Abtec

CYBER SECURITY: BEST PRACTICE GUIDE

A practical guide for how to keep the bad guys at bay without breaking the bank.

Introduction

The need for businesses to have strong cyber security has increased from being little more than an insurance policy to being of key strategic importance.

This change has been driven largely by the evolution of the threats now facing even small businesses. However, many government departments and an increasing number of private businesses are also now insisting on minimum standards across their supply chains. Organisations are now seeing that their security stance can directly impact their ability to win new business.

Demonstrating that your organisation takes security seriously is a valuable signal to customers. It could also provide a significant competitive advantage.

The current economic climate means that any any significant new investment is likely to need to demonstrate ROI, meaning security expenditure is likely to be at the back of the queue.

It would be great if security could become a one-size fits-all solution, but what works for one organisation is unlikely to be directly applicable to another.

So how do you ensure that your organisation is where it needs to be? And how do you level up to ensure your security stance keeps you safe, keeps clients' minds at rest, AND keep the finance team happy?

This document examines the practical steps you can take, divided into levels of cyber security 'maturity' and outlines areas where improvements can be made that make a measurable difference without incurring unnecessary cost.

Stage 1: Improve your security by using what you've got.

Cyber security can be overwhelming when you're starting with very little: The sheer number of products, the types of threats they claim to prevent, and the regulatory compliance issues you may face can leave you not knowing where to start. The good news is, just implementing the fundamentals of good security can enable your business to make a significant leap forward in its resilience.

Bringing some discipline to perhaps neglected processes can immediately ensure unseen vulnerabilities are fixed and that the "have a go" bad actor must work significantly harder to get into your systems. Make life difficult for a hacker, and many will simply move on to the next target.

So where DO you start?

A solid starting point is to create a regular checklist of activities that need to happen every month: ensuring that key devices, applications and user behaviors are reviewed, and any remedial action taken.

Step One: Password management

Possibly the simplest of all the security measures to implement, and yet one so often overlooked by organisations is simply insisting on your team using better password hygiene. Too often we see employees using the same handful of passwords across all their devices and accounts, and what's more using passwords which are far too easy to guess. What this means is, if an employee's Facebook account gets hacked, their problem can quickly become yours as the hacker uses those same compromised login details to access your systems.

Action: Train your employees on the importance of good password hygiene.
Action: Enforce strong passwords for employees.
Action: Use a corporate password manager.

Step Two: Firewalls

Essential gatekeepers to your internal network, it's important that you have firewalls in place, and they are configured correctly (including ensuring admin passwords are adequately secure). Ideally, you'll have boundary-level firewalls on your network, as well as additional software firewalls on individual connected devices. If you're running Microsoft Windows, you'll like have access to inclusive firewall protection. Make sure that this is turned on and regularly updated.

Action: Implementing a firewall on your network or take out a managed firewall solution from an IT solutions company.

Step Three: Configuration

Too often manufacturers of IT equipment provide devices with poor default security features: admin logins are often set as Admin / Password123 or similar. While that may save a few minutes during, initial set up, a worrying number of customers never change these settings, leaving them vulnerable to attack.

Action: Change any default admin logins to stronger ones.

Step Four: User Access Control

Managing user access is a key consideration of a robust security stance. While it's comforting to think that all our internal users are careful and trustworthy, it's a sad fact that most data breaches come from compromised user credentials, or users acting inappropriately.

Action: Review the user accounts on any networked devices in your company and delete any that are no longer needed. Set up a process of reviewing this regularly.
Action: Ensure that administrators set appropriate privileges so that only those who need access to sensitive information (customer data, financial information etc.) have access to it.

Step Five: Malware protection

Since the start of the pandemic, we have seen a significant increase in the frequency and complexity of Malware and, in particular ransomware attacks, usually delivered through malicious emails or websites.

"Grey" software, that which is downloaded to a device without admin's knowledge is a huge potential threat to security, and again has flourished post-pandemic as users have sought to find their own means to replicate in-office functionality at home.

Action: Introduce anti-malware software. Microsoft Windows already includes core anti-malware functionality as standard, scanning incoming emails and downloaded files.
Action: Restrict application downloads to pre-approved apps.
Action: Enforce admin approval for application downloads is an easy way to regain control.

Step Six: Patching

We've already spoken about securely configuring your new network devices and applications. But once configured, regular updates need to be installed to remain secure. In 2021, 37% of critical vulnerabilities in businesses' security came from outdated components. Most software and hardware vendors will regularly release updates for their products when vulnerabilities have been found, so failing to 'patch' is rather like leaving the back door unlocked.

Action: Introduce a schedule of checking for updates at least fortnightly – or if too onerous, outsource your patching to a third party.

The no/ low cost approach

You may have noticed that many of the above paragraphs refer to products and services you already have at your disposal. That means that with little to no cost, you can put your organisation on a solid security footing, and likely be in a far better place than many of your peers. Ultimately, at Abtec this is where we want all our clients to be at a minimum.

If you're at all unsure where to start, pick up the phone and chat to one of the team.

Cyber Essentials: making security a competitive advantage

Everything listed in this section aligns with the Government "Cyber Essentials" certification. This certification not only provides you with peace of mind that your security stance meets accepted standards, it also provides an increasingly important competitive advantage when winning new business.

Many organisations – and all Government departments – now insist on their suppliers having Cyber Essentials certification as a minimum. Without it, you're not even going to make a shortlist. And even for organisations who may not actively insist on certification, being able to demonstrate that you take security seriously is often a big tick in the box when it comes to winning prospects' confidence.

Stage 2: Build on what you've got

You may already feel that you've got the basics covered – and that's great, but if you think you need to take some additional precautions (and there's always something more you can do to make your business more secure) there are still plenty of cost-effective options. While some of these may need a little more hand holding from an experienced IT service provider, we're confident they still represent a great individual step up in your security provision.

Step One: Plan and identify your risks

Whatever your current security position, it's always worth having a questioning mindset. The pace of technological change and the activity of hackers means there is always a new threat, a new weakness found.

Creating a simple risk registry is a great way of staying on top of your IT assets, and enables you to build a picture of where weaknesses may lie.

This is not an afternoon's work: it will take time and Abtec can help with this, but it's money well spent in terms of understanding all your assets and your vulnerabilities.

Action: Create a risk registry, or contact Abtec to help you identify your risks and create this with you. For each device, think about how it could be compromised, and how to mitigate any weaknesses:

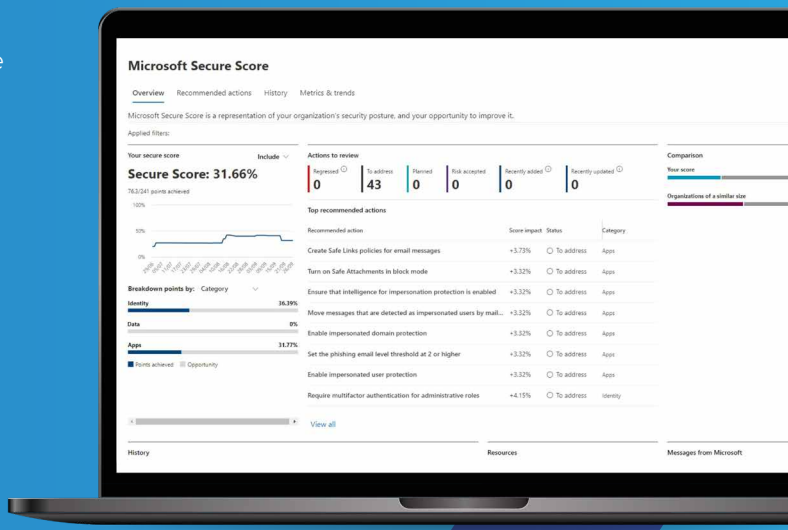
- ✓ Have any factory default passwords been changed?
- ✓ Unnecessary users removed?
- ✓ Is firmware and software up to date?
- ✓ Are inbuilt security features (such as BitLocker on Windows laptops, or the software firewall on your ISP's router) turned on and operating as they should?

Step Two: Microsoft 365 configuration

With a few exceptions, Microsoft 365 is ubiquitous in almost all businesses. And yet, it still surprises us just how few instances have really been set up correctly. In fact, MS365's simplicity is its greatest weakness: because it's so easy to get the basics up and running, it's easy for business owners to assume that everything's in hand. From ensuring logging settings are correctly configured, to putting appropriate back-up in place there are several straightforward configuration changes possible that turn your instance from a potential risk to a security stronghold.

Microsoft Secure Score is a great - and often overlooked - tool which can help you understand your best next steps across your applications, identity and data. It provides specific pointers as to areas where improvements can be made within Microsoft 365 to tighten up any current shortcomings. It's worth checking out within your MS365 admin dashboard.

Action: Explore the security administration area of your MS365 account. This can be a daunting task, however Abtec can help.



As a Tier One Microsoft Partner we can help you implement:

- **Multifactor Authentication**

An additional level of security which forces users to verify their identity through a secondary factor – such as one-time passcode, or biometric scan – on top of their standard password.

- **Conditional and privilege user access**

An intelligent feature which restricts user access based on observed behaviours (such as attempting a login from an overseas territory) or by role (e.g. restricting access to financial applications and data to the accounts team).

- **MS365 back-up**

While Microsoft will back up a small amount of data by default, it falls short of many businesses' regulatory requirements and carries no guarantee. It's worth checking that your data is backed up effectively and compliantly.

- **Microsoft Defender**

Often misunderstood as a 'basic' firewall, Defender is, in fact, so much more, providing a dashboard through which you can administer many of the key security requirements of your Windows endpoints (users' machines) as well as informing you of trending threats you may fall victim of, and monitoring suspicious activity across your network.

Step Three: Cloud email filtering

Beyond the inbuilt email security features of Office 365, you can further protect your employees and your assets by using a cloud email filtering service. Imagine these as a car wash for email; they scrub your inbound and outbound emails of spam, and malicious threats before they reach your users' devices or your mail server. These services are low cost, effective and always up-to-date on the latest threats, as there are teams of people updating the algorithms to protect your inbox 24/7.

Action: Talk to Abtec about your email filtering needs to protect your email communications.

Step Four: WIFI and network management

Network security is a complex topic as it covers so many different technologies and configuring all of these optimally can be a challenge. However, there are a number of steps to ensure that your wired and wireless networks within the business, and your devices accessing the network from outside its perimeter remain secure.

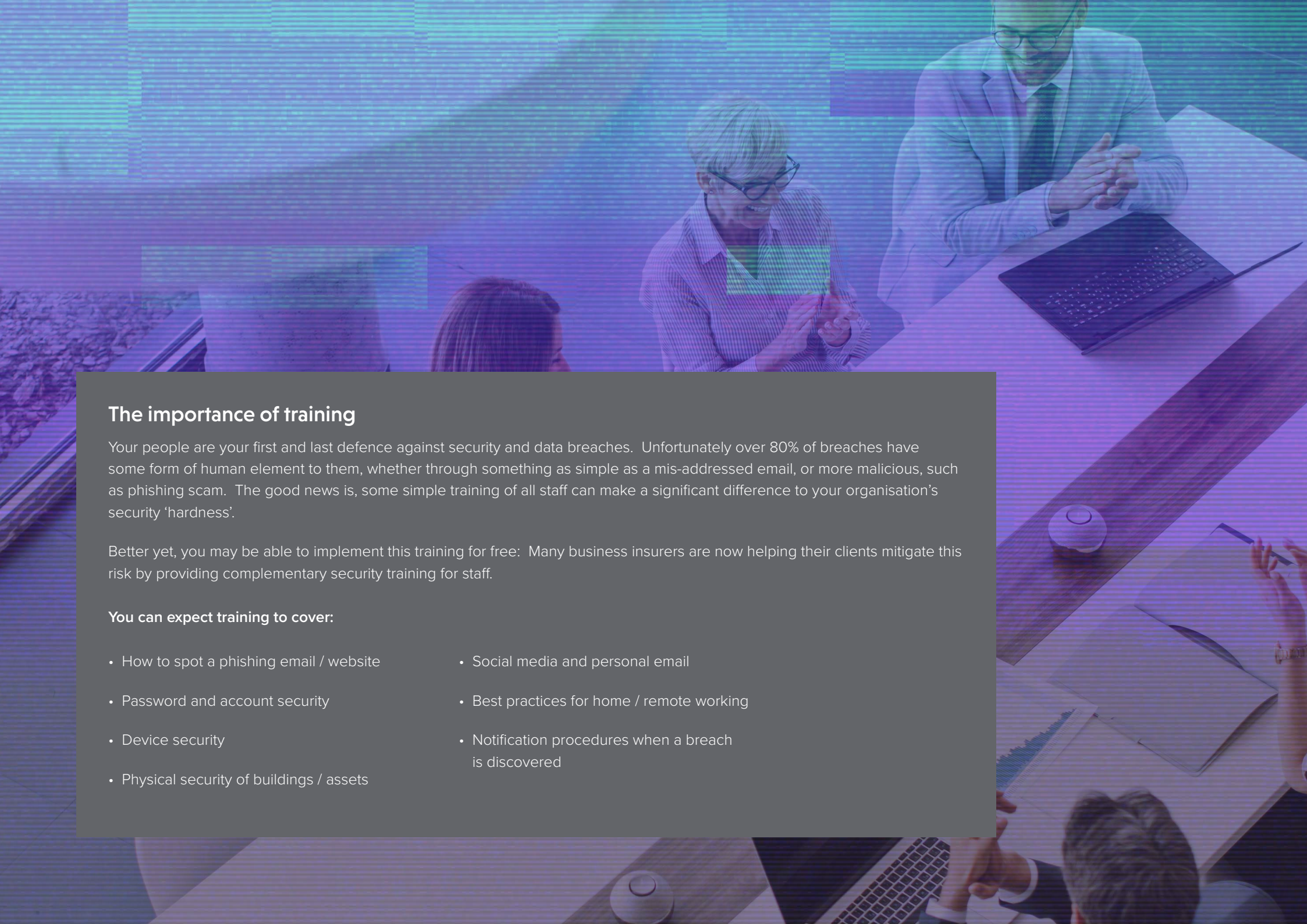
We've already spoken about access control, which is a key factor in ensuring basic network security by limiting any individual's scope, but we can take this to the next level with network segmentation: as the name suggests this means we can effectively ring-fence parts of the business on their own networks – allowing select users and applications across boundaries, but essentially preventing users of one network from ever gaining access to the others. This could be as simple as separating guest users in a hotel from the broader business network, or for segmenting a network for IoT devices from core business functions. A good example of this in practice is for organisations offering payment via PDQ card payments: Segmenting traffic from these devices onto its own secure network using password and MAC address protected Wi-Fi SSIDs not only spares staff and customers the pain of slow connections, it also ensures compliance with PCI-DSS standards.

Action: Talk to an Abtec advisor about the types of user accessing your network to get guidance on how to keep your network secure.

Compliance: Reassure your customers by meeting regulations

Customers value companies that look after their data and who take cyber security seriously. Compliance regulatory demands is a key part of showing that your security measures are top notch.

Implementing measures that protect, process and store your data in line with PCIDSS requirements, FSA/FCA regulations and GDPR is often more straightforward than it might seem and is business critical for any business falling under their remit.



The importance of training

Your people are your first and last defence against security and data breaches. Unfortunately over 80% of breaches have some form of human element to them, whether through something as simple as a mis-addressed email, or more malicious, such as phishing scam. The good news is, some simple training of all staff can make a significant difference to your organisation's security 'hardness'.

Better yet, you may be able to implement this training for free: Many business insurers are now helping their clients mitigate this risk by providing complementary security training for staff.

You can expect training to cover:

- How to spot a phishing email / website
- Password and account security
- Device security
- Physical security of buildings / assets
- Social media and personal email
- Best practices for home / remote working
- Notification procedures when a breach is discovered

Stage 3: Security as a Business Fundamental

If you've got this far and have still not found a means to improve your security stance, then you're already in a great place! By the time you reach stage three, security should have become a fundamental of your business operations: all staff (that's right – not just the IT department!) should recognise they have a role to play, and we are no in the realm of specific security software – and managed services – to take things to the next level.

At this stage, it's not unusual to want to bring in external help, in part to get expert opinion on where any undiscovered improvements might lie, but also, as security by now is likely to have become a significant resource drain, to help share the load – and risk - of security management. Key services performed at this level do now come with a price tag, but still can be cost effective if managed properly.

Step One: Full security audit

This is probably your next best step in understanding how and where to boost your security further. Stepping back and using third party tools to probe your network, penetration testing -perhaps even physical security tests – will provide often quite eye-opening insights into where opportunities for improvement will remain. A well conducted audit should be able to provide you with a list of improvement areas, and prioritise them based on severity, cost to fix etc.

Action: Talk to Abtec about arranging a security audit of your network.

Step Two: Dedicated email encryption

As we've seen, email is a key consideration for maintaining a strong security stance, as it is your organisation's main connection to the outside world. As such, it's also a potential gateway through which to deliver malicious programmes into your network, and exfiltrate information from it. We've seen that Microsoft 365 protects your business to an extent, but when you need to take additional precautions – perhaps because of the sensitive nature of data you handle, the profile of the clients you serve, or simply the size of your business, a dedicated tool may be the answer.

Action: Book a call with an Abtec advisor to run through your options.

Step Three: Outsourcing your security operations (Managed SIEM / SOC)

One popular way of mitigating an organisation's compliance responsibilities is by outsourcing your security operations to an external provider. Doing so has multiple advantages for the business and for the team:

- Unlike internal staff, outsourcing providers usually provide round-the -clock support. (it's no coincidence that most security breaches happen on weekends and public holidays).
- Managed Security operations take much of the pressure associated with security away from your core IT staff, leaving them to wok on higher value projects while your IT service provider takes on the burden of managing, triaging and investigating all those security alerts.
- Patching, device management, backups and more can all be managed around the clock, not "got around to".
- Your organisation is able to call on a dedicated team of security experts, and enterprise-level tech, with a wealth of up to date threat awareness. That means more attacks headed off at the curve, and any issues are remediated more quickly.

Action: Get in touch with us today to get detailed advice on how we can help manage your security.

We addressed backup for Microsoft 365 earlier in this document. That's an essential step in starting to safeguard your business from attack, but really is a first step to take to protect core office applications and data, but as your organisation grows, simply having a backup is the absolute minimum you need.

One of the biggest challenges with disaster recovery – particularly as your business grows - isn't the recovery of the data itself, but replicating the infrastructure configuration, applications and processes that enable business to restoration of business services. Having the right disaster recovery solution in place can make the difference between a restoration of service time being a matter of hours, or a matter of days – even weeks.

The 3-2-1 rule of Disaster Recovery

A simple rule of thumb when considering a full disaster recovery plan is the "3-2-1" rule, which essentially breaks down as follows:

3: You should be taking at least three copies of your data (and environment).

This ensures that, should your first back up fail, or be corrupted, you have an appropriate fall back.

2: These copies should be stored on at least two different media.

Keeping copies on a tape / disk as well as in the cloud reduces the risk associated with either format failing.

1: Keep one copy off site (or disconnected from your main digital network infrastructure).

In a physical disaster, such as a fire, if your production server and your backup are on the same premises, they are likely to suffer the same fate.

Equally, in a digital context, hackers or malware can detect backup locations within your network. 'Airgapping' – backing up to a disconnected, third party cloud environment (airgapped) keeps those backups away from harm.

About Abtec

Abtec helps organisations like yours maximise your use of technology to work smarter and more efficiently.

We are a group of specialist technology companies that focus on providing our clients with secure and agile IT infrastructure, technology-enabled smart buildings and a range of professional services to inject expertise and transfer knowledge.

That includes ensuring that you're able to make the best possible use of the software and tools already at your disposal. We also provide guidance on any additional technology solutions or services you need to keep your business and your business data secure.

For clients requiring outsourced IT security support, our team of experienced, highly qualified security specialists are on hand to provide managed a range of services from training through to managed SOC.

Established in 1991 and based in Leicestershire, we're trusted by SMEs across the country to support their business-critical infrastructure and applications. We work across sectors, including many heavily regulated industries where security compliance is paramount.

But we're more than simply faceless IT support: our relationships are built on forming true partnerships with our clients, that give them faith in the technologies underpinning and facilitating their business, its growth, and its security.

If you'd like to chat with us about any of the issues raised in this document, or just want to understand what your next steps might be to improve your security stance, please get in touch – we're always happy to help.

Email: **enquiry@abtecnet.com**

Tel: **01858 438 500**

Abtec