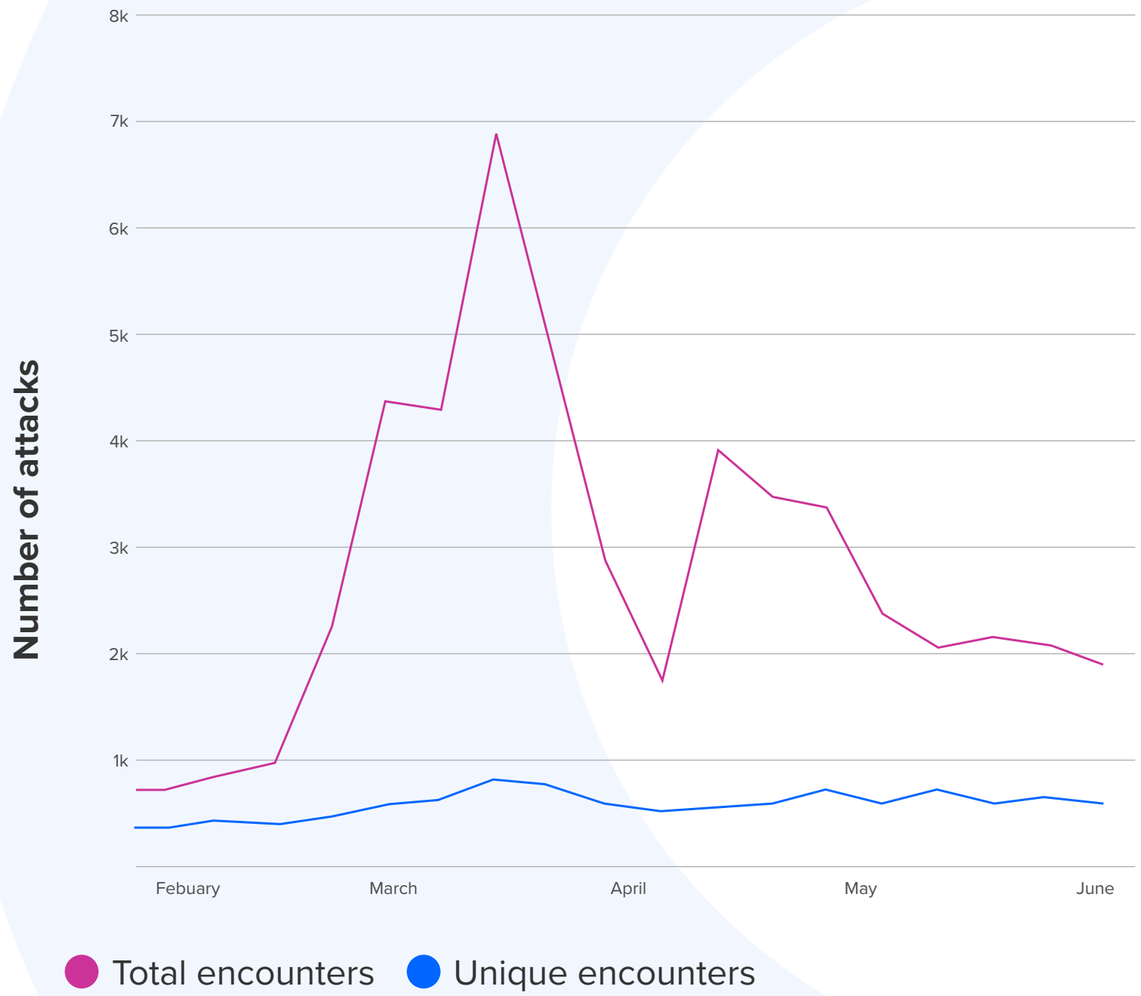
- **Nine out of 10 coronavirus domains are scams.**
- **Half a million Zoom accounts are currently for sale on the Dark Web.**

COVID-related attacks are here to stay, but subsiding

Research by Microsoft reveals a dramatic increase in COVID-themed attacks spiking with lockdowns in March. Although they persisted throughout 2020, the numbers have never reached the levels seen early on. It's also interesting to note that the number of unique malware threats is far lower than the total number of encounters.

Spear phishing attacks three times more likely since COVID

A variety of phishing campaigns are taking advantage of the heightened focus on COVID to distribute malware, steal credentials, and scam users out of money. Scamming and brand impersonations account for 88% of these phishing attacks. Particularly since mid-July 2020, there has been a sudden increase in Emotet phishing attacks on UK and US organisations.



Sectors targeted by ransomware, April to June 2020

Malware on the increase

A range of common malware is being distributed through coronavirus-related phishing, especially modular variants.

COVID has driven a 72% to 105% ransomware spike

Ransomware samples (captured malicious files and code) have grown 72% since the beginning of the pandemic.

Our own research indicates that retail and manufacturing have been significant targets for these ransomware attacks.

However, threats are rising across the board. For example, there was a 187% increase in cyber incidents reported by UK financial services in 2020 compared to 2019.

New types of cybercriminals

Cybercrime is increasing in sophistication and becoming easier to execute, with malware as a service available on the Dark Web enabling novice attackers to carry out sophisticated attacks. But where are attacks coming from?

- **1%** featured multiple parties
- **1%** involved partner actors
- **Only 4%** of breaches required the attacker to take more than four actions
- **55%** of attacks were carried out by organised crime
- **70%** of breaches are executed by external actors
- **Only 30%** involved internal actors

Vulnerabilities and myths

Don’t blame human error too much

The classic stat is that about 90% of data breaches are caused by human error. Thinking about process, training and review are all critical components of an effective cyber security programme. However, you have to take a pretty broad definition of human error to hit that 90% figure. It’s important to think about the technical aspects of your security system as well – firewalls, monitoring, antivirus, etc.

This year’s Verizon’s DBIR reported that DoS attacks (hacking) were responsible for over 50% of breaches. The report also notes a high number of internal-error-related violations (881, versus last year’s 424). However, they point out that this is at least partially due to improved reporting.

On the outside looking in

It’s important to note that 70% of breaches in 2020 were caused by external parties. This highlights the importance of taking endpoint and network security seriously. Process and internal protections won’t stop a DoS attack as it occurs, or help you recover after the fact.

Money is the root of most breaches

Espionage makes headlines but accounts for only 10% of breaches. The majority of breaches (86%) continue to be financially motivated.

It’s important to stay vigilant

Increased data exposure to new devices and distributed user groups requires constant attention. The best security systems continually update to manage change and support internal flexibility without hindering commercial growth.

It’s critical to move beyond traditional and static perimeter defence security models to find more agile methods of protection. But the more flexibility you build into your defence, the more important it becomes to monitor and engage in active security measures. Done effectively, this will actually create a more efficient system, but it requires planning to get right.

How is the industry responding?

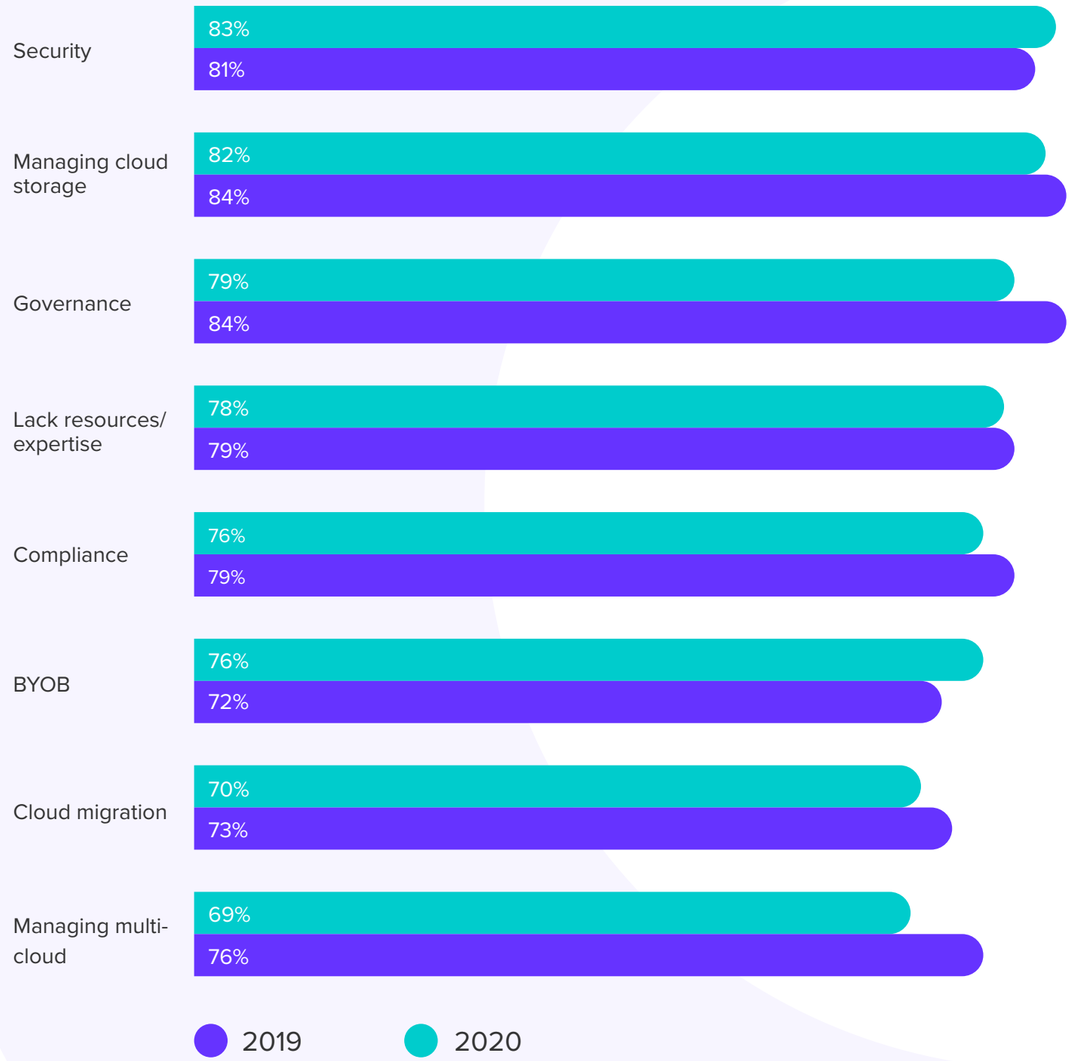
It's been necessary to move quickly in order to respond to change. Cyber security teams have needed to move from routine tasks to rethinking critical components of how they operate. However, not all updates have been effective. There is a big difference between break-fix solutions and sustainable foundations for a better future.

What's more, although there is increasing awareness of cyber threats, the economic situation is squeezing some cyber budgets. It's critical to find solutions that are able to do more with less in order to keep your operations secure.

Security identified as the top cloud challenge

On-premises protections disappear once employees are outside the office. Even if employees do log into a company network before accessing cloud data, they may be doing so from an unsecured internet connection using a personal device with outdated security software.

With cloud platforms accelerating the use of remote working during the pandemic, security issues need to be identified and actioned promptly. Cloud security has always been a serious topic. However, we can see positive shifts in how security is perceived.



Expected cyber security spending by organisation size and sector (in the next 12 months)

Expected spending change in next 12 months by industry (no time)

- Increase
- Small increase
- No change
- Decrease

Budget changes vary dramatically by industry

McKinsey projects that overall spending should taper off in industries that were hit hard by COVID, while holding steady or even increasing in other sectors.

Gartner projects slow growth in spending overall. Cyber security grew at 12% (CAGR) in 2018, and it's projected to decline to only 7% (CAGR) by 2023. Something to keep in mind is the potential that cybercriminals target industries and brands that they believe are suffering and have, therefore, reduced cyber spend.

Gartner clients also report that boards are pushing back on investments and want to understand the outcomes that are being achieved. By 2023, Gartner estimates that 30% of CISOs (Chief Information Security Officers) will be measured on their ability to create value for the business.

Pro tip: If you want help talking to the board, check out our free resource — The Board Presentation Toolkit: Cyber Security and Threat Management.

Endpoint security is an important investment

Endpoint security is an approach to cyber security that focuses on user devices. However, its goal is to protect the network, not each individual endpoint. An effective EPP (Endpoint Protection Platform) can deliver centralisation of security (and control) and the decentralisation of risk.

Note: An endpoint is any physical device that is the end point of a network – desktops, laptops, mobile phones, tablets, servers and virtual environments can all be considered endpoints.

Endpoints are where the most valuable data can be the least protected. With the switch to remote working, this is even more true. They have access to all data needed to conduct business, and every endpoint represents a useful target for cybercriminals, even if no sensitive data is present. A response to this threat is reflected in across-the-board increases in spending on endpoint security.

Endpoint security allows for better security outcomes, relying on cloud-based security tools which free end-user devices from the bloat associated with managing this capability locally. The whole system can be updated faster, deliver better outcomes and enable easier management. It also gives the opportunity to partner with proactive management and response services.

Microsoft is the endpoint market leader

Microsoft is the only vendor that can provide built-in endpoint protection capabilities integrated with the operating system (OS), making it unique in the EPP space. Windows Defender Antivirus is now a core component of all versions of the Windows 10 OS and provides cloud-assisted attack protection.

Where Microsoft is making real transformations, however, is with advanced threat protection. Microsoft Defender Advanced Threat Protection (ATP) is now Microsoft Defender for Endpoint. This solution adds a range of capabilities on top of standard Windows Defender, including:

- EDR (Endpoint Detection and Response) capability.
- Monitoring and reporting on Windows Defender Antivirus and Windows Defender Exploit Guard.
- Vulnerability and configuration management.

It uses a combination of technology built into Windows 10 and Microsoft's robust cloud service to provide:

- **Endpoint behavioural sensors:** Collect and process behavioural signals from the operating system and send this sensor data to your private, isolated, cloud instance of Microsoft Defender for Endpoint.
- **Cloud security analytics:** Behavioural signals are translated into insights, detections, and recommended responses to advanced threats.
- **Threat intelligence:** Identifies attacker tools, techniques, and procedures, and generates alerts when observed in collected sensor data.

Microsoft is betting heavily on endpoint security. It's a key point for upselling clients to Microsoft 365 E5, which is a significant element of the Defender for Endpoint story (Defender is the larger portion of the cost of E5).

Adding managed services to complete the picture

Endpoint security significantly improves an organisation's ability to respond to change within remote workflows. But it needs human-led cyber incident management, prevention and analysis to be truly effective in today's hostile digital landscape. Although the data suggests that only large organisations are currently increasing managed security budgets, it's an important point to consider.

Most organisations, especially smaller ones, struggle to stay on top of the large volumes of alerts generated when managing an active response unit. It's necessary to understand what's important and what isn't – and then action alerts in a timely fashion. A partner can provide the flexible resources required to deliver full coverage effectively, and free you to focus on your actual business while remaining secure in the current threat landscape.

Six Degrees Managed Detection and Response is delivered in collaboration with Microsoft Defender for Endpoint. This combination offers a unified endpoint security platform for preventative protection, post containment investigation, and contextualised response. It delivers:

- Deployment, configuration, and management to your unique data management policy.
- Expertise to apply industry-specific intelligence to your organisation's risk profile, elevating your cyber security.
- 24x7 real-time alert management, detection and response by our cyber security experts.
- Continuous review of threats contained and proposed remediation advice to reduce future risk.
- Trended reporting of critical threat metrics to quantify the risks that have been contained.

How to create a new best practice

It’s important to rethink the basics of cyber security. In order to meet the demands of 2021 and beyond, security teams will need to do more with less, while managing a more dangerous landscape. That means:

- More security
- Less technology to manage
- Less operational oversight
- Less cost
- Less risk
- More visibility and agility to respond to threats

It’s critical to avoid:

- Siloed on-premises tools and datasets that lack visibility, correlation, and automation.
- The addition of new tools that complicate operations without adding value.
- Poor security outcomes that endanger business goals and objectives.

Fundamentally, perimeter-based and traditional cyber security operations do not have the flexibility or endpoint visibility required to manage remote access. We’ve seen the industry move towards endpoint investments. However, it’s worth setting out a response strategy in more detail. Let’s walk through how to take the information we have discussed to this point and apply it to the specifics of your own business.

Step 1: Understand your risks and vulnerabilities

The key to effective security is to understand:

- **Vulnerability to attack**
- **The value of critical assets**
- **The profile or sophistication of potential attackers**
- **Your organisation's appetite for risk**
- **Key business goals requiring security investments**

There is no one answer to these questions. Although it's important to look at industry-wide trends, you need to tailor investment and planning to your specific needs. For example, if your business hasn't made a transition towards remote working, a lot of the advice supplied here won't be relevant — or at least not as critical.

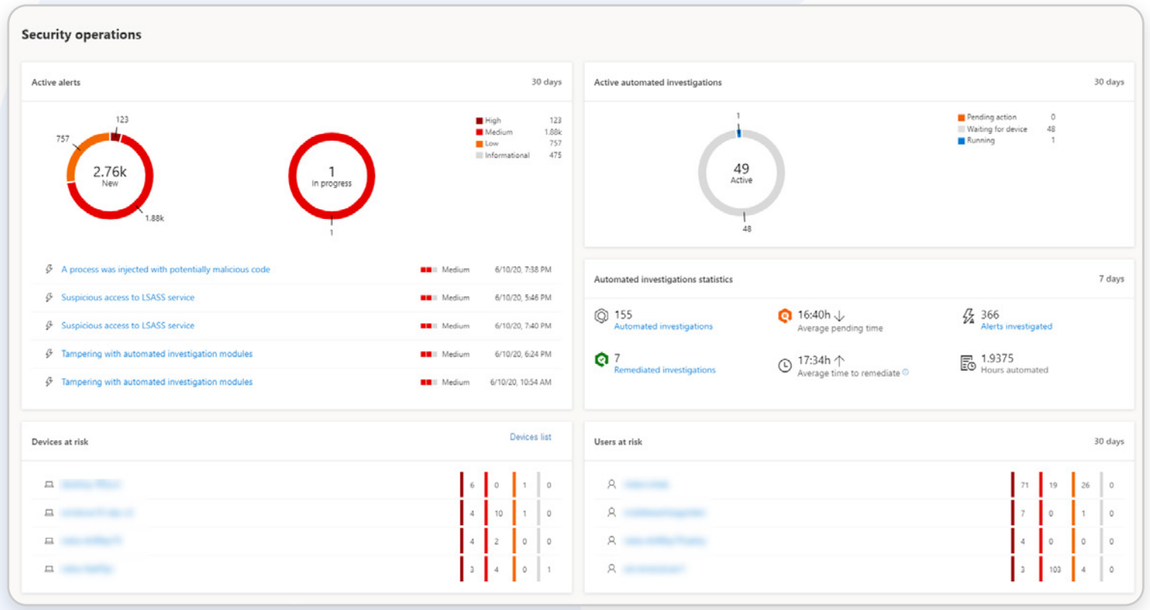
Your security solutions need to weigh your organisation's appetite for risk against objectives (KPIs), capacity for investment and known threats. Ultimately, valuing all of these factors using financial measurements makes it far easier to compare trade-offs and determine the ROI of investments. Fundamentally, a cyber security risk assessment will help you understand your requirements and make good, evidenced internal decisions. Get in touch if you want help.

Step 2: Embrace endpoint security

For most organisations, investing in endpoint security will be the right move. It can enable you to create an effective and agile security framework that can accommodate the needs of remote access without creating security vulnerabilities. When security capabilities are unified in platforms, apps, and cloud services, integrated endpoint security can provide a seamless and completely transparent experience.

All endpoint security solutions should be expected to provide:

- Data classification and loss prevention
- Insider threat monitoring
- Network and privileged user access control
- Anti-malware
- Email gateways
- Endpoint Detection Response (EDR)



As we've pointed out, Microsoft has become a leader in endpoint security solutions. There are other options. However, if you are already a Microsoft 365 user, upgrading to Microsoft Defender for Endpoint is an easy move that will provide access to leading-edge capabilities – and is an outcome that **we can help you achieve**.

Step 3: Create a managed response team

If you want true flexibility and reliability, a managed response team will help you do just that. Cyber-threats aren't passive, and your defence needs to respond in kind. That means access to specialists who not only check compliance with your security approach but continuously monitor the actions of the hackers.

As stated, DoS attacks account for more than 50% of breaches. With a managed service added to endpoint capabilities, you can build in cyber incident management, prevention and analysis – right down to the endpoint.

To use Microsoft as an example, your team will be able to leverage the Defender for Endpoint security platform to get regular updates and manage incoming alerts. At Six Degrees, we do this by partnering Defender for Endpoint with proactive forensics delivered by cyber security professionals operating 24x7 from an onshore Cyber Security Operations Centre (CSOC).

A full-service solution like ours will:

- Mitigate the cyber security risks of maintaining a remote workforce.
- Reduce hackers' ability to expand cyber-attacks across your infrastructure.
- Minimise the risk of a data breach resulting in financial, operational and reputational damage.

Pro tip: Look to MSPs to provide support

You can create an incident response team in-house, or partner with a managed service provider (MSP) to access on-demand resources at lower cost. Although there are some benefits to having an in-house team, the ability of an MSP to immediately scale-up resources in response to an incident is a more efficient method for achieving equally secure results.

Fundamentally, cyber security partners let you stay focused on what matters most, your business. Cyber security should always enable business goals. Part of that is about creating secure systems, but it's also about getting out of the way. If all of your in-house resources are focused on security, you won't have the bandwidth to actually get things done. **At Six Degrees, we provide managed response services** and can work with you to create a team that is able to succeed.

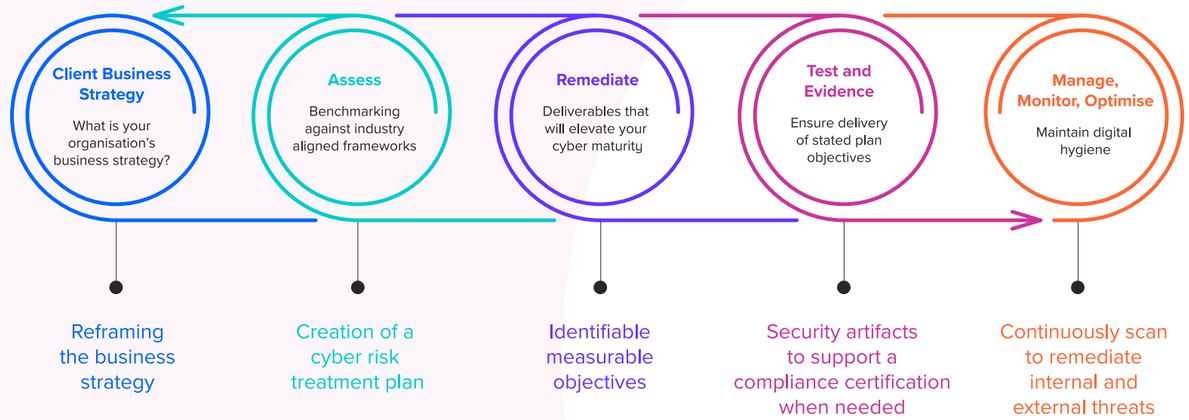
Step 4: Understand the cyber journey

It's essential to build a repeatable cyber security process that will help you prioritise the right strategies, experiment with new options and hone in on what works best without creating vulnerabilities. Remember, cyber security is not a destination, it's an ongoing process. The danger is that businesses implement a security programme and think they're done. They're not.

You can spend a great deal of money developing the necessary standards, guidelines and procedures required by a comprehensive security program, and spend more on the technology needed. But if the situation changes, inflexible investments can become redundant quickly.

The best strategies are those that can be applied flexibly to new situations, and help you incrementally improve your systems to stay secure. This is one of the significant benefits of endpoint and managed security solutions.

Effective security requires a continuous process that includes:



The circular nature of this journey means that by selecting your largest blind-spot, you can then work your way through all of the critical questions that need to be answered to develop a robust set of actions.

Do not ignore the human dimension of security; there is a cultural aspect that must become part of the DNA of the organisation. But the right tools are critical to getting the job done.

Step 5: Stay focused on outcomes

There is no reason to invest in cyber security technology or processes simply for the sake of it. You want to make investments that align with your business, your risk profile and your appetite for risk. Cyber security should enable you to take strategic and tactical actions that further business goals and drive commercial success. Fundamentally, focusing on outcomes is the best way to:

1. Target your cyber investments in the most efficient and effective way possible.
2. More successfully communicate the value of cyber security to your business and gain support for additional resources and investment.

In general, cyber security can end up being considered a cost centre when everything is going right. In a crisis, you will have everyone's attention, but then it's too late to do anything about it.

Communicating what effective cyber security will enable your business to achieve and comparing those commercial outcomes against the cost of investment is an effective way to centre your organisation around cyber and gain support for the investments your business needs to stay secure. By thinking about how cyber will enable marketing, HR, finance and more, you can reach across functions and create advocates for cyber spend that sit outside of traditional IT.

Remember, delivering commercial success is the real purpose of your business. Your ability to stay focused on outcomes is one more reason that looking for cyber security partners can be so valuable.

A safer tomorrow

Shifts in how we work are occurring all over the economy, and security needs to keep up. BYOD and remote working are here to stay, and creating a flexible and digital workspace is critical. Although segments of the economy are experiencing significant budget constraints, there are opportunities in effective investment.

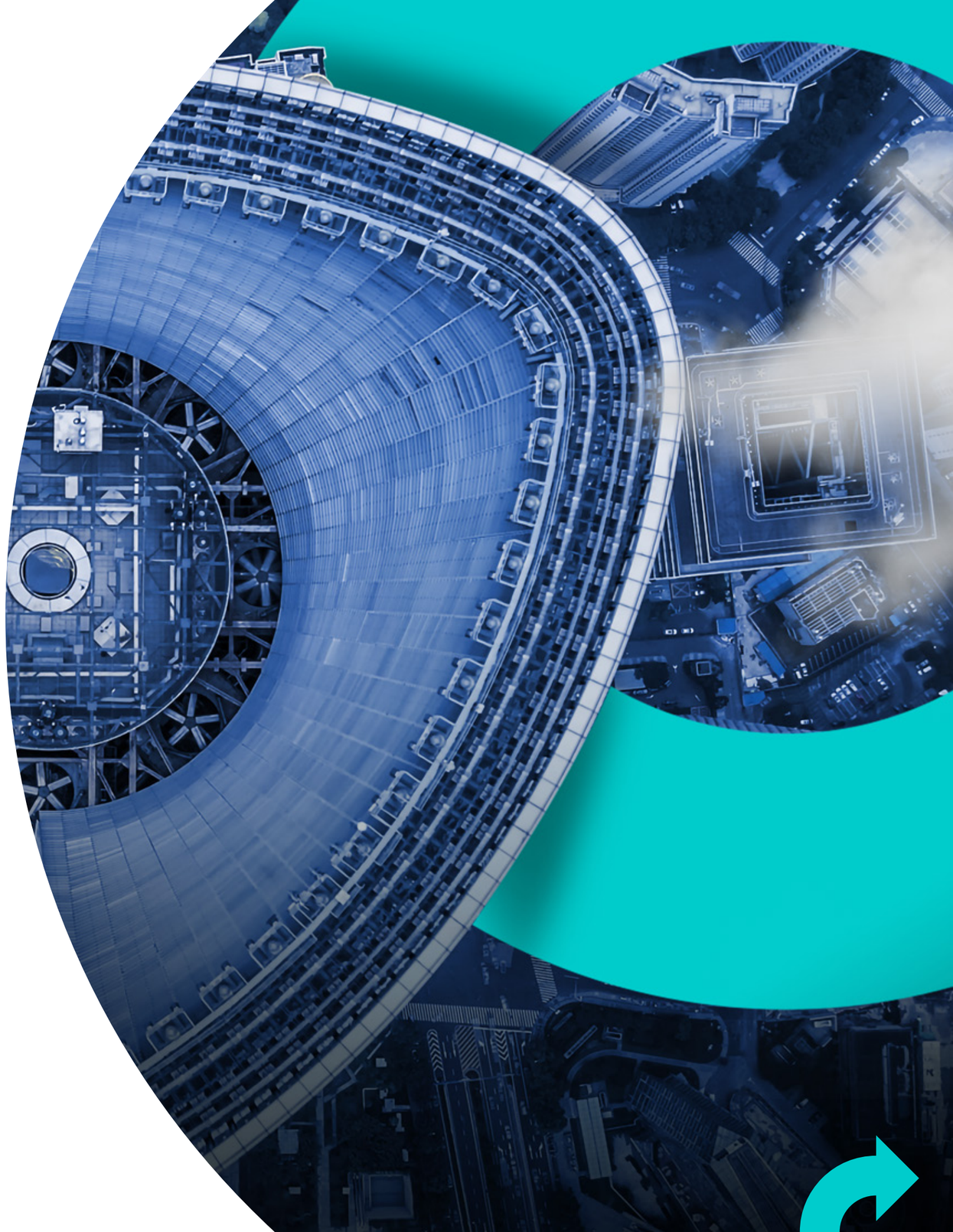
More than ever, cyber security sits at the heart of commercial success. The need to transfer more data and more workflows online makes cyber critical to executing new business strategies.

The structures we put in place today will shape the future, and it's essential to build long-term sustainable foundations.

By understanding the opportunities, it's possible to make the right investments now and justify that spending to build a safer tomorrow. We believe the key to effective and flexible cyber outcomes is a combination of endpoint security and managed services to deliver proactive and reactive defence within an agile framework.

Invest In Cyber Security Today To Build A Safer Tomorrow

Chat To Our Experts



Bibliography

- **Pg 4** “we saw record breaking figures”: **www.oliverwyman.com**
- **Pg 4** 1. Remote Working Statistics: **www.ons.gov.uk**
- **Pg 5** “87% of global IT decision-makers agree that 2020”: **www.logicmonitor**
- **Pg 5** Graph: **info.flexera.com**
- **Pg 5** Graph: “Projected shifts in workloads by 2025 before and after COVID”: **www.logicmonitor**
- **Pg 6** “Grow 6.3% in 2020 to total $257.9 billion”: **www.gartner.com**
- **Pg 6** “More than half of cloud decision-makers”: **resources.flexera.com**
- **Pg 6** Table: “Type of data that will move to cloud”: **resources.flexera.com**
- **Pg 7** “Number of attacks 2020”: **www.microsoft.com**
- **Pg 7** “Three most common causes of security breaches”: **enterprise.verizon.com**
- **Pg 7** “Nine out of 10 coronavirus domains are scams”: **www.zdnet.com**
- **Pg 7** Graph: **securelist.com**
- **Pg 7** “88% of these phishing attacks”: **www.securitymagazine.com**
- **Pg 7** “Emotet phishing attacks”: **www.6dg.co.uk**
- **Pg 8** Graph: “Sectors targeted by ransomware, April to June 2020”: **www.6dg.co.uk**
- **Pg 8** “There has been a 187% increase in cyber incidents”: **www.6dg.co.uk**
- **Pg 8** “1. New types of cybercriminals”: **enterprise.verizon.com**
- **Pg 9** “DoS attacks (hacking) were responsible for over 50% of breaches”: **enterprise.verizon.com**
- **Pg 11** Graph: **flexera.com**
- **Pg 12** “Overall spending should taper off in industries that were hit hard by COVID”: **mckinsey.com**
- **Pg 12** Table: **mckinsey.com**
- **Pg 12** “Projected to decline to only 7% (CAGR) by 2023”: **www.gartner.com**
- **Pg 13** Table: **mckinsey.com**
- **Pg 14** “Microsoft is making real transformations”: **docs.microsoft.com**
- **Pg 18** Screenshot: **docs.microsoft.com**

Six Degrees

Six Degrees. Beyond Cloud.

We help customers enjoy all the game-changing potential of cloud. We create secure, flexible platforms that set organisations free to achieve and exceed their boldest aspirations, whatever those may be.

Beyond Cloud
6dg.co.uk