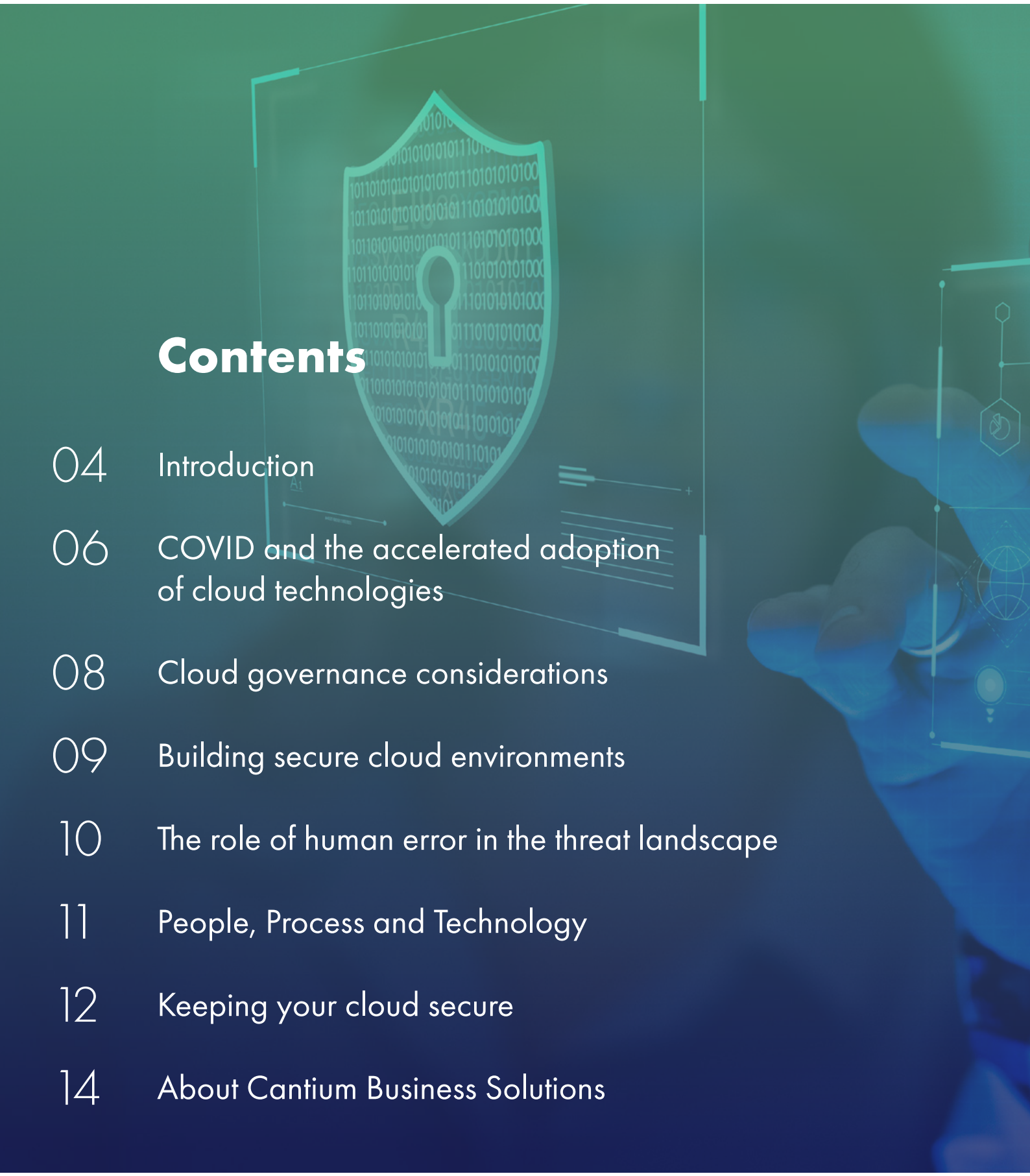
Cantium
Business Solutions

Cyber Security for the Public Sector



Contents

04 Introduction

06 COVID and the accelerated adoption of cloud technologies

08 Cloud governance considerations

09 Building secure cloud environments

10 The role of human error in the threat landscape

11 People, Process and Technology

12 Keeping your cloud secure

14 About Cantium Business Solutions


A1
INNOVATION
INNOVATION
Data-A
DATA

Introduction

2020 caused major disruption to both our physical and digital worlds. With many public sector organisations forced into dispersed and virtual settings, we've seen the swift adoption of remote systems and networks to enable collaborative working and more agile processes. However, this rapid transition has also exposed a range of security vulnerabilities from securing remote access to targeted phishing campaigns, giving cyber criminals the opportunity to exploit the uncertainty brought about by the pandemic and cause chaos.

Over the past year, the sophistication of threats has quickly increased, evolving to harness techniques that make attacks harder to spot and breaching even the most resilient targets.

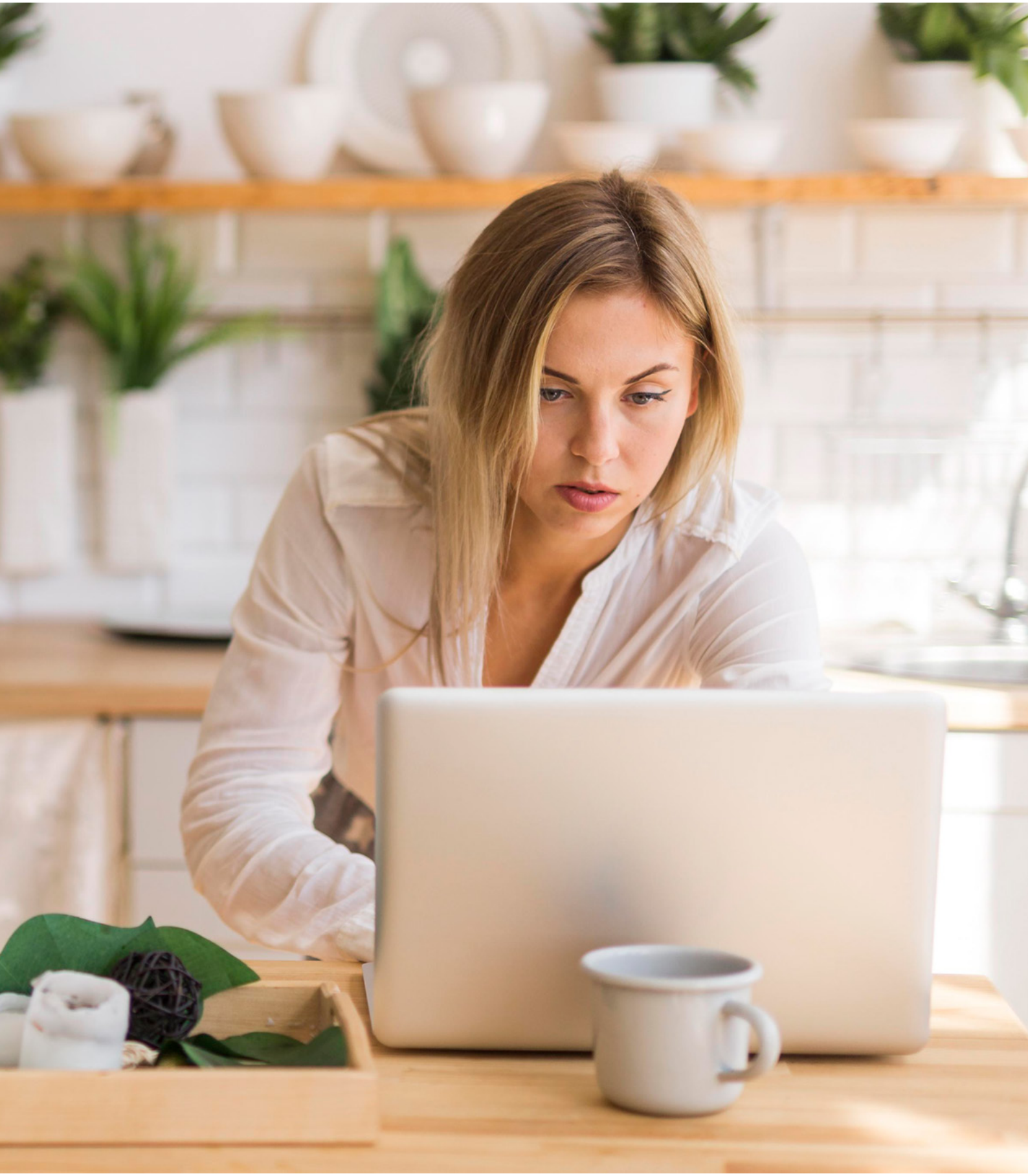
Justin Torgout, Director of The South East Cyber Resilience Centre explains, "Cyber criminals are looking to make their attacks more targeted to infiltrate bigger organisations that are likely to progress a better yield in relation to the data they can harvest and then sell on the dark web."

There has been a sharp increase in the number of ransomware attacks over the past year, and the National Cyber Security Centre (NCSC) suggests that the way in which cyber criminals are operating is also changing. Previously, victims of ransomware attacks were denied access to data until a ransom was paid. New tactics employed by cyber criminals include threatening to leak sensitive information to the public until payments are made. The NCSC also reported an increase in the number of cyber security incidents this year, claiming on average British businesses have been protected against an average of 60 attacks per month.

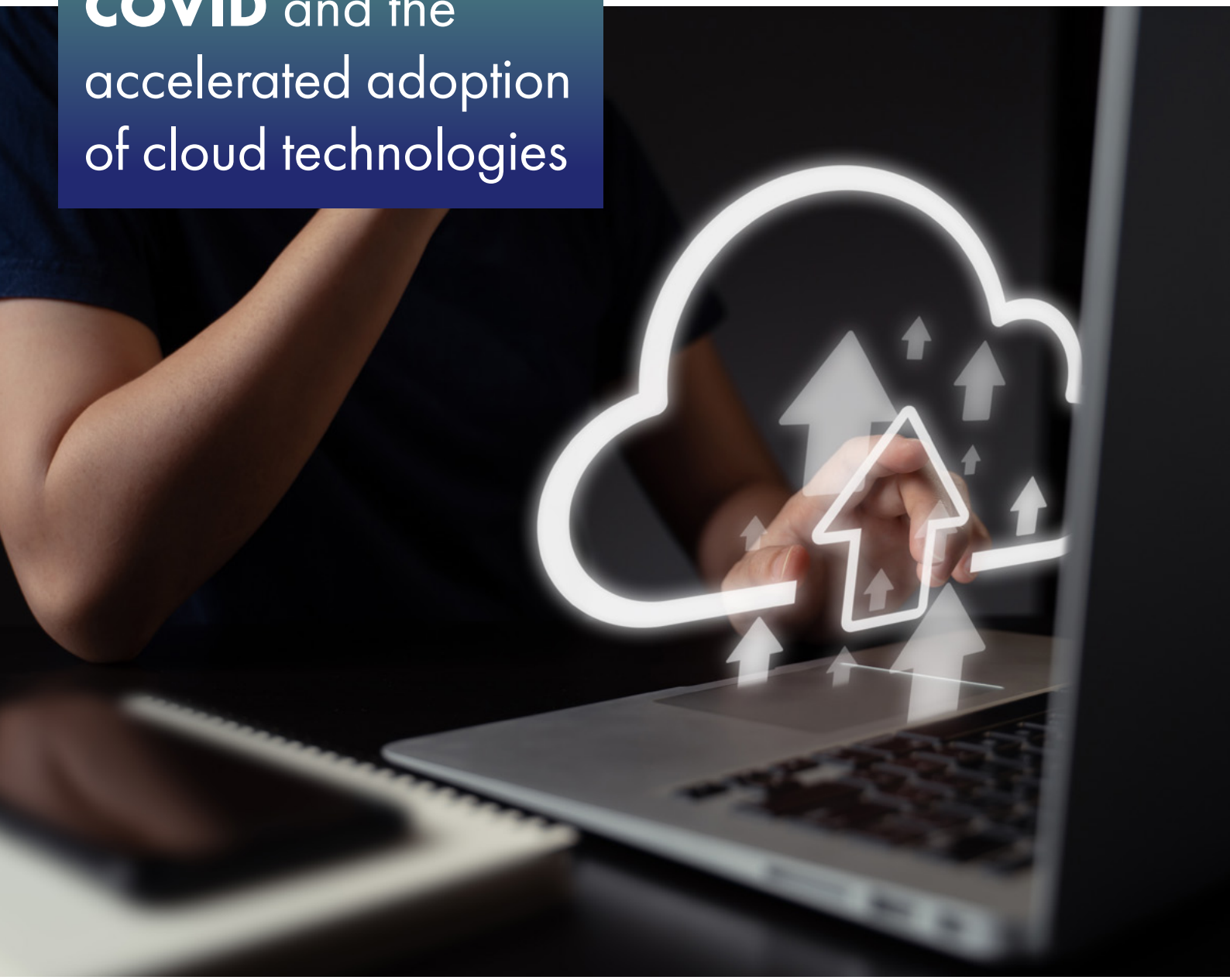
Amidst the disruption of the coronavirus pandemic, cyber criminals have taken the opportunity to prey on vulnerable organisations. London authority Hackney Borough Council was the target of a particularly serious cyber attack in October 2020 that saw personal identifiable information stolen and published online. The attack is continuing to disrupt services and IT systems months on, derailing house purchases as the council is unable to process land search requests. The NCSC's support for the healthcare sector has seen the centre scanning more than one million NHS IP addresses for vulnerabilities. This has subsequently led to the detection of 51,000 indicators of compromise.

The evolving threat landscape, coupled with rapid digitisation and a largely dispersed workforce, brings increased security concerns. The volume of sensitive information now held and shared across networks by public sector organisations means they are valuable targets – this poses an opportunity for attackers but also defenders. Now is a good time to evaluate cyber security risk and exposure to determine whether existing controls and measures are robust enough.

In this paper we will explore how public sector organisations can achieve cyber resilience and ensure solutions are right for the long-term – sharing our insights, knowledge and experience on how to manage cloud environments and proactively protect your networks, systems and data.



COVID and the accelerated adoption of cloud technologies



Undoubtedly the disruption over the last year has prompted an accelerated adoption of cloud technologies. Services were spun up almost overnight, and they played an instrumental role in maintaining operational resilience and enabling public sector organisations to continue delivering vital frontline services to citizens. For many, the pandemic has been a catalyst for change and brought home the need for greater flexibility, scalability and a robust IT infrastructure.

Policies like the government's 'Cloud First' approach have been key in enabling the public sector to embrace this recent period of accelerated digitalisation. The approach encourages the consideration of cloud solutions before any other option and is designed to reduce public sector spending on outdated IT and technology ecosystems. With the use of legacy technology comes vulnerabilities and a greater risk of being exploited by cyber criminals.

Rather than spending valuable funds on hardware, software, licensing and renewal fees, organisations pay the provider for what they use, when they need it. Cost reduction is one of the main benefits of cloud environments, but organisations also gain much more with IT infrastructure that allows the workforce to be more flexible and gives organisations the ability to adapt to change.

The pandemic has seen the demand for public services peak at various points in the past year. With an old-style server in a data centre, IT teams would have built the infrastructure to meet the capacity required for peak demand. By using the cloud, services can be easily scaled to meet requirements, providing organisations with the ability to manage costs and meet rapidly changing demands.

Clearly, the promise of cloud is enormous, but even accelerated cloud migration projects need to be well thought out. Ultimately, organisations need to strike a balance between making the most of the efficiencies modern cloud-based environments bring whilst ensuring that the pace of uptake is never at the expense of security for users and above all else, the citizens they serve.

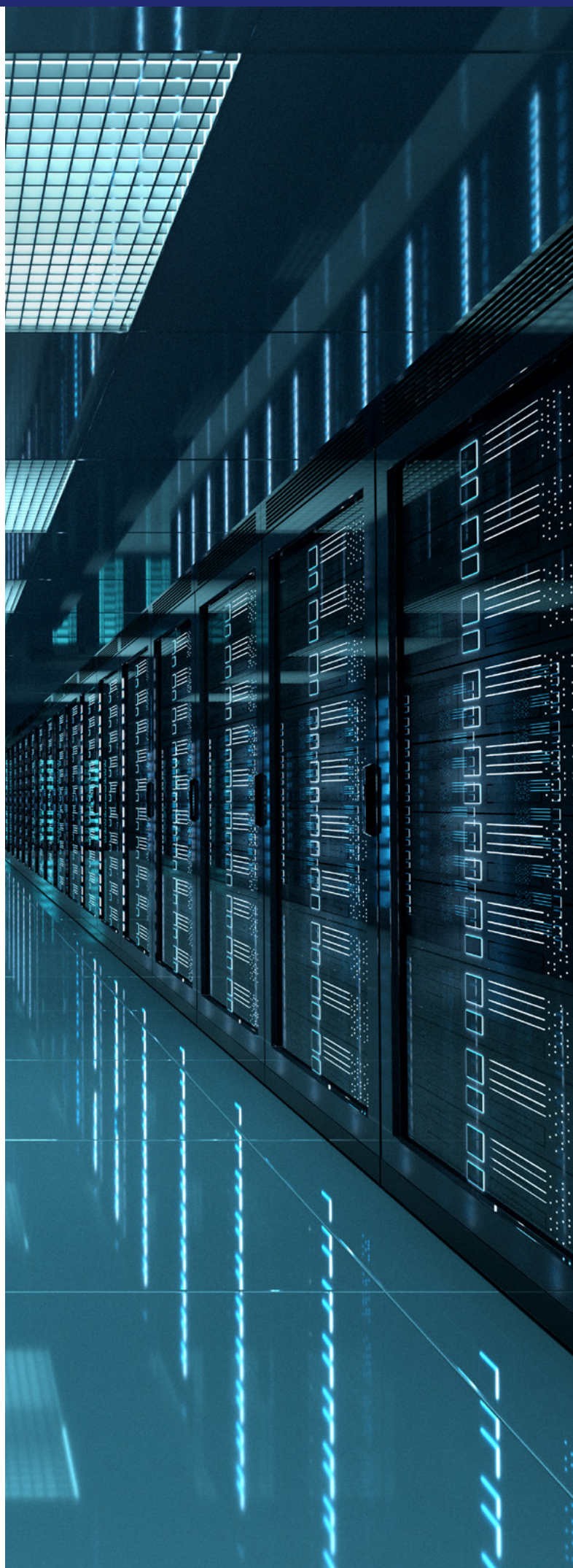
Cloud governance considerations

Given the challenges the public sector faces, from budget constraints to digital capabilities and compliance – now is a good time to take a step back and check that those newly implemented solutions have been bedded in correctly and are right for the long-term.

Data governance considerations need to come into play. It's important that sensitive data is stored and managed in line with regulatory requirements - not only to maintain compliance with regulations such as GDPR, but also to mitigate security concerns. Public-facing organisations need to maintain strict control over sensitive data and retain the ability to delete or destroy that data when required. A lack of effective data governance is a worry, mainly because poorly structured data makes it much more difficult to detect and monitor when something goes wrong. Any misuse of data, especially in the public sector, can have far-reaching consequences and could lead to a loss of citizen trust.

Spend on cloud services also needs to be in line with expectations. Cost governance practices may very well be different for each organisation and vary between departments. For instance, those organisations operating in the health and social care sectors are likely to have longer-term storage needs, as they will need to keep records for greater lengths of time. Mapping out the right infrastructure will help public sector organisations gain a realistic view of what the cloud will provide from a technological and financial perspective.

With attacks becoming increasingly sophisticated and more targeted, frameworks such as ISO 27001 can also be followed to ensure best practice and help organisations manage their information security by addressing people and processes, as well as technology. Ultimately, cloud governance shouldn't be an afterthought. Without it, organisations will struggle to control costs, reduce human error and protect valuable data.



Building secure cloud environments

As public sector organisations become increasingly reliant on mobile devices and cloud-based technologies to run their teams and vital services – networks, services and devices become prime targets for cyber criminals.

"There are an estimated 22 billion devices connected to the internet worldwide, all of which provide a route into hacking, phishing and attacking organisations. This makes cyber security a global issue for the sector," explains Mark Scott, CEO at Cantium Business Solutions.

Everybody thinks they won't fall victim to an attack, until they do. So here are some points for consideration when it comes to building secure cloud environments.

Firstly, understand the types of data that you intend to store in the cloud. This will help guide you to the types of security tools and processes that will need to put in place. It's important to ensure the most appropriate controls are used so the organisation isn't hindered and can still gain the full benefit of using the cloud.

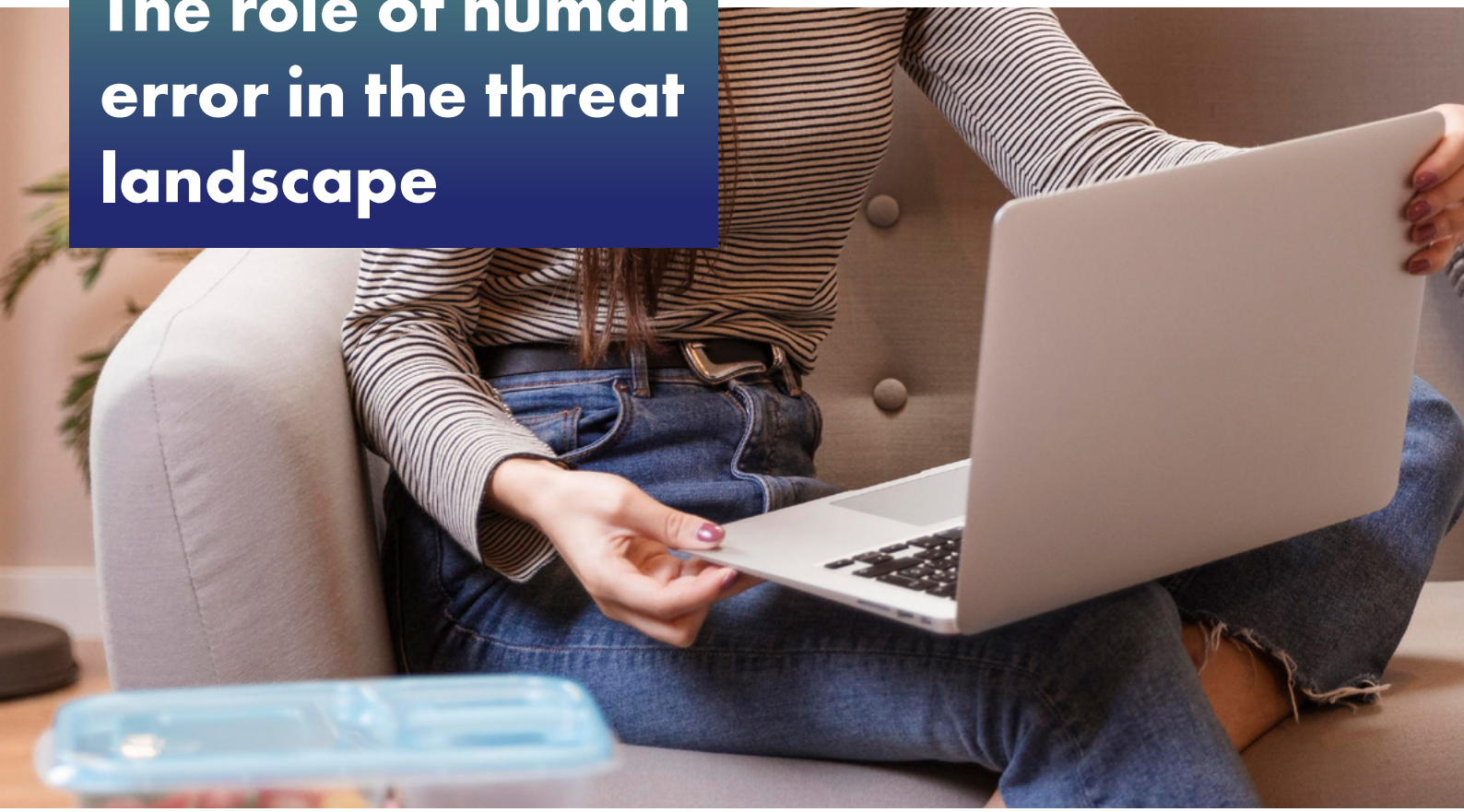
Different types of data will need to be secured in different ways. If, for instance, the organisation is using collaboration platforms, then there is a need for employees and users to be able to communicate in a safe and secure way. Locking away collaborative tools and file sharing capabilities in a way that's too complex or restrictive will prove counter-productive. Instead, understand the types of information that are shared across the platform and take steps that will allow employees to share data in a safe and practical way.

Data classification can play a part in helping to secure collaboration platforms and solutions, for example, stopping employees sharing sensitive information such as child protection records with users who are not authorised to view them. Getting data classification right from the start and driving policies from the centre makes it much easier to keep data safe and secure. Ultimately, employees need to be protected by policies that stop them from inadvertently exposing confidential data.

However, this is very different from the type of security implemented around a business application database. When it comes to protecting applications and databases, security needs to be a core part of the design. The crux of this is good product architecture and understanding that cyber security processes need to be layered in. This approach minimises the risk of exposing information residing in the cloud and should centre around the zero-trust security model. The model is based on the principle of maintaining strict access controls and not trusting anyone by default, even those already inside the network.

By layering applications behind several defensive barriers, it's easier to prevent unintended consequences and employees are only able to access the systems and data they require. Segmenting the network in this way and breaking it into a multi-layer structure enables organisations to hinder cyber criminals, restrict their movement across the network and stop them from reaching mission critical data.

The role of human error in the threat landscape



Cyber criminals are opportunistic by nature and familiar with the struggles that IT departments face. The weak point in any security chain is, more often than not, human. Organisations can build a thousand walls to protect their systems, but employees will always be the most significant risk.

The move to a remote and flexible workforce means that the lines between home and work have become blurred. This change in working patterns brings an increased cyber security risk profile due to the dispersed nature of the workforce. Unintentional actions can cause, spread or allow security breaches to occur and being in a home environment means that employees are more susceptible to attacks.

Whether its people downloading a malware-infected attachment or failing to use a strong password, the more employees an organisation has, the higher their risk profile. The increase in remote working also highlights a greater risk: that individual departments or teams are trying to solve IT bottlenecks themselves. In an attempt to maintain productivity, unapproved software or applications could be downloaded and installed without the involvement of the IT department – bypassing the usual governance checks. The use of personal devices, commonly known as Bring Your Own Device (BYOD) and unmanaged, applications is commonly referred to as 'Shadow IT'.

The problem with these make-do solutions is that nobody has visibility over the data associated with the applications and the users accessing it. Unapproved applications can also compromise an organisation's existing cloud policy and IT strategy. This is where Role Based Access Controls come into play, as they help to restrict the actions employees can undertake and limit damage.

Mark Scott suggests: "To successfully mitigate risk, organisations need to treat internal and external security with equal weight and ensure that it is seen as a shared responsibility by everyone in the organisation. In addition, it's important for public sector organisations to keep an eye on the medium and long term, recognising that remote work may become the norm for many employees long after the pandemic has ended."

People, Process and Technology

People, processes, and technology form the basis of an organisation's security strategy. A lack of attention to any of these three factors will inevitably lead to gaps. Balancing each component is the best way to identify risks and match them with the right tools, cultural norms and workflows to effectively manage risk.

People

Employees can create some of the most significant risks to cyber security. However, when they are well informed, they can also be an advantage and the first line of defence. Educating employees is incredibly important, and they need to have basic knowledge about information security and potential threats. Having the right mindset around cyber security is vital. Getting them interested in security, encouraging the swift reporting of incidents and keeping them motivated to keep their equipment and devices safe will all help to create a robust cyber security culture.

Process

Processes are key to the implementation of an effective cyber security strategy. Well thought out security policies, security awareness programmes, and access control procedures are essential. Not only do they help prevent and detect threats, but they are also crucial in defining how the existing activities can be used to mitigate risk. These processes must be continually audited and as mentioned previously, frameworks such as ISO 27001 provide an opportunity to create specific processes. Proper preparation significantly reduces the risks of cyber incidents and it's important that all processes and procedures are documented as part of the framework and for auditing purposes.

Technology

Technology is fundamental when it comes to cyber security. There are a whole host of technologies that the public sector can implement to layer their defences. By identifying the most common risks the organisation faces, it becomes easier to identify the controls that need to be put in place, and the technologies to support them. Technology can be deployed to prevent or reduce the impact of cyber risks, depending on your risk assessment and what you deem an acceptable level of risk.

Finally, organisations should look closely at network segmentation. Cyber criminals will target networks to gain access and exploit critical data, whether that is medical records, housing and benefit information or financial records. Segmenting networks enables IT departments to separate sensitive data into different subnetworks. This helps to cut off access to different parts of the network in seconds rather than hours, something that can help to limit exposure if there is a breach.

Keeping your cloud secure

The good news is that with a layered security strategy, many cyber security challenges are surmountable, especially with the correct tools and the appropriate cloud partners in place. Below, you will find some actionable steps that will be useful in securing data and helping to prepare for a cyber security breach.

Regularly review the Business Continuity Plan

A Business Continuity Plan (BCP) should help an organisation recover from business interruption. This could be a natural disaster, large-scale IT system outage or a cyber security attack. Without regularly reviewing BCPs and updating them with the latest information, the organisation could find itself unprepared for new problems that arise. When it comes to securing infrastructure from internal and external threats, a BCP is critical in getting back up and running swiftly. It's more than likely the organisation will face threats; it's the response that makes the difference.

The BCP should also include disaster recovery. This is where mission critical functions are identified so that when a disaster recovery process is invoked, the BCP can define what services need to restored first in order of importance.

Conduct table-top exercises

Table-top exercises improve capabilities to respond to real events. With ever-changing scenarios, processes should be regularly checked for operational efficiency and effectiveness. Do your staff know the role that they play if your organisation comes under a cyber attack, where data needs to be recovered and systems are locked?

Top-down responsibility for cyber security is encouraged. It's important that senior figures are at the table when these exercises are being planned out. With the financial and reputational impacts of a cyber security attack being so large, and the Information Commissioner's Office looking to hold directors directly responsible, there isn't room to point fingers.

Data location and classification

Understand what data is located where. Whether it is stored on-premise or in the cloud, it's important to know where it resides as well as the data sovereignty laws the information must adhere to. For example, if the organisation was targeted by an attack, are your backups are encrypted, do you know what information is held there? Many organisations are unsure.

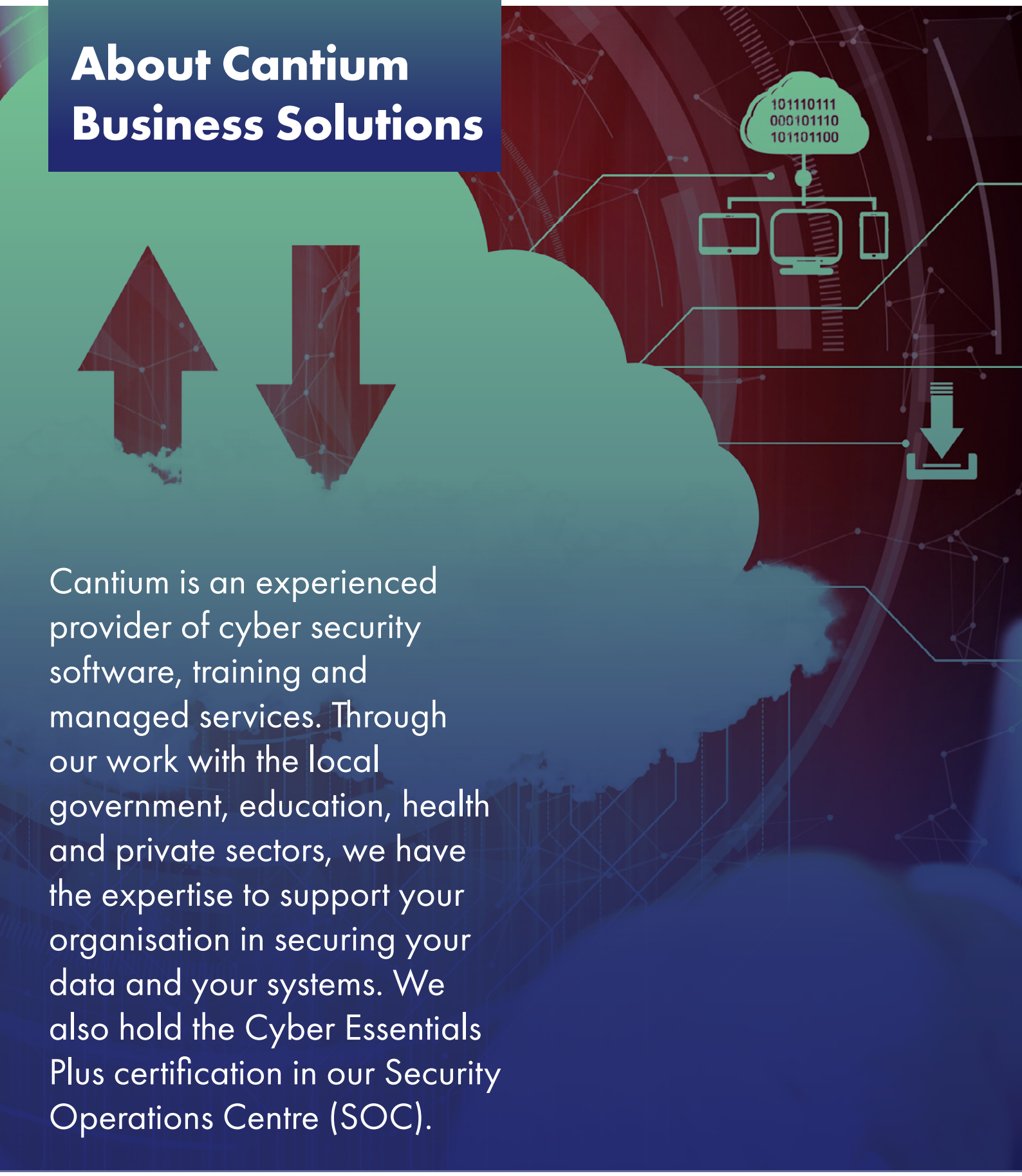
It's not always about protecting the elements that immediately come to mind - that's where a good data backup and archiving strategy comes into play. Consider how much data is stored in one location. Storing everything in one place can make the organisation a more attractive target to cyber criminals. It's important to start by assessing what is currently being protected and why – this will help identify any gaps.

Managed service providers

Having a dedicated external resource frees up internal teams and allows them to focus on business-critical work. This approach enables the public sector to harness expertise, without the cost of hiring – and the provider can manage regular patches and upgrades, backups, proactive monitoring, incident management and response.

Work with a reliable partner who has a good understanding of the challenges the public sector faces and has knowledge and experience of working with various customers in the sector. Before going ahead and working with a managed service provider, make sure you understand the requirements of the relationship and who is expected to do what. This is another consideration when it comes to making sure data remains protected.

About Cantium Business Solutions



Cantium is an experienced provider of cyber security software, training and managed services. Through our work with the local government, education, health and private sectors, we have the expertise to support your organisation in securing your data and your systems. We also hold the Cyber Essentials Plus certification in our Security Operations Centre (SOC).

Cantium
Business Solutions

Sales@cantium.solutions

03000 411 115

cantium.solutions