10 things every business owner should know about tech security

What's the point of this report?

Every day we see even quite big companies pay out for technology-related issues that they could have avoided. When that's a few pounds, it's probably not a big deal (although why spend money you don't need to?), but it's easy to overlook basic security and strategy when it comes to protecting your company data, equipment and people.

Security breaches and costly oversights are not only experienced by big organisations, even smaller companies can end up losing money or being in the position of shutting the stable door after the horse has already bolted. Don't let this be you!

Review each of these ten points in relation to your business. Think about what it would cost your business if you do nothing. Is it worth it? Make a conscious decision to put a preventive strategy in place, so your business is protected.

1: Cyber Security and Insurance

Cyber insurance has become essential for businesses of all sizes, yet many SMEs remain uninsured against digital threats. A cyber-attack can cost UK businesses an average of £4,200 per incident, with costs escalating dramatically for data breaches involving customer information. Recent high profile cases have hit the news headlines with costs running into millions – several banks, M&S, Jaguar LandRover and others. And not all were covered by cyber insurance.

Before purchasing cyber insurance, understand what's covered. Most policies include business interruption losses, data recovery costs, legal fees, and notification expenses following a breach. However, insurers increasingly require businesses to demonstrate robust security measures before providing cover. This means implementing multi-factor authentication, regular security updates, employee training, and documented incident response plans.

Don't wait until after an incident to discover coverage gaps. Many policies exclude ransomware payments or have specific requirements around backup frequencies. It's good practice to review your policy annually and ensure it aligns with your evolving business operations. Remember that insurance is your safety net, not your security strategy; prevention remains far more cost-effective than recovery.

Document all security measures you implement, as this evidence may be required during claims processing and can potentially reduce your premiums.

2: Phishing

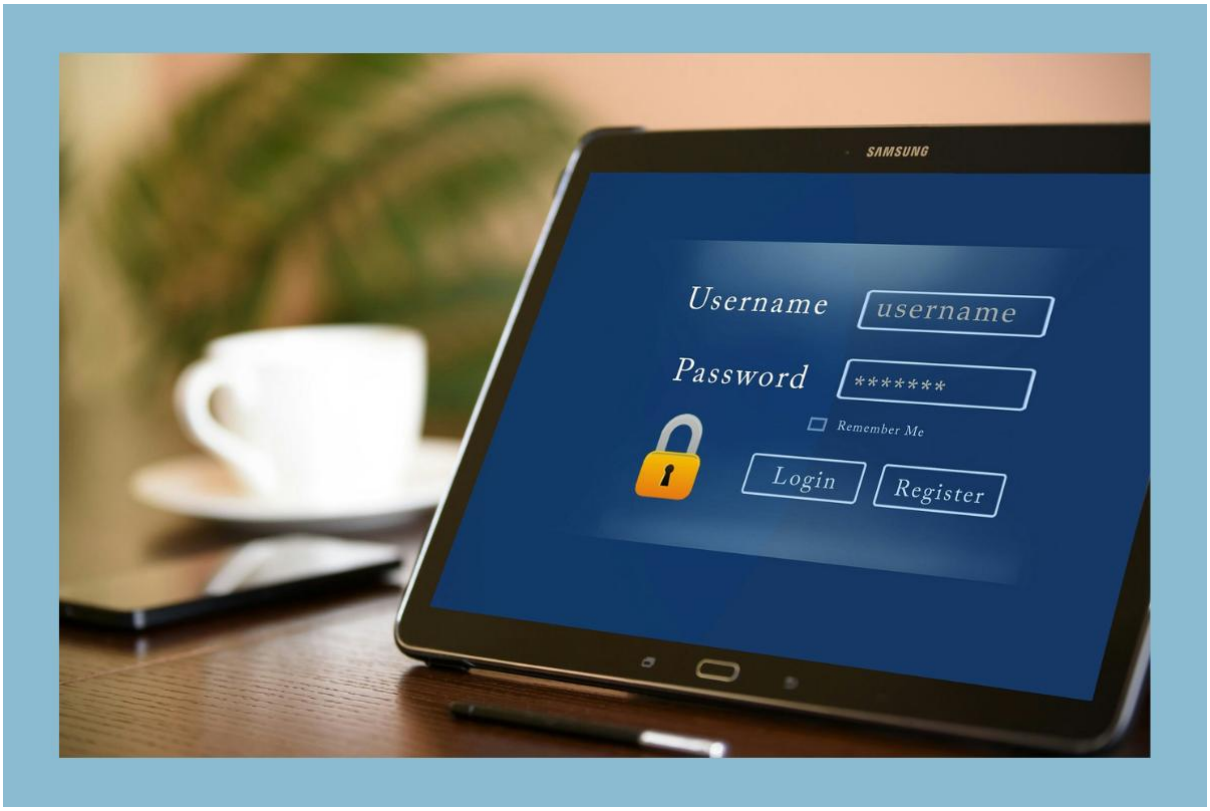
Phishing remains the most common entry point for cyber criminals, accounting for over 80% of reported security incidents. These deceptive emails, messages, or websites trick employees into revealing sensitive information or downloading malicious software. For SMEs, a single successful phishing attack can lead to devastating financial losses and reputational damage.

Modern phishing attacks have evolved beyond obvious spelling mistakes and suspicious links. Criminals now use sophisticated techniques including spear-phishing (targeted attacks using personal information) and business email compromise, where attackers impersonate senior executives to authorise fraudulent payments. These attacks can be incredibly convincing, often replicating legitimate communications perfectly.

Training your team to recognise phishing attempts is crucial. Teach them to verify unexpected requests through alternative communication channels, hover over links before clicking to reveal true destinations, and be suspicious of urgent requests for sensitive information or payments, or changes in bank account information. Implement a culture where employees feel comfortable questioning suspicious communications without fear of embarrassment.

Technical defences are equally important. Deploy email filtering solutions that identify and quarantine suspicious messages, implement SPF, DKIM, and DMARC protocols to prevent email spoofing, and ensure web browsers have anti-phishing features enabled. Regular simulated phishing tests can help identify vulnerable employees and reinforce training effectively.

3: Passwords



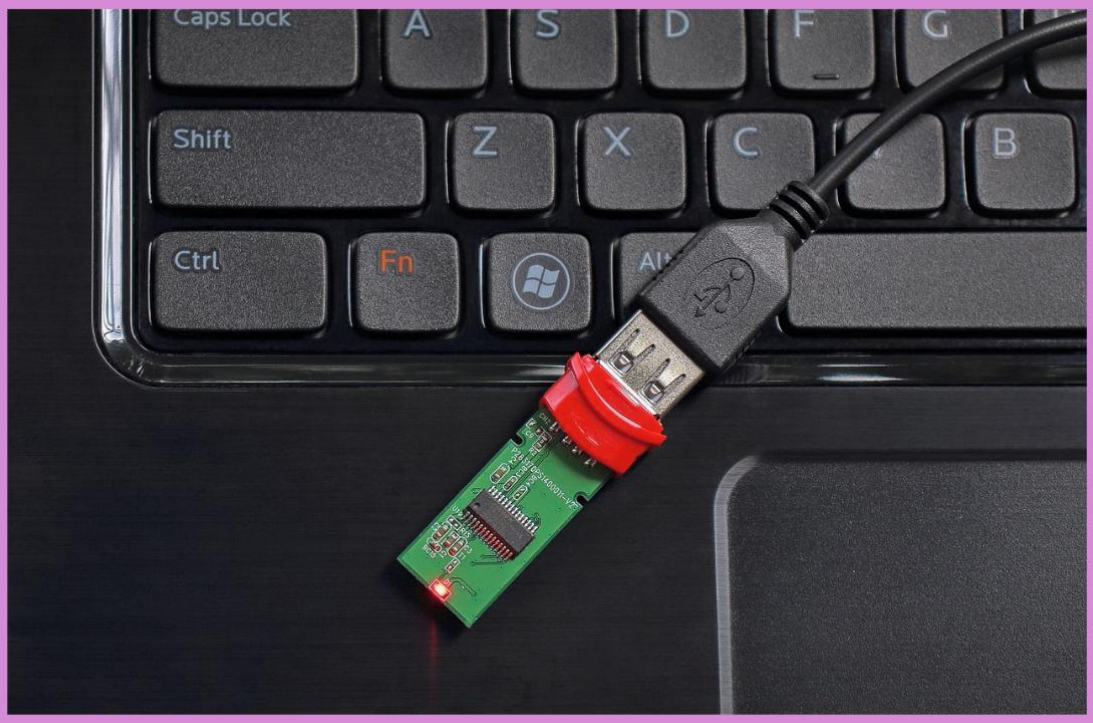
Weak passwords remain one of the most exploited vulnerabilities in business security. Despite widespread awareness, many employees still use passwords like 'Password123' or recycle the same password across multiple platforms. When credentials are compromised in one breach, criminals systematically test them across numerous services.

Strong passwords should be at least 12 characters long, combining uppercase and lowercase letters, numbers, and symbols. However, length matters more than complexity—a 16-character passphrase like 'BlueElephantsDanceTango!' is both stronger and more memorable than 'P@ssw0rd'. Consider using the "three random words" method recommended by the National Cyber Security Centre, making passwords easier to remember whilst maintaining security.

Password managers are essential for modern businesses. These tools generate and store complex, unique passwords for every account, requiring employees to remember only one master password. This eliminates the dangerous practice of password reuse and removes the temptation to write passwords on sticky notes. Many password managers also offer secure sharing features for team credentials and can audit your organisation's password health.

Implement multi-factor authentication (MFA) wherever possible. Even if passwords are compromised, MFA provides a critical second barrier. Avoid SMS-based authentication when alternatives exist, as SIM-swapping attacks are increasingly common. Authenticator apps or hardware tokens provide significantly better protection for your most sensitive systems.

4: Backup



Data loss can devastate a business overnight. Whether from ransomware, hardware failure, human error, or natural disaster, losing critical business data without backups can mean permanent closure. Research shows that 60% of small businesses that lose their data shut down within six months.

The 3-2-1 backup rule provides robust protection: maintain three copies of your data, store them on two different types of media, and keep one copy offsite. This approach ensures that no single failure point can eliminate all your data. For example, maintain your working data, a local backup on an external drive or NAS device, and a cloud backup service.

Automation is crucial; manual backups are forgotten backups. Schedule automatic backups daily for critical data and weekly for less frequently changed information. However, automation isn't enough, you must regularly test your backups by performing restoration drills. Many businesses discover their backups are corrupted or incomplete only when desperately needed during a crisis.

Consider your recovery time objective (RTO) and recovery point objective (RPO). How quickly must you restore operations, and how much data loss can you tolerate? Mission-critical systems may require continuous replication, whilst less critical data might tolerate daily backups. Document your backup procedures clearly so any team member can execute recovery if necessary, and ensure backups are protected with encryption and access controls to prevent them becoming another vulnerability.

5: Cloud Storage

Cloud storage has revolutionised how businesses manage data, offering scalability, accessibility, and cost-effectiveness that traditional on-premise solutions struggle to match. However, moving to the cloud doesn't automatically mean your data is secure; responsibility is shared between the provider and your organisation.

Check your cloud provider has strong security credentials, certifications like ISO 27001. Ensure compliance with UK GDPR requirements, and that your data is physically stored and processed where there are robust data protection laws. Major providers like Microsoft OneDrive, Google Drive, and Dropbox offer business-grade solutions with advanced security features, but these must be properly configured.

Not every employee needs access to all data, grant access only to information necessary for each role. Use cloud providers' built-in sharing controls to prevent accidental exposure of sensitive documents. Regular audits of sharing permissions can reveal forgotten external shares or former employees retaining access.

Enable versioning and recovery features to protect against accidental deletion or ransomware encryption. Most cloud providers retain previous file versions and deleted items for specified periods, providing crucial recovery options. Combine cloud storage with your backup strategy rather than treating it as your sole backup; remember that cloud storage is working data, not archived backup. Consider encrypting particularly sensitive information before uploading it to the cloud, maintaining control of encryption keys.

7: Equipment

Physical hardware represents a significant security consideration often overlooked in favour of digital threats. Lost or stolen laptops, unattended devices, and improper disposal of old equipment can expose sensitive business information just as readily as a cyber attack.

Implement full disk encryption on all devices containing business data. Modern operating systems include built-in encryption tools (BitLocker for Windows, FileVault for macOS) that protect data if a device falls into wrong hands. Enable remote wipe capabilities through mobile device management (MDM) solutions, allowing you to erase data from lost or stolen devices before information is compromised.

Physical security matters equally. Employees should use privacy screens in public spaces to prevent shoulder surfing, and Kensington locks should secure devices in offices or when working remotely from shared spaces. Encourage a clear desk policy where devices are locked away when not in use, and never leave laptops or phones unattended in vehicles.

Equipment disposal requires careful attention. Simply deleting files or reformatting drives doesn't permanently remove data—forensic recovery remains possible. Use certified data destruction services that provide certificates of destruction, or use military-grade data wiping software before disposing of or repurposing old equipment. For highly sensitive environments, physical destruction of storage media may be appropriate. Remember that printers, copiers, and multifunction devices also contain hard drives that store copies of processed documents and require secure disposal.

7: WiFi and Routers

Your network infrastructure forms the foundation of your business's digital security. A compromised router or poorly configured WiFi network provides criminals with unfettered access to everything connected to it, yet many businesses neglect these critical components.

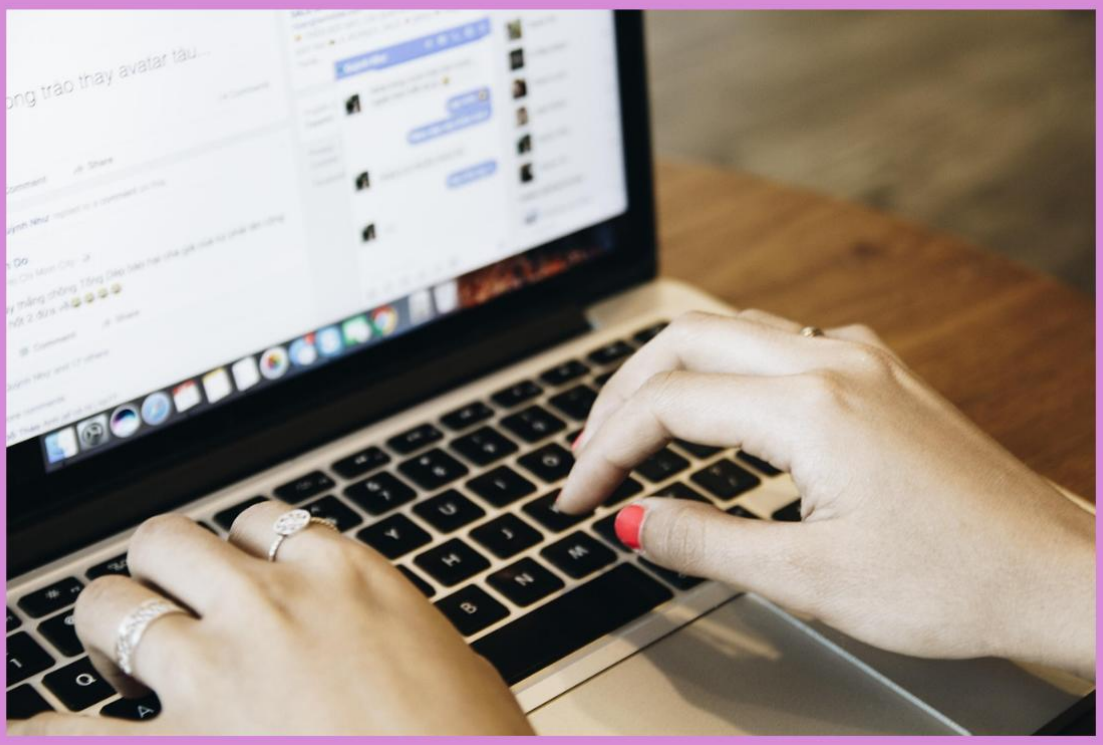
Change default administrator credentials immediately on all routers and network equipment. Manufacturers ship devices with standard usernames and passwords readily available online, making them easy for attackers to access. Use strong, unique passwords and change them regularly. Disable remote management features unless absolutely necessary, as these provide additional attack vectors.

Implement WPA3 encryption for WiFi networks, or WPA2 as a minimum if older devices require it. Never use WEP encryption or leave networks unsecured. Create separate networks for different purposes: a primary network for business devices, a guest network for visitors (with client isolation enabled), and an isolated network for IoT devices like smart thermostats or security cameras.

Keep router firmware updated regularly. Manufacturers release updates addressing newly discovered vulnerabilities, but unlike computers and phones, routers don't typically update automatically. Schedule monthly checks for firmware updates, or enable automatic updates if your router supports this feature. Disable unnecessary features like WPS (WiFi Protected Setup), Universal Plug and Play (UPnP), and unused ports to reduce your attack surface.

Also, think about where your router is located. Poor signals are often simply poorly located routers!

8: Applications



The applications your business depends on daily represent both productivity enablers and potential security vulnerabilities. Every installed application expands your attack surface, and outdated or poorly secured software provides criminals with easy entry points to your systems.

Maintain a comprehensive inventory of all applications used across your organisation, including both officially sanctioned software and shadow IT (applications employees install independently). This allows to track licensing compliance, and remove unnecessary software that creates risk.

Implement a rigorous patch management process. Software vulnerabilities are discovered constantly, and vendors release updates addressing these flaws. Enable automatic updates wherever possible, particularly for operating systems, web browsers, and security software. Where automatic updates might disrupt operations, establish a schedule ensuring patches are applied within days, not weeks or months.

Exercise caution with browser extensions and plugins. These small additions can access vast amounts of data, including passwords, browsing history, and form inputs. Only install extensions from trusted sources, grant minimum necessary permissions, and regularly audit installed extensions to remove those no longer needed.

Enforce application white-listing where practical, allowing only approved applications on business devices. This prevents malware installation and ensures employees use supported, secure software. At a minimum block execution of applications from temporary folders and user-writable locations where malware typically attempts to run.

9. Work Phones

Mobile devices have become indispensable business tools, yet they often receive less security attention than computers despite containing equally sensitive information. Work phones access company email, store customer data, and increasingly serve as authentication factors for accessing critical systems.

Implement mobile device management (MDM) solutions that allow centralised security policy enforcement. MDM enables you to require screen locks, enforce encryption, manage application installations, and remotely wipe devices if lost or stolen. Even for small businesses with just a few devices, basic MDM solutions provide essential security capabilities at reasonable costs.

Modern phones support work profiles or containerisation that segregates business information from personal apps and data. This protects company data whilst respecting employee privacy, and simplifies data removal when employees leave without affecting their personal information.

Educate employees about mobile-specific threats. For instance, use VPNs when accessing business systems over untrusted networks. Disable Bluetooth when not in use to prevent unauthorised connections. Be cautious about which apps receive permissions to access contacts, location, camera, or microphone, as malicious apps exploit these permissions to harvest sensitive information.

Keep operating systems and applications updated. Enable automatic updates for apps, and prompt employees to install operating system updates promptly. Consider replacing devices that no longer receive security updates from manufacturers, typically after three to five years.

10. Policies for Privacy, Social Media and AI Use

Written policies provide the framework for consistent security practices across your organisation. Without clear policies, employees make inconsistent decisions that create vulnerabilities, and you lack grounds for enforcement when security requirements aren't met.

Privacy policies must address UK GDPR compliance, defining how your business collects, processes, stores, and protects personal data. Document who has access to different data types, how long information is retained, and procedures for handling data subject requests. Ensure employees understand their responsibilities under data protection legislation, as individual staff members can be held personally liable for violations.

Social media policies should balance employee expression with business risk management. Define what employees may share about the company, customers, and projects, particularly on personal social media accounts. Address the risks of social engineering, where criminals gather information from social media to craft convincing attacks. Establish guidelines for official company social media accounts, including who may post, approval processes, and responding to security incidents or data breaches publicly.

AI tool policies have become essential as these technologies proliferate. Define which AI tools are approved for business use and for what purposes. Ensure employees understand the danger of sharing sensitive customer information, proprietary code, or confidential business data into public AI systems like ChatGPT may be inadvertently sharing it with third parties. Establish clear guidelines about

what information may be shared with AI tools, and consider enterprise AI solutions that offer enhanced privacy and data protection.

Review and update all policies annually, ensuring they reflect evolving technologies, threats, and regulatory requirements. Most importantly, communicate policies clearly to all employees and provide regular training. Policies gathering dust in filing cabinets provide no protection – they must be living documents that guide daily decisions and behaviours across your organisation.

Thanks for reading this report – I hope you'll find some useful tips you can put into practice in your business.

If you have questions or need help with any of these issues, our team is always ready to offer a helping hand. If technology isn't your thing, we're always happy to help you to set up your systems so your business is well-protected.

Whether you have a one-off problem or want a regular support service you can trust, we can deliver. Most of our IT support can be done remotely, but if you need us on site, we can do that too.

From choosing your initial IT setup, to networking your building, nothing is too much trouble.

EJJB IT CONSULTING

support@ejjb.co.uk

01474 878724

https://www.ejjb.co.uk