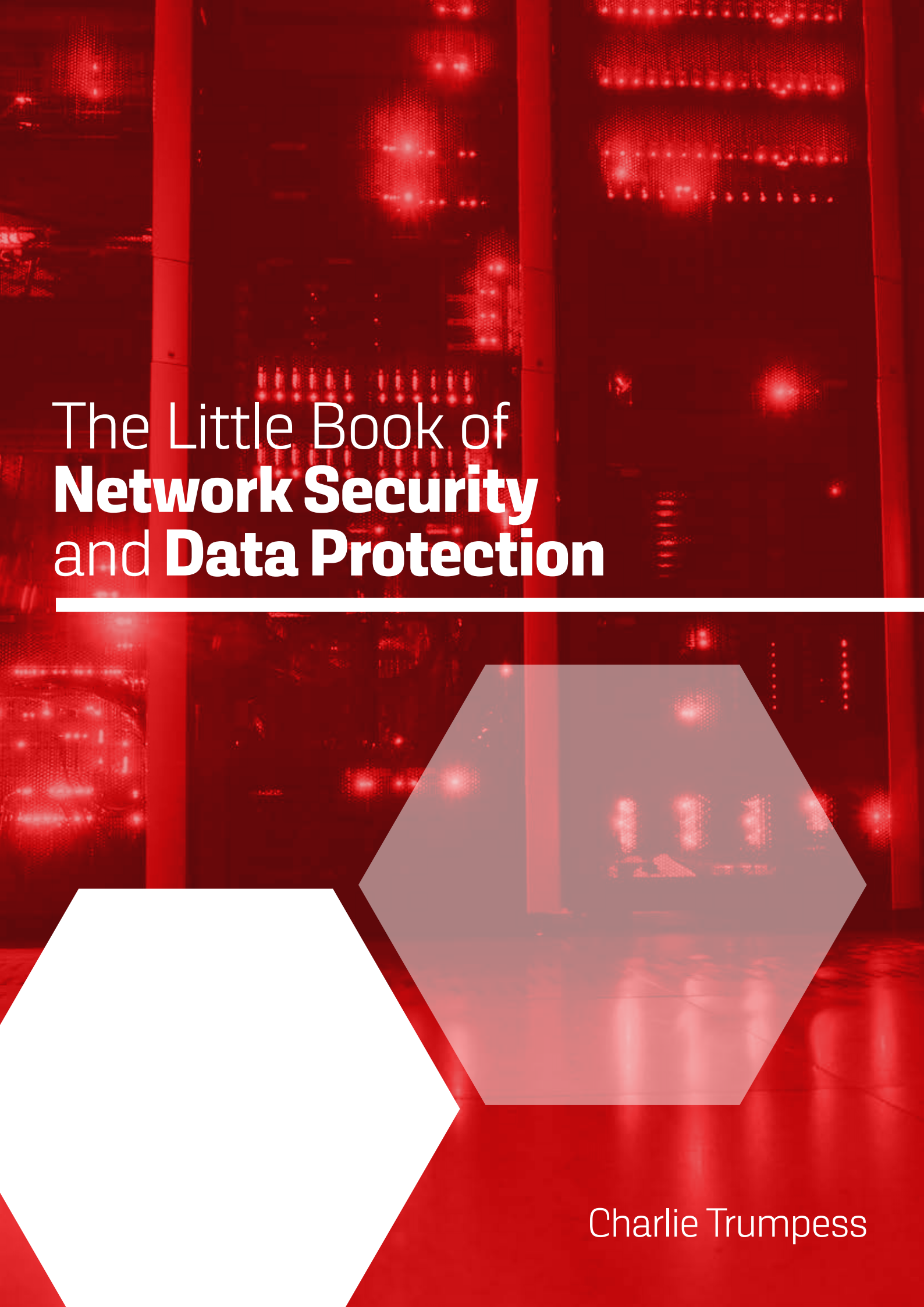
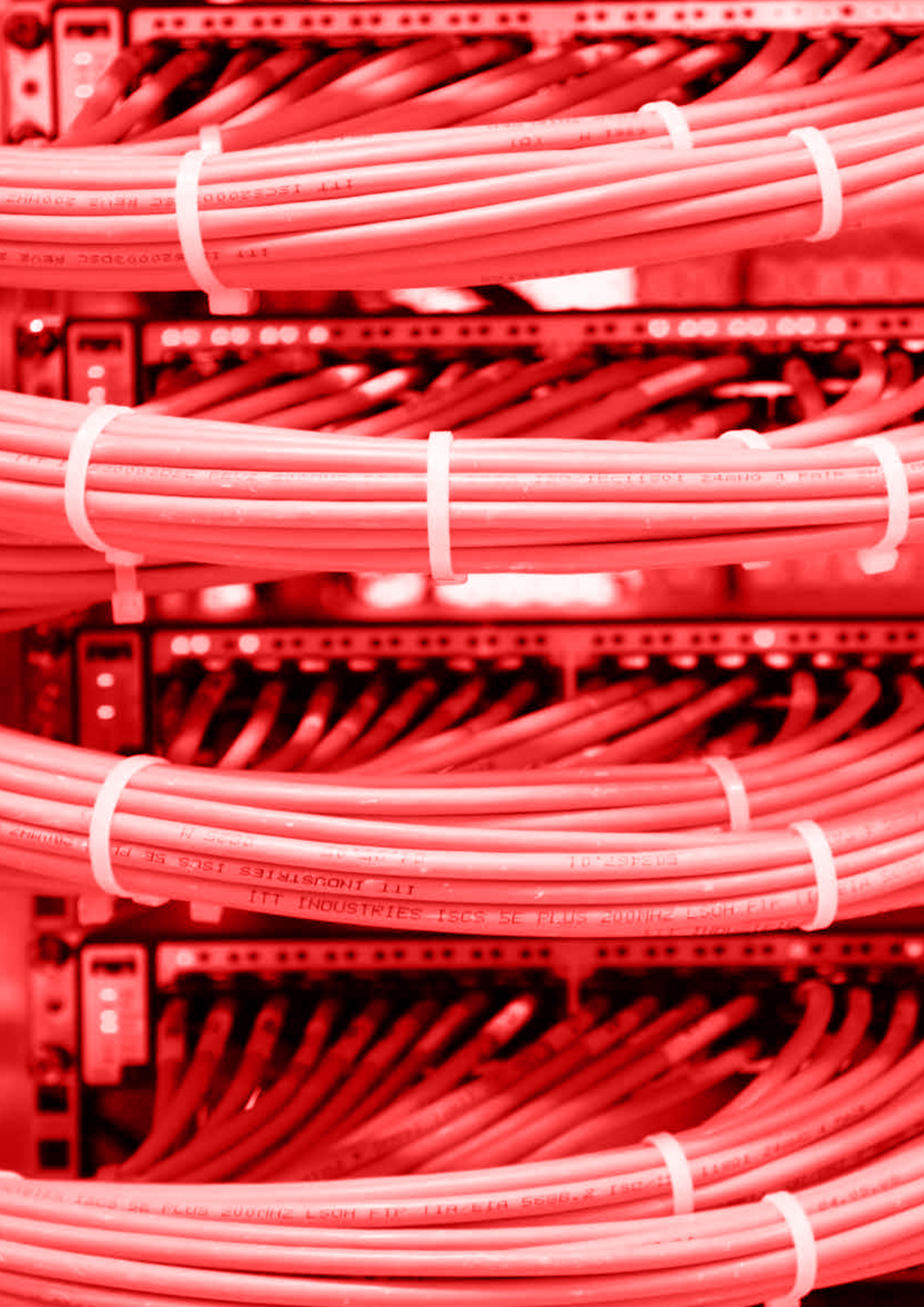


The Little Book of **Network Security** and **Data Protection**

Charlie Trumpess


ITT INDUSTRIES ISCS 5E PLUS 200MHZ LSOH F/UTP

The Little Book of **Network Security** and **Data Protection**

Charlie Trumpess

Contents

Introduction

An Uncomfortable Truth

Ransomware is a hot topic right now. Recent high profile malware attacks like WannaCry show just how vulnerable organisations are to cybercrime. Designed to take your corporate data hostage, ransomware is a growing problem, and no one is safe. Globally, it's estimated that ransomware affects another company every 40 seconds. Ransomware attacks doubled during 2016. Overall, cybercrime cost UK firms £34.1bn last year. The statistics are alarming, but also hide an uncomfortable truth. Many organisations fail to take the most basic precautions to protect themselves.

For the remainder of this book, we look at the three core elements of improved network security: people, processes and solutions.

Human Error

While the multitude of threats from malware and hackers might cause sleepless nights, the real danger to your corporate data is probably closer to home. According to the Information Commissioner's Office (ICO), human error remains the main cause of data breaches in the UK. Staff need much better training and greater awareness of everything from opening suspicious emails to using unsecured file-sharing apps. We will take a closer look at user awareness and training in chapter one.

Upgrades, Patches and Version Control

The WannaCry cyberattack revealed just how many firms are still running old, unpatched, unsupported versions of Microsoft Windows. In 2016, it was found over 60% of UK SMBs placed themselves at needless risk by continuing to use old, unsecured versions of Internet Explorer (IE). Certainly, there is no such thing as 100% security. However, you are not powerless. You can mitigate the risks of becoming a victim.

See Chapter Three: Patch Management.

Backup Plans

Regrettably, bad things happen, even to the most prepared organisations. Human error, hardware failures, malware attacks, power outages and natural disasters. When the worst happens it pays to have a backup plan. That means multiple secure backups of all your company data, so everything is recoverable at a moment's notice.

See Chapter Four: Always Have a Backup Plan.

Anti-Virus

Although WannaCry caught many firms off guard and caused a nice media storm, the fact is that most enterprise-grade anti-virus applications, such as Webroot, can stop malware at the point of attack. It is vitally important to have robust endpoint security policies and oversite of all the devices that connect to your network. How's your BYOD (Bring Your Own Device) policies? Do you know which employees use personal devices on your network? Naturally, anti-virus is only as good as the latest update, the consistency of its deployment, and your firm having an integrated approach to network security.

See Chapter Seven: Anti-Virus Endpoint Security.

Advanced Security

In the popular video game, Resident Evil the shadowy Umbrella Corporation creates a highly advanced, self-aware and homicidal security system called the Red Queen. The Red Queen adapts, evolves and anticipates new security threats, making her a formidable adversary. Today's advanced security systems might not be up to Red Queen standards yet, thank goodness, but they are evolving fast. Solutions such as Cisco's Umbrella gives organisations greater visibility and control of all Internet connected devices, over all ports, even when the users are off the corporate network. Umbrella does some clever stuff, learning from Internet activity to spot the telltale signs of a potential attack before it ever happens. Advanced network security is a big subject, which is why we will dedicate an entire chapter to it.

See Chapter Eight: Advanced Solutions.

Chapter One

The Human Factor of Cybersecurity







Any security system is only as good as its weakest link. In the cybersecurity world, the weakest point is nearly always the human element. Around 40% of UK firms have suffered at least one data breach in the last 12 months. The most common form of breach is a staff member unwittingly clicking on a malicious link within a fraudulent email. Like the shockwave from an explosion, the outcome from a cyberattack can be far-reaching and extremely damaging. In recent years, firms such as payday lender Wonga, Tesco Bank and mobile phone operator Three have had thousands of customer records stolen, lost millions of pounds, seen share prices plummet, and found their brand reputations in tatters.

Human Error

Public awareness of high profile cyber-crimes seems to have little effect on our workplace behaviour, but does inhibit personal online activities, such as banking and shopping. Research by AXELOS found that most UK organisations significantly underestimate the human element of cyber risk. In fact, half of the UK's worst data breaches during 2015 were caused by human error. International standard for information security ISO 27001 and some insurance policies require firms implement cybersecurity training. However, most companies only provide training to senior managers and the IT department. Typically, end user awareness training is a far more casual, ad hoc affair for everyone else.

Security Strategy

A cybersecurity strategy can only be effective where you have clear policies and procedures that everyone understands and follows. Otherwise, your own staff will constantly undermine your IT security regardless of what countermeasures you put in place. First, you need to assess the potential risks to your IT infrastructure, and decide what to prioritise. Next, ensure senior management advocate IT security as a business imperative. Finally, implement a clear information management regime with the appropriate checks and balances. User education will play a critical role in raising awareness of cybersecurity risks and changing behaviours.

Raising Awareness

Changing how people think and behave isn't easy. You might need some expert help. According to research from AXELOS, "The one-dimensional and outdated cybersecurity awareness training provided by most UK organisations is not fit for purpose and is limiting employees' ability to understand what good cyber behaviours look like." Before you do anything, you will need to establish a base level of cybersecurity awareness. Next, rather than bombard staff with masses of information, focus on your top three threats. In the UK, this might be raising awareness of fraudulent email phishing attacks, password protection and use of unsecured file sharing applications, for example.

Audiences Segmentation

When building your end-user awareness programme it is important to consider your different audience groups, and how best to communicate with them. Educational research suggests that interactive rather than passive learning tools and techniques produce the best results in terms of engagement and retention. Remember, there are different types of learners. Some people respond better to visual stimulus while others prefer auditory, text or a kinaesthetic approach (learning by doing).

Games

The more interactive, group-based, relevant and fun you can make your awareness programme the better. Developed by PwC, Game of Threats™ is a cyber-threat simulation designed to test critical thinking and decision-making. The game rewards good decisions and penalises teams for making poor choices in critical situations. Ultimately, players come away with a better understanding of what steps they must take to improve cybersecurity across their organisation.

Free Training Tools

Awareness of UK government-backed cybersecurity initiatives and standards remains low. In a recent survey only 8% of respondents said they were aware of the Cyber Essentials scheme. Currently, only 20% of UK employees receive any cybersecurity or awareness training, and that figure is skewed in favour of larger enterprises. However, there are a number of free cybersecurity courses available such as Future Learn, Responsible for Information e-learning and ESET Cybersecurity Awareness training to get you started. A quick Google search will reveal a dizzying choice of paid tools, techniques and online courses to help you implement a user awareness programme.

Assessment

Having created your cybersecurity policies and introduced awareness training, you will want to measure the effectiveness of your scheme. As phishing attacks are so prevalent, you might send a fake fraudulent email to all employees as a test. You can then measure the number of people who click on a potentially malicious link and the number of people who report the email as suspicious. You could then repeat this exercise randomly as part of a phishing assessment of end user awareness. Alternatively, you can run a full network and security assessment in secret. Use this assessment as a baseline before your users start their awareness training, and then run a comparative check after your people have completed the course.

For more information on cybersecurity and network assessments:
Contact us now – 01462 426 500

Penalties of Inaction

Incredibly, most cyberattacks and data breaches go unreported. Many firms simply lack an awareness of who to report to, why to report breaches, and what reporting achieves. Nevertheless, failing to take the most basic cybersecurity precautions, not reporting accidental data loss and malicious activities can prove costly. The 2015 hack of telecoms provider TalkTalk cost the company an estimated £60m and 100,000 lost customers. They also received a £400,000 fine as the regulator found the cyberattack was completely preventable. New General Data Protection Regulations or GDPR will require every organisation to report data breaches to the Information Commissioner's Office from May 2018. Penalties for failing to comply with GDPR will be severe. Learn more on Chapter Six: GDPR and Cybersecurity Readiness.

Top Tips

1. Raising user awareness of cybercrime and data security starts at the top.

2. Changing human behaviour isn't easy. Use different types of media tailored to your target audiences for best training results.

3. Assess the state of your network security before training starts so you can measure results effectively.

Chapter Two

Segmented Networks & User Privileges

As we have seen, you are more likely to be a victim of a data breach or cyberattack due to the negligent or malicious actions of someone within your organisation. Network segmentation or segregation can improve data security by restricting user access behind the perimeter firewall. As the name suggests, network segmentation means dividing your IT network into a number of subnetworks or zones, such as finance and human resources. In this way, you restrict user access to only those with the right privileges. Should a hacker or computer virus gain unauthorised access to your network, segmentation will limit the harm done. Similarly, local network failures are contained rather than causing widespread problems, such as unexpected downtime. Network segmentation is often a regulatory condition for those operating in highly regulated sectors such as finance and healthcare.

Third Parties

Depending on the nature of your business, you might need to provide network access to third parties such as suppliers and partners. First, you should have a policy in place to vet third parties before you give them access to your systems. Next, ensure that they have segmented access, restricting their activities to essentials only. Any data files transferred to third parties should be done using a secure protocol, encrypted in transit and at rest. Finally, you will want to have an incident plan in place should a security breach occur.

Need to Know

Operating on a “need to know” basis is something common to intelligence services, the police and military around the world. The idea is simple and effective, you only tell your field agents enough about an on-going operation for them to perform their assigned tasks. Should an agent be compromised, captured and interrogated they can only reveal a small piece of the overall operational plan. Similarly, resistance fighters, activists, criminal gangs and terrorist groups often adopt a cell structure, which restricts a member’s knowledge of the organisation to just a few individuals. This helps protect the group from informers and undercover law enforcement. In the IT world, user privileges determine what you can and cannot do on the network, a bit like operating on a need to know basis. However, many organisations fail to apply the concept of least privilege, whereby the majority of staff are limited to a standard user account. Only a select few have super user or administrative rights. By limiting user access you reduce the risk of malicious activity and human error causing major disruption.

User Privileges

Out of the box, Windows PC users login with an administrator account. It's easy enough to create a standard account, but how many people do? Subsequently, any hacker or malware can quickly take full control of your device, change settings, access any file and monitor your activity, usually without your knowledge. The computer you are on right now might be part of a botnet performing a denial of service attack or sending spam. Of course, organisations have to worry about more than just external threats. Disgruntled or negligent employees with the wrong user privileges and full network access can easily cause mayhem. Finally, organisations must consider what user rights they assign to IoT or smart devices that are being used everywhere from environmental controls to alarm systems. Many of these devices are inherently unsecure. A recent Forrester report on identity management found that 80% of breaches involved the misuse of elevated privileges, such as those used by systems administrators, super users, and those with root access.

Risky Inactive Users

The days of a job for life are long gone for most of us. Today, many of us will have between 10 and 15 jobs in a lifetime. On termination of a contract, an employee usually returns their company car, laptop, mobile, credit card and keys to Human Resources. The IT department deactivates the leaver's email and user account. The company and individual happily go their separate ways, except when they don't.

A few years ago, I worked for an international IT company as a contractor. After my contract ended, quite amicably, I discovered I still had access to the company's website CMS and analytics. I retained these privileges for some years until the company was the subject of a takeover. This simple oversight meant I could have easily changed or deleted website content. Clearly, failing to disable or delete the network user accounts of former employees represents a major security risk. Inactive user accounts enabled in Active Directory are also tempting targets for outside attackers. After all, it's a valid account so less likely to be noticed when accessing the organisation's private data and applications, depending on privileges. Because the account is inactive, the original owner is no longer around to alert anyone that something is wrong.

Every organisation must find the right balance between the operational needs, IT and security. Next, an organisation must develop effective procedures for managing identities and user privileges. Wherever possible, only grant minimal user privileges to carry out required tasks. Identify and review all those with privileged user status. Don't allow passwords to be shared, and establish processes to monitor and manage any shared accounts. Ensure you have processes in place to disable or delete inactive accounts in Active Directory after an agreed period. By 2018, it's estimated that 60% of insider misuse and data theft will be the result of poor user access management and sufficient controls.

Top Tips

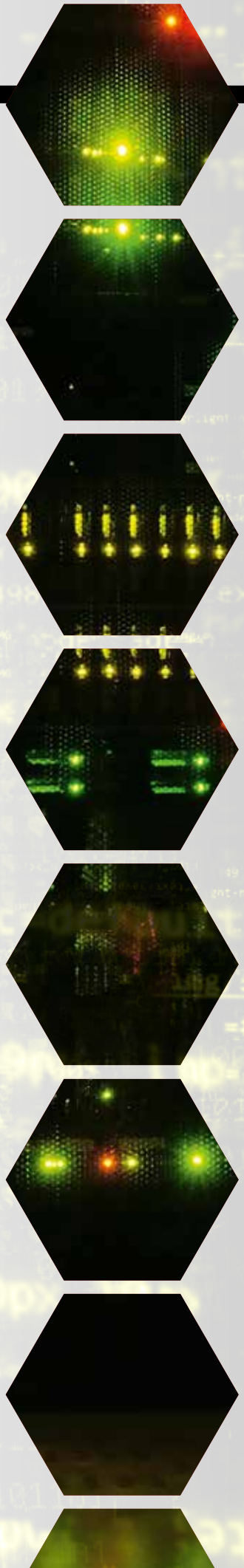
1. Segmenting your network into subnetworks or zones can help prevent the spread of malicious applications and insider misuse.

2. Apply the concept of least privilege, whereby users only have enough network access to perform their specific roles.

3. Ensure you have a process in place to disable or delete inactive user accounts from the Active Directory.

Chapter Three

Patch Management



Until recently, patch management was barely a consideration for many organisations. Instead, 'install and forget' was the common approach to deploying systems. In fact, many systems were rarely or never patched. Of course, the rise of cybercrime and myriad of threats has changed all that, or has it?

Incredibly, 44% of security breaches occur after vulnerabilities have been identified and solutions found. A report by BMC and Forbes Insights found that many months often elapse before identified security vulnerabilities are fixed, leaving organisations needlessly exposed.

The devastating financial and reputational costs of a security breach are well documented. At the same time, the risk of a breach has increased exponentially. That's why patch management is now regarded as a critical part of an integrated defence strategy.

The Cost of Complexity

The rapid evolution of IT systems has meant increased complexity, more points of entry and a greater attack surface ripe for exploitation. Today's IT professionals must look beyond core systems, and safeguard enterprise business applications, remote sites, desktop operating systems and mobile devices. At the same time, businesses have become far more reliant on technology for everything. Even short periods of unplanned downtime can cause disproportionate harm.

Erroneous Task

So, what does good patch management look like and how do you manage it? The key objective of a patch management program is to create a consistently configured environment that is secure against known vulnerabilities in all systems and applications. This sounds simple enough. However, in reality patch management can become a complicated, time-consuming and erroneous task, even for smaller businesses with limited IT infrastructure.

There are many software solutions available to help with patch management but this is only part of the solution. To be successful, patch management requires a combination of people, process and technology.

Where Are You Now?

At this point, many organisations turn to IT frameworks such as ITIL (Information Technology Infrastructure Library) to provide a structure and best practice for executing effective patch management. We would recommend you review your patch management strategy. Does it include the right components of people, process and technology? If not, then this is something you should tackle quickly before it becomes a bigger issue.

IT Audit

It might seem obvious, but a good place to start is by conducting an audit of all your IT systems and endpoints. You can only manage IT assets you know are part of your network, so understand what you have, where it's located, what operating systems and applications are running.

Do you need help performing an IT audit?

Contact us now – info@modern-networks.co.uk

Rationalisation

You might want to think about standardising hardware and software choices, making everything easier to manage. You will also want a list of all the security controls you have in place. In this way, you'll know what requires attention when alerted of a vulnerability. You might also want to think about doing a risk assessment, so you can prioritise your workload. Rationalising your IT will help make it more manageable, but replacing kit or applications because they're going end of life is seldom immediately necessary. Vendors typically continue support, security upgrades and patches for years. Once again, having the right people and processes in place will help you make informed decisions that support your business.

Patch Staging

When a patch becomes available, you should resist the urge to push it out across your network immediately. Sometimes, patching a system can have unforeseen consequences and cause problems. Doing a quick Google search and checking IT forums, for example, can provide an early warning that something is wrong with a patch and offer possible solutions. We would recommend you adopt a patch staging process, whereby patches are applied gradually across your organisation rather than in one go.

Top Tips

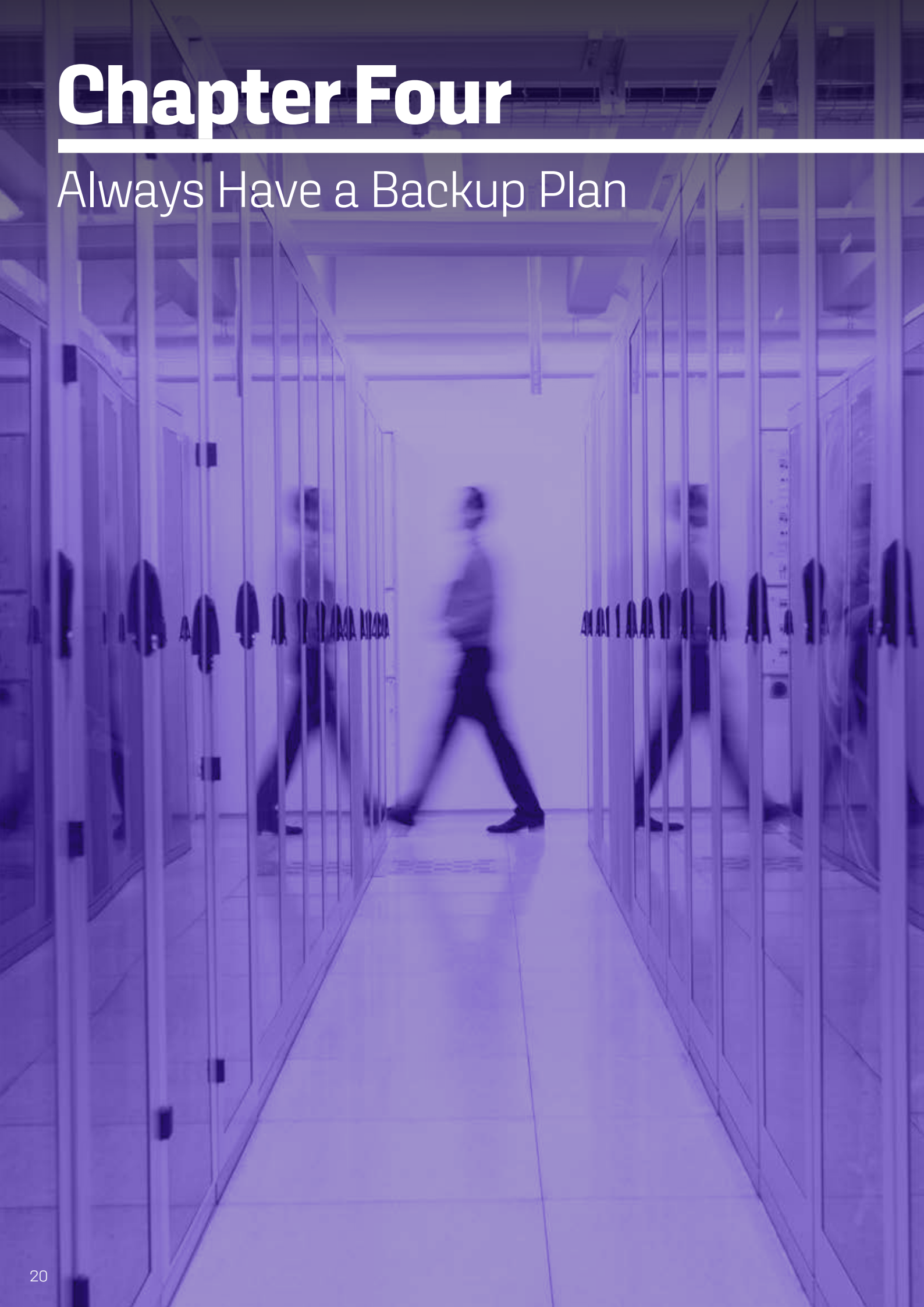
1. Focus your patch management strategy on people, processes and then technology.

2. Conduct an IT audit so you have a clear picture of everything on your network.

3. Patch staging will reduce the likelihood of a new patch causing unforeseen problems.

Chapter Four

Always Have a Backup Plan



Amazingly, over a third of organisations do not backup their valuable data. Of the remainder, many firms have outdated or unreliable backup systems. The result being critical data is either corrupt, out of date or missing when it's needed most. Eliminating ransomware, for example, will require you wipe your systems. So, you'll need a companywide backup plan to quickly recover from the attack. The more frequent the backups, the less data is lost.

Strategy

Whatever your industry, data backup, archiving and recovery are critically important. You must develop a clear strategy. First, you will want to think about just how much data you're going to generate, it's probably a lot more than you would imagine. On the plus side, the costs of storage have fallen dramatically.

Redundancy

Next, you need to plan for redundancy. What happens if you backup fails? An on-premise server can instantly restore lost or corrupt data to the local network, but not if the building burns down, floods or collapses due to an earthquake. Then you will be glad of your Cloud backup. It means you can find a temporary office, recover your data and be back in business.

Compliance

You will certainly want to think about your legal and regulatory obligations around data storage, backup and recovery. Highly regulated industries, for example, have rules around data handling, retention, disposal and auditing. Not all data is created equal, so you might want to adopt different backup and retention policies for business critical and non-critical data.

Remote Workers

Over 30% of a company's data resides locally, on PCs, laptops and mobile devices. However, laptops are vulnerable to theft, damage, human error, mechanical failure and malware. Adopting an automated, secure Cloud backup ensures the integrity of your data, wherever it resides, even outside the corporate firewall, making it the perfect solution for remote workers.

Cloud-to-Cloud

Finally, some firms rely heavily on Cloud-based applications such as Office 365 and Salesforce. Certainly, these services are highly resilient and secure. However, many Cloud-based applications have limited data retention periods, which is no good if you are a regulated industry that must retain every email and document for 7 years. Some vendors offer very limited liability when it comes to compensating you for lost, stolen or corrupt data. Only you know the true value of your data to your business. Of course, having all your data reside with one vendor gives them a lot of power and makes it harder for you to go elsewhere. Having a backup gives you some leverage, and makes migrating to another service easier.

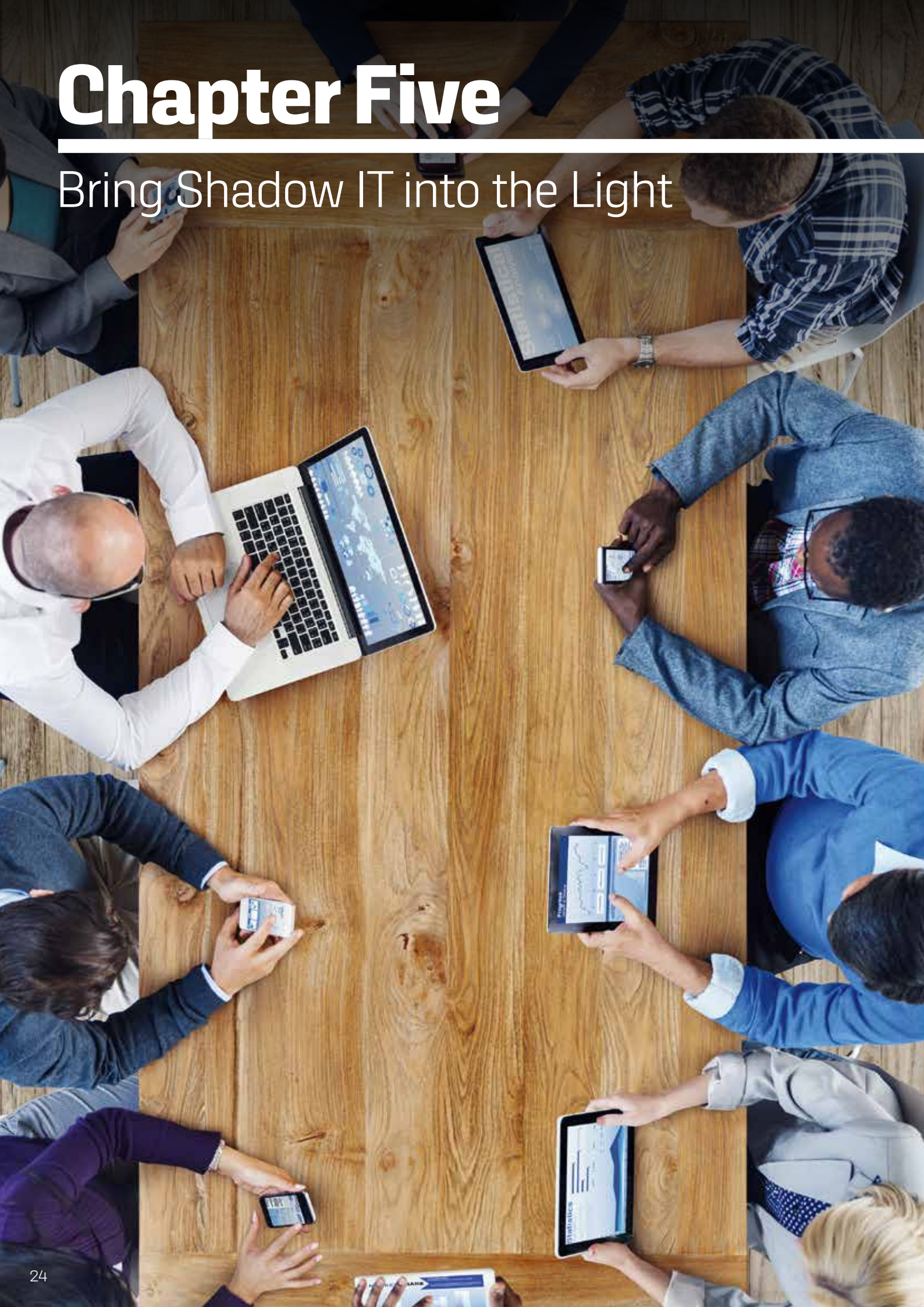
The reputational and financial cost of a high-profile cybersecurity or data breach can be immense. A study by the British Chambers of Commerce found that 93% of businesses that suffered a data loss for 10 days or more filed for bankruptcy within a year. Half of them went out of business almost immediately. At Modern Networks, we understand the importance of having a secure, fully integrated data backup, storage and recovery strategy. We are always happy to discuss your business needs, provide expert advice and practical solutions.

Top Tips

1. Have a clear backup and recovery strategy.
2. Keep multiple copies of your data.
3. Backup frequently.

Chapter Five

Bring Shadow IT into the Light



We've all done it, used our personal email, a popular file sharing app or something similar to get the job done. In fact, around 80% of employees admit to using unapproved, often unsecured software applications for work purposes. On the other hand, only 8% of organisations have any idea what shadow IT applications staff are using. Shadow or stealth IT might sound a little creepy or threatening, but in reality it's just a catchall term for any application not officially sanctioned for use by your organisation.

Cyber Threats

The problem is that every time someone uses an unsanctioned application to get something done, it exposes your organisation to cybercrime and accidental data loss. Of course, work completed using shadow applications might not be compatible with internal systems, and valuable data cannot be backed up or recovered if it never resides on your network in the first place. By 2020, Gartner predicts that a third of all successful cyberattacks will be achieved via shadow IT resources.

The more technologies we all use in our work and everyday lives the greater the risks. According to a report by the UK's National Cyber Security Centre, a range of fake business-enabling mobile apps appeared in 2016 designed to steal users' login credentials. Cybercriminals have also started to exploit social media sites knowing that many employees regularly check Facebook and Twitter feeds throughout the day, and especially at lunchtime, using company devices. Clicking a link on a hilarious cat video while at work can prove just as damaging as opening a malicious email.

The IT Bypass

Shadow IT has become something of a double-edged sword for many organisations and IT departments. After all, shadow applications clearly meet important business needs otherwise they wouldn't be so widely used. However, the IT department simply cannot do its job if it's bypassed and left in the dark about what applications people are using. Most employees adopt shadow applications without considering the security risks or compliance issues. When data resides on a third party application, outside of the knowledge or control of an organisation's IT department, it is quite clearly at risk. Ignorance is no defence when sensitive client or personal data leaks out of your organisation and ends up on the Dark Web for sale. Failing to meet regulatory obligations about how sensitive data is handled, stored and shared can lead to prosecution, big fines and negative publicity.

Let's get Visible

There is no-one-size-fits-all solution to the shadow IT conundrum. However, a pretty good place to start is visibility. How can you manage anything if you're in the dark about what Cloud applications are being used in your organisation? A small business with extremely limited IT resources might simply ask employees and departments what applications they are using. You might not get a completely truthful answer, but it's a start. Medium and larger firms might look at a Cloud access security broker (CASB) such as Cisco Cloudlock. Essentially, a CASB sits between an organisation's IT infrastructure and the Cloud service providers. It then enables you to see which Cloud applications people use, and any data being transferred or shared. What's more, CASBs can provide risk assessments of the apps used. The organisation can then define rules, procedures and restrictions to ensure data compliance and security. Similarly, data loss prevention (DLP) solutions like Cisco Stealthwatch give you complete visibility of your entire network out to the Cloud, and provide valuable insights and early detection of security vulnerabilities and potential threats.

Greater User Awareness

For many organisations, BYOD, a more agile, mobile workforce and cheap, instantly accessible Cloud applications have been a godsend. The downside is a greater "attack surface" for you to defend and others to exploit. Alongside the high-tech solutions, better user education and situational awareness is critically important to reduce the likelihood of data breaches and cyberattacks. IT security procedures and policy documents are no good to anyone sitting on the company server, lost and forgotten. The UK's National Cyber Security Centre suggests, "Giving the right user training and awareness interventions at the right times can help prevent security compromises. An organisation's staff can be one of its most effective defences, yet for many businesses a lack of user-centred security design is leaving them vulnerable."

Crime Report

Lastly, reporting cybercrime and data breaches is vital to identifying vulnerabilities and combatting threats. A survey by Barclays Bank and Institute of Directors (IoD) found that nearly ¾ of data breaches and cyberattacks go unreported by business. Clearly, the fear of a hefty fine from the Information Commissioner's Office (ICO), which has the power to impose monetary penalties of up to £500,000 for breaches of the UK Data Protection Act, is one deterrent to reporting. However, many firms do not report breaches simply because there was no material loss or damage caused. Nevertheless, those same firms spend more time and money on improving cybersecurity. Of course, bad publicity and potential loss of business is a powerful deterrent to reporting.

GDPR and NISD

The European Union's General Data Protection Regulations (EU GDPR) comes into force on May 25th 2018. GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected. That means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Penalties for those failing to meet the new requirements are extremely severe. Similarly, the Network and Information Security Directive (NISD) focuses on protecting critical IT infrastructure across European states. Those businesses that the directive categorises as essential services, such as utilities, air transport, banking and some Cloud services will have to comply, meet all security requirements and report incidents to the appropriate authorities. The UK will adopt these new regulations regardless of its decision to leave the EU.

Learn more about GDPR in the next chapter.

Into the Light

Shadow IT is an opportunity and a threat to most businesses. Overstretched, under resourced IT departments often struggle to meet the many, varied demands of today's tech savvy workers. Corporate governance has often been woefully inadequate in its understanding and response to the widespread adoption of shadow applications. The security risks aside, shadow IT clearly offers tools and technologies that make people more productive, collaborative and efficient. Organisations must make more of an effort to educate users about the dangers and benefits of using shadow applications for work purposes. Similarly, staff must accept a greater burden of responsibility for the applications they use to get the job done.

Top Tips

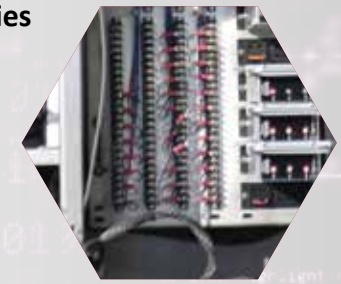
1. To better manage your network and data, first, you need visibility of who and what are accessing your systems.

2. Technology can help you better manage your network, but don't forget processes and people are just as important in maintaining data security.

3. The laws on data protection are getting much tougher. The consequences of failing to comply with regulations, already severe, could put many more firms out of business.

Chapter Six

Cybersecurity and GDPR Readiness



Media hype around GDPR (General Data Protection Regulation) has produced considerably more heat than light. GDPR is the European Union's replacement for things like the UK's Data Protection Act (1998). The new regulations are set to come into effect in May 2018. All companies wishing to trade with the EU must be GDPR compliant. The UK will adopt GDPR regardless of its decision to leave the EU. The main driver behind GDPR is that current data protection legislation is no longer fit for purpose, having been written into law decades ago when digital technology was in its infancy.

Into the Unknown

Regardless of all the media and marketing hype, the truth is that we just don't know what the full implications of the new data protection legislation will be. Certainly, it is true that there are substantial penalties for non-compliance, but we still don't know how different European states or the UK will actually interpret various elements of the new regulations. Surely, no one will benefit from Draconian penalties and excessive red tape that stifles business activity and innovation.

Data Protection

In reality, GDPR isn't that much different from current data protection legislation. It's simply being brought up to date. The main personal data protection principles remain the same. Personal data should be:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection.

Individual Rights

Some of the new rights for individuals include the "right to be forgotten" and data portability (the right of individuals to obtain and reuse their personal data for their own purposes across different services). There will be new provisions to increase the protection of children's data such as parental consent for under sixteens wanting to sign-up for online services and a stronger "right to be forgotten". Under the new regulations, you must also be able to demonstrate compliance. That means clear processes, procedures and metadata management. The new legislation further distinguishes between general personal data (contact details) and sensitive data (medical records, religious beliefs and unique biometric identifiers, for example).

Naturally, the regulations require you keep personal data securely. However, the directive is not specific or prescriptive about how you secure the data you hold. Data controllers must report personal data breaches to their supervisory authority and, in some cases, the affected individuals. This must be done within 72 hours where feasible.

The Information Commissioner's Office (ICO) provides plenty of information on what steps you can take now to prepare for GDPR compliance. Visit the ICO's website for their handy 12-step checklist.

Cybercrime

Today, all organisations should consider themselves targets of cybercrime. No one is immune. The new regulations build on what is required by existing data protection legislation. Firstly, you should take appropriate organisational and technical measures to protect your systems and the data that resides on them. Although not a mandatory obligation, it is recommended that personal data is always encrypted.

Your IT systems should be secure, resilient and backed up. In the event of a physical or technical incident, you should be able to recover all personal data records in a timely manner. You should also have a process in place to regularly check the effectiveness of your data security. As well as meeting new obligations on data breach reporting, organisations must keep their own internal records of all data breaches and similar incidents.
All scaremongering aside, the truth is that having an IT security strategy in place will help mitigate the risks from cybercrime while ensuring you meet many of your data protection obligations.

User Awareness

Firstly, as we have already seen, the majority of data breaches are caused by human error, not technical failings. It is important that everyone across your organisation is aware of cybersecurity threats, and assumes their share of the responsibility to keep your corporate data safe. Your staff should be properly educated about risk mitigation through good practices and procedures.

See chapter one for more information on user awareness and training.

Cybersecurity Audit

Next, you'll want to determine the current state of your cybersecurity and define where you need it to be. This process can be broken down into policy, employee and technical assessments. You will probably find a mix of easily fixed vulnerabilities and those that will require a more planned, long-term response. Naturally, any business critical operations assessed as vulnerable should take priority in your remediation plan.

Constant Monitoring

Running a cybersecurity audit gives you a snapshot of your strengths and vulnerabilities. However, once you've conducted the remedial work necessary to close any identified gaps, you still have work to do. The cybersecurity landscape is constantly changing and new threats emerge all the time. Subsequently, you will need to establish a regime of constant monitoring.

According to the National Cyber Security Centre (NCSC), "Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements." The NCSC provides a 10-step checklist for cybersecurity monitoring.

For more information on IT network and cybersecurity assessments:

Contact us now – 01462 426 500

Remediation

Unfortunately, you can take every conceivable precaution and still be the victim of cybercrime, so it will pay you to be prepared should the worst happen. It's important you have the right skills and technical resources to quickly identify, isolate and deal with threats while minimising their impact on your business operations. Building resilience into your systems, ensuring business critical data is backed up and establishing a coherent disaster recovery plan will make a significant difference to your organisation's survivability after a cyberattack.

Plan for the Worst

Currently, no one knows exactly how the UK or European states will choose to interpret or enforce GDPR. There is a wealth of free advice and guidance available from the UK government and its various agencies to help you comply with the new regulations. Certainly, it makes good business sense to take every precaution to safeguard your corporate data from accidental or malicious breaches, and have contingency plans in place should an incident happen.

Cyber Essentials

The UK government has a Cyber Essentials scheme that you can refer to in order to help address important cybersecurity concerns. You can use this as the foundation stage of your cybersecurity strategy before looking at the finer details. Once completed you can then self-certify for Cyber Essentials.

See: UK government's 10-steps to Cybersecurity

Top Tips

1. GDPR becomes law across the EU including the UK in May, 2018.
2. Main personal data protection principles remain the same as Data Protection Act (1998) with some new additions such as right to be forgotten, data portability and child protection.
3. Having an IT security strategy in place will help mitigate the risks from cybercrime while helping you meet many of your data protection obligations.

Chapter Seven

Anti-virus Endpoint Security

The number and variety of cyberattack faced by organisations continues to grow daily. Businesses of all sizes and across all industries are being targeted. To compound the problem, the attack surface is becoming greater and more varied with the proliferation of mobile devices, Cloud services and BYOD. This is creating a major headache for security professionals trying to counter this growing threat.

Ransomware

The enormous global press coverage of recent ransomware attacks put cybersecurity front of mind for many organisations. The term "ransomware" was probably new to many people until May 2017. However, ransomware is not a new issue, but is a multi-billion dollar problem.

Damaging Fallout

Besides the immediate monetary loss, the longer-term fallout from a malware attack can be devastating. There's the public relations nightmare and reputational damage done to the brand. Other consequences include regulatory compliance issues, legal action, operational disruption, lost customers, cancelled contracts, raised insurance premiums and difficulty obtaining credit. In a 2017 global study, over 30% of firms reported a loss of revenue and nearly 25% lost customers as a result of a data breach.

Think Data Breach

Unfortunately, there is no such thing as 100% security. However, you can take precautions and safeguards to protect your data, reduce the likelihood of being a victim of an attack, and ensure you can recover quickly should the worst happen. Many CIOs now think in terms of when will our organisation suffer a breach, and how will we respond to minimise the impact. Although there is no silver bullet of data protection, you can take a number of precautions. In the remainder of this chapter we will look at anti-virus as a crucial piece of your security puzzle.

Security at the Endpoint

So why is anti-virus important? Anti-virus is a key component of endpoint protection and is used to prevent, detect and remove malicious software. It helps protect against a variety of attacks including viruses, ransomware, Trojans, worms and many other types of attacks. If you don't have anti-virus software deployed across all of your devices we recommend you address this immediately.

Question the Status Quo

If you already have anti-virus, it is still worth asking the question: does it give your organisation the right level of protection you need? Do you regularly audit your systems to ensure that all your endpoints (PCs, tablets and mobiles) have anti-virus software installed, and are they running the latest definitions? This is a critical point, as many organisations deploy anti-virus software as a 'set and forget' solution but fail to monitor the endpoints and ensure they are continually protected.

Do you need an IT network and security assessment? We're here to help.

Contact us now – 01462 426 500

Central Administration

It is crucial that you choose a solution that can be centrally managed by an administrator. Anti-virus providers regularly release new updates for new threats as they are detected. If your software isn't centrally managed or requires the user to update the software 'at their convenience' it may not happen at all, and leave your network vulnerable.

Does Your Anti-virus Measure Up?

Secondly, how does your anti-virus score in independent tests? Organisations such as PassMark carry out independent testing of anti-virus solutions covering a range of areas such as reliability, usability, detection and performance. If your solution doesn't score well in these tests you should reconsider its suitability for your organisation.

Inexpensive but Vital

Anti-virus doesn't need to be an expensive solution but is a key component of your security strategy. The costs can be as little as a couple of pounds per user per month with flexible plans and options to suit most businesses. The key is to have the right level and type of protection that's appropriate for your business and the data you hold.

Top Tips

1. Choose an anti-virus solution that's been independently tested.
2. Choose an anti-virus that can be centrally managed.
3. Choose your anti-virus based on business needs.

Chapter Eight

Advanced Solutions

In this chapter, we will look at a range of solutions designed to safeguard your network from infiltration and detect any malicious software that is present. Cybercrime is a multi-billion dollar business. This means attackers are very well funded, and will continue to produce better, more disruptive malware and viruses. FBI research has found a single ransomware campaign can generate $60 million annually. Capable of generating massive profits for the cyber criminals, ransomware and other forms of cybercrime are with us for years to come.

Umbrella Roaming

Umbrella Roaming is a Cloud delivered service that protects all your employees' devices, even when they are not connected to your network. It works by blocking user requests to malicious domains at the Internet DNS layer, which means a connection is never made.

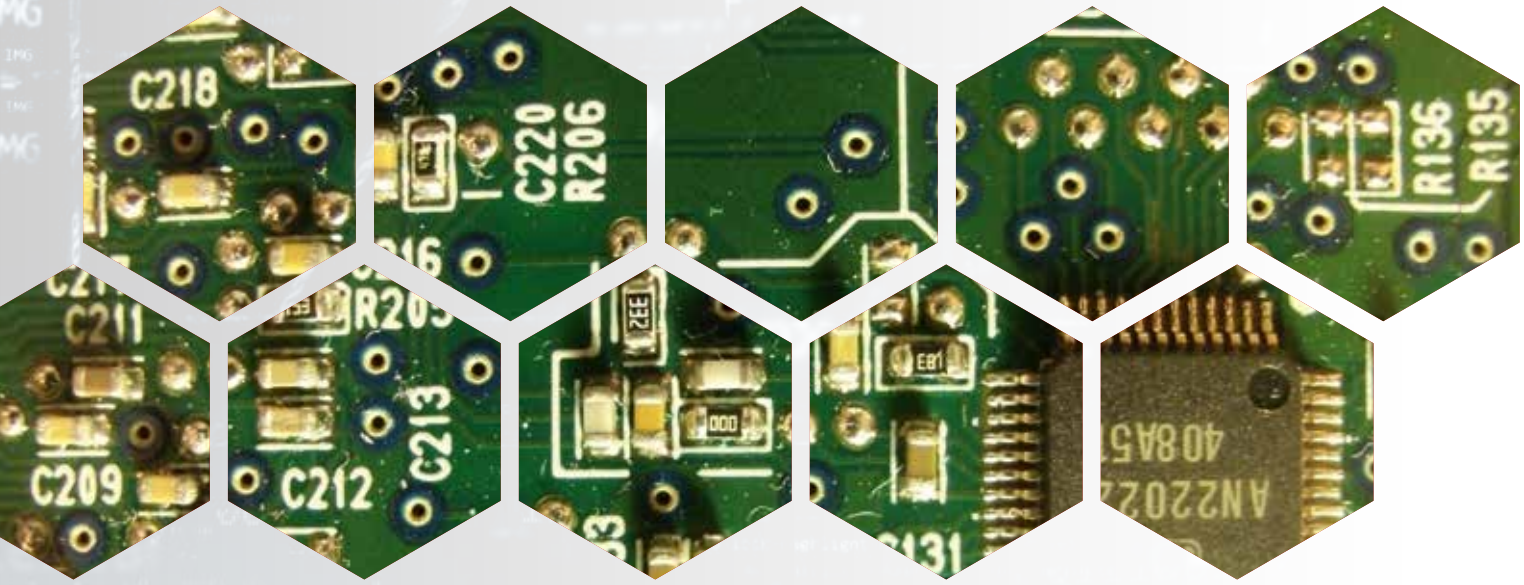
Umbrella Roaming constantly analyses real-time, diverse data sets to learn Internet activity patterns. It then uses machine learning and complex algorithms to spot trends, patterns and threats before an attack even happens. Because Umbrella Roaming is a Cloud delivered service, it is completely device and platform agnostic, and can eliminate potential blind spots when users are not in the office.

Currently, if users are working remotely without a VPN connection the perimeter security such as a firewall is being bypassed. Umbrella Roaming ensures every device gets the same level of corporate protection regardless of where your employees are based, working from home, in the office or at a motorway services.

ISE Potential Threats

Do you have complete visibility of all the devices connecting to your network? Do you know if all those devices are security compliant and only running approved applications? Identity Services Engine (ISE) is an application that enables you to better manage and secure your corporate network. ISE includes a posture service allowing you to check and verify the state of all devices connecting to your network before granting them access.

Working across both wired and wireless, corporate and guest networks you can control the devices connecting, and make sure they meet your specified criteria for access. For example, what operating system is a device running? Is it patched sufficiently? Does it have enterprise anti-virus installed and is it up to date? If not, you can quarantine the device, and give the user limited or no access until they have addressed the problem. This can significantly increase your level of control over devices that have the potential to threaten or infect your network.



Before, During and After an Attack

Advanced Malware Protection (AMP) for endpoints provides protection against the most advanced cyberattacks, will prevent breaches and block malware at the point of entry. It will also rapidly detect, contain, and remediate advanced threats if they evade front-line defences, such as firewalls, and get inside your network. As we have said in previous chapters, no prevention method will catch every threat. However, AMP will help you be prepared when advanced malware does get inside. AMP enables you to see executable file activity across all of your endpoints, so you can spot threats quickly and fix them.

One area where AMP differs from other solutions is it continues to monitor and record activity after a file is on the endpoint. It continues to watch, analyse and record file activity, regardless of the file's disposition. When malicious behaviour is detected, AMP shows you the recorded history of the malware's behaviour over time: where it came from, where it's been, and what it's doing. The malicious file is then quarantined automatically, any damage done is fixed and further harm prevented across all endpoints on your network.

Threats You Cannot See

On average, malware goes undetected for around 200 days. That's 200 days cybercriminals are inside your corporate network doing harm. To even the playing field, Stealthwatch uses flow data to give you incredible visibility across your entire network including the data centre and Cloud. First, it establishes a baseline for normal network behaviour. Next, it uses advanced analytics to identify unusual patterns and alert you of possible threats.

Stealthwatch can help you spot a compromised device talking to an external command and control server, detect abnormal traffic and identify data exfiltration, if unusual file transfers are taking place. Without an application like Stealthwatch, the first time you learn there's been a data breach is when your customers' data goes on sale or is splashed across social media.

Choose Wisely

These are just a handful of advanced cybersecurity solutions available to you. They vary in complexity and costs. Naturally, we would recommend you evaluate your current levels of protection; check they are adequate for your needs and compliant with your industry standards. However, before you rush out and spend a shed load of cash because the Board have been reading the newspapers; take a moment to consider your security needs and options.

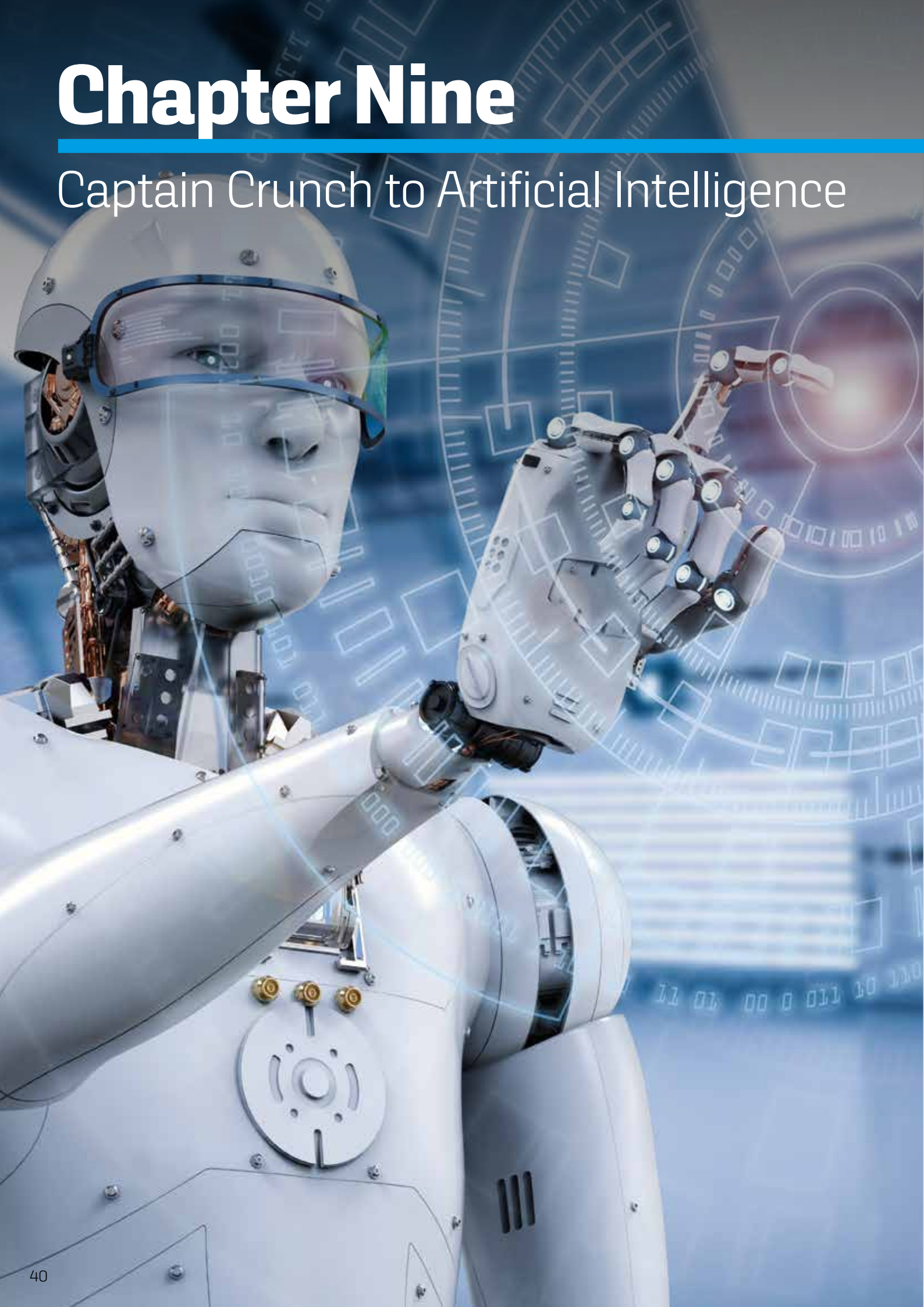
First, you need to agree what are your security priorities. Next, shortlist vendors and applications that meet your requirements now and for the near future. Get some independent advice and look at what existing customers have to say about applications. Look at total cost of ownership (TCO) and any hidden fees. You will also want to think about support and service levels. Take the applications out for a test drive, and give your IT people a chance to look under the bonnet.

Top Tips

1. Assess your current IT network security.
2. Agree security priorities.
3. Evaluate different applications based on your needs, budget, TCO before purchasing.

Chapter Nine

Captain Crunch to Artificial Intelligence



Back in 1971, the makers of Cap'n Crunch breakfast cereal had no idea what they had done when they included a seemingly harmless toy whistle in every box as a promotional gift. Just one of many people who enjoyed a bowl of Cap'n Crunch cereal was a young computer enthusiast named John Draper. John found that the Cap'n Crunch toy whistle produced exactly the same 2600-hertz audio tone needed to open a telephone line and allowed him to make free long-distance calls. Nicknamed "Captain Crunch", John had successfully hacked the US telephone system. John went onto share his discovery with two enterprising Berkeley college students, who saw a business opportunity in being able to hack the telephone network and make free calls. Sometime later, the two Berkeley students, Steve Jobs and Steve Wozniak, would go onto found a little computer company called Apple.

The Greatest Threat to Business

Since that fateful morning back in 1971, when John Draper found a toy whistle in a box of breakfast cereal, computer hacking and cybercrime have become one of the world's most serious problems. Forbes estimates that cybercrime will cost businesses in excess of $2 trillion USD by 2019. Multinational technology giant, IBM's Chairman, CEO and President, Ginni Rometty, recently said, "Cybercrime may be the greatest threat to every company in the world." Of course, the damage done by cybercrime goes far beyond the business community. It threatens international peace, democracy, individual privacy, health and public safety. Just as the problem of cybercrime has grown and mutated, so have the motivations of the cybercriminals. Certainly, political activism, espionage and terrorism remain key motivators. However, cybercrime for profit has seen the most dramatic increase in recent years. Organised criminal gangs now run sophisticated crime-as-a-service operations while ransomware attacks have roughly tripled in frequency year-on-year.

Open Doors

Our every increasing dependence on digital technologies and poor digital hygiene have created the perfect storm of cybercrime. Weak password policies, leaving ex-employees on your Active Directory, failing to patch or replace for known vulnerabilities, using shadowy IT applications for business purposes, and opening suspicious emails and text messages are some of the most common reasons businesses and individuals fall victim to cybercrime. These are crimes of opportunity, like leaving the doors and windows of your building wide-open.

Simple Solutions

Creating, communicating and enforcing some simple, common sense IT security policies could save you a world of pain. Disable and then remove dormant user accounts from your Active Directory after 30 days. Once manufacturers stop producing critical security updates for end of life hardware and software, you need to replace it. You keep it running at your own peril. The majority of data breaches are the result of human error such as losing paperwork, emailing data to the wrong person, mistakenly uploading confidential or sensitive information to public websites, gossiping and being indiscreet on social media. A lot of this stuff might seem trivial, but brute force attacks, ransomware and spyware are successful because people use weak passwords and don't patch or replace their systems when they're clearly vulnerable.

As our computer networks become more complex, dispersed and interconnected so the attack surface grows proportionally. Every smart device you hook-up to your network represents an opportunity and a threat. The environmental sensors that control your eco-friendly building, for example, might be just the gap in your IT security perimeter that a hacker has been waiting to exploit. A recent survey by the Electrical Contractors' Association (ECA) and Scottish electrical trade body SELECT found that some four in ten smart buildings in the UK do not currently take any steps to counter cyber threats. To take maximum advantage of mobility, big data or the Internet-of-things (IoT) requires you have a network infrastructure that's resilient, scalable and secure.

Robots

There will be tens of billions of connected devices jostling for bandwidth by 2020. Keeping tabs on all those devices will be no easy task, let alone ensuring they're secure. Predicting the future is a notoriously tricky task. For decades, robotics and artificial intelligence (AI) have been the stuff of science fiction and horror movies. However, today we are seeing the first widespread and successful use of these technologies. We see robots deployed in manufacturing, logistics, utilities, scientific research, law enforcement and the military. Primarily used to offer help and advice, chatbots are deployed everywhere from social networks and ecommerce websites to call centres, banks and healthcare providers. Online giants Amazon and Netflix use sophisticated, self-learning systems to study the shopping and viewing habits of their customers, so they can better serve them.

AI, machine learning (ML) and quantum computing offer the possibility of cybersecurity systems capable of identifying threats the moment they emerge anywhere in the world. Automatous systems that can anticipate a cybercriminal's next move based on previous behaviours, and take action without any human intervention. Similarly, cybercriminals will probably harness AI-based technologies to launch sophisticated attack agents designed to avoid detection and adapt to changing defence strategies.

Ajay Arora, CEO and Co-founder of data security firm Vera suggests, "We need to adopt intelligent and automated security systems. Automation means investing in tools that automatically secure data based on location, context, the recipient, the user's identity, and more importantly, tools that don't require constant human interaction. We simply cannot rely on employees or our partners to do the right thing."

The Spread of IoT

IoT devices are expected to spread faster than smartphones and tablets once did. Given the diversity of operating systems, absence of security features and lack of regulation for these devices, we may see large-scale cyberattacks against businesses and consumers. As always, regulation will probably follow in the wake of a series of damaging, high profile incidents. According to McAfee Labs 2017 Threats Predictions Report, "Internet of Things malware will open a backdoor into connected buildings and could remain undetected for years. There should be no doubt that networks of devices infected with malware without their users' knowledge will be one of the most common cybercrimes in years to come."

No Simple Answers

The cyber-threat landscape continues to evolve, and no one security vendor can or will offer a complete solution to the problem. Instead, organisations will have to work with security consultants and trusted partners such as Modern Networks to combine best-of-breed solutions to meet their own unique set of requirements, challenges and risks. Today, successfully changing employee attitudes and indifference towards cybersecurity will go a long way to preventing many accidental data breaches, phishing and other social engineering attacks.

The anticipated spread of smart, connected devices into every conceivable part of our work and home lives will certainly pose major security challenges. A requirement of the new European General Data Protection Regulation (GDPR) is data security by design. In other words, manufacturers and software developers must build data security features into their products. This particular GDPR obligation might prove an important weapon in the ongoing fight against cybercrime in years to come.

Top Tips

1. The war of cybersecurity versus cybercrime has only just started and will only intensify.
2. Create, communicate and enforce simple, common sense IT security policies, and adopt defence in depth approach to network security and data protection.
3. The majority of cybercrimes remain crimes of opportunity. You can mitigate many of these risks by taking simple remedial actions, such as patching known vulnerabilities, and raising user awareness.

Summary

Cybercrime is an unpleasant fact and daily occurrence. However, many organisations continue to ignore the new reality and take inadequate precautions to protect themselves or their customers. Subsequently, private and public sector organisations continue to find their names splashed across the media because of embarrassing data breaches or successful system hacks.

Tremendous Cost of Cybercrime

Around 60% of smaller businesses will cease trading within six months of a data breach or cyberattack due to the financial burden and reputational damage. The costs of cybercrime can be tremendous in terms of financial penalties, negative publicity, lost customers, downtime and higher insurance premiums. Nevertheless, the majority of data breaches can be attributed to human error or staff negligence. Similarly, over 70% of cyberattacks exploit known, patchable vulnerabilities.

In order for organisations to get a better grip on network security and data protection, they need to think about three things: people, processes and then solutions.

People, Processes, Solutions

Organisations need to change the employee mindset, so cybersecurity is at the forefront of their thinking rather than a distant afterthought. That means user awareness training and communications programmes. Organisations also need to review processes and procedures to ensure they are fit for purpose. Have you identified and prioritised your security assets, such as personal customer data? Have you done any threat modelling? Next, audit your IT network to identify vulnerabilities. Develop a remediation plan to improve security where it matters most. Evaluate different solutions that can provide you with a defence in depth.

Backup

Unfortunately, there is no such thing as complete cybersecurity. Should the worse happen, and you are the victim of a cyberattack or data breach, it's critically important you have a reliable backup and recovery plan that can swing into action.

Regulation

The full implications of new EU data protection legislation remain to be seen, but promise to be far more stringent in certain areas, such as right to be forgotten, data portability and breach reporting. Having a coherent IT security strategy will help mitigate risks and ensure you meet many of your data protection obligations.

Brave New World

The Internet of Things and proliferation of connected devices will almost certainly dictate the future of network security. The more interconnected devices, the more potential entry points for hackers and malicious applications to exploit. The brave new world of artificial intelligence, machine learning and quantum computing promises many new user benefits, business opportunities and asymmetric threats.

Every human activity comes with some level of risk. Good networks security can help mitigate many of the risks associated with doing business, ensure regulatory compliance, reduce liabilities and protect an organisation's reputation.

About Modern Networks

Established in 1999, Modern Networks is an IT and telecoms managed service provider (MSP) helping clients across the UK maximise the value of their entire IT infrastructure. The company has offices in Hertfordshire, Cambridgeshire and Manchester. We have considerable expertise within commercial property management working with over thirty managing agents and a thousand sites. Our clients include CBRE, Cushman and Wakefield, Savills, JLL and Lee Baron. We are a corporate member of the British Institute of Facilities Management (BIFM). We are also a Gold member of the Service Desk Institute and offer ITIL best practice standards of IT support.

Enterprise

Modern Networks provides advanced, innovative IT managed solutions for over 200 varied enterprise clients from accountancy firms, travel agents and media companies to national charities and not-for-profits. The company is a certified partner for Cisco, HP, Microsoft, VMware, NetApp and Pure.

RADD Telecoms

Our sister company, RADD Telecoms is one of the UK's leading data cabling installers. They also provide business WiFi, CCTV and secure access control systems.

Our range of IT and telecoms services include:

Our other services include:

- IT consultancy, design and build.
- IT network and security assessments
- Competitively priced, fixed monthly fees
- Simple on-boarding process
- IT cabling, access control and CCTV
- Digital signage
- Business computers, tablets and mobiles
- Business email and software
- UK based IT support
- Wired and wireless computer networks
- Cyber security
- Data storage, backup and recovery
- Cloud computing
- Telephony, business Internet and broadband.

About the Author

Charlie Trumpess, DipM, MCIM, CM
Charlie is a marketing professional with over 20 year's experience working for a range of tech companies in the UK and Northern Europe. He holds a professional diploma in marketing (DipM), is a Member of the Chartered Institute of Marketing (MCIM) and a CIM Chartered Marketer (CM).

Contacts

Modern Networks, Hitchin
18 Knowl Piece
Wilbury Way
Hitchin, Herts
SG4 0TY
01462 426 500

Modern Networks, Manchester
20–21 Albert Square
Manchester
M2 5PE
0161 667 3100

www.modern-networks.co.uk

Company No. 3881576
VAT Reg. GB 750991117

Useful Web Links

- National Cyber Security Centre: **www.ncsc.gov.uk**
- GCHQ: **www.gchq.gov.uk**
- ActionFraud: **www.actionfraud.police.uk**
- UK Government: **www.gov.uk**
- Cyber Essentials: **www.cyberaware.gov.uk/cyberessentials**
- Information Commissioner's Office: **https://ico.org.uk**
- EU General Data Protection Regulation (GDPR): **www.eugdpr.org**

modern networks

modern-networks.co.uk

Email: **info@modern-networks.co.uk** Call: **01462 426 500**
18 Knowl Piece, Wilbury Way, Hitchin, Herts, SG4 OTY