Cyber Security Guide

Cyber Resilience Starts With You

www.sharp.co.uk

SHARP

Introduction

In today's digital-first world, cyber threats are a daily reality. From phishing emails and business email compromise to AI-enabled voice and video impersonation, the threat landscape is evolving fast. No matter your industry, company size or job role, every organisation is at risk and understanding your part in cyber security is essential to staying secure.

In this guide, we'll take a closer look at the most common cyber threats facing organisations today, offer our advice on staying secure and will discuss compliance and cyber insurance.

Contents

01: The Threat Landscape

The UK remains one of the most targeted nations for cyber crime, with 43% of businesses reporting a cyber breach or attack in the past year.

In this section, we'll take a closer look at social engineering – a prevalent tactic used to exploit human behaviour and explore how AI is increasingly being used to enhance these attacks.

Prevalent Social Engineering Attacks

What Is Social Engineering?

Social engineering is when someone tricks you into giving away information or access by pretending to be someone you trust. Common techniques include phishing, spear-phishing and Business Email Compromise. It's not a technical hack; it's a psychological one.

Think of it like this:

If someone called you pretending to be from IT and said, "We need your password to fix your account," and you gave it to them, that's social engineering. They didn't break into your system. You unknowingly let them in.

Why It's So Common

Cyber criminals know that people are often the weakest link in security. That's why phishing emails, fake login pages, and impersonation scams are so popular, they're easy to send, and they work.

In fact, phishing remains the leading cause of cyber breaches or attacks, responsible for 85% of incidents in businesses and 86% in charities, according to the UK Government's Cyber Security Breaches Survey 2025.

What makes these attacks so convincing is the use of Open Source Intelligence (OSINT). Criminals gather publicly available data from company websites, social media, and job boards to tailor attacks. This helps them impersonate staff, guess credentials, and craft realistic phishing messages.

OSINT makes social engineering smarter, more targeted, and harder to detect—making it a growing threat to businesses and individuals alike.

The Most Common Social Engineering Threats

- Phishing
- Business Email Compromise (BEC)
- Quid Pro Quo
- Spear Phishing
- Pretexting

SHARP

Social Engineering Scenarios

To help clarify the differences between each type of social engineering threat, we've used Oliver's recent trip to Türkiye as a consistent reference point to show how these attacks can unfold in real-world scenarios.

1. Phishing

Scenario: Oliver receives an email from what appears to be a travel agency:

"Hi Oliver, we hope you enjoyed your recent trip! To claim your exclusive travel voucher, please click the link below and confirm your details."

Threat: Generic and mass-targeted, this phishing attempt uses a believable hook to lure him into clicking a malicious link. They'll send this to thousands of people, most of which haven't just been on holiday but will be hoping that the ones who have – will click.

2. Spear Phishing

Scenario: Oliver gets an email that appears to be from a colleague, Jane:

"Hi Oliver, hope Türkiye was amazing! Can you quickly review the attached supplier contract Jane mentioned before she left? We need your approval today."

Threat: Highly targeted and personalised, this spear phishing email uses insider knowledge and urgency to trick Oliver into opening a malicious attachment.

3. Business Email Compromise (BEC)

Scenario: An attacker compromises Jane's email account and sends this to Oliver:

"Hi Oliver, I hope you enjoyed your holiday to Türkiye. Sorry to bombard you on your first day back but could you urgently send £8,500 to the new supplier. Details attached. Thanks!"

Threat: This BEC attack leverages a trusted internal account to request a fraudulent financial transaction.

4. Pretexting

Scenario: Oliver receives a call from someone claiming to be from IT support:

"Hi Oliver, we noticed unusual activity on your account after your trip to Türkiye. We need to verify your login credentials to secure your access."

Threat: The attacker creates a false narrative to manipulate Oliver into revealing sensitive information.

5. Quid Pro Quo

Scenario: Oliver gets an email from someone claiming to be a cyber security researcher:

"Hi Oliver, I'm offering free security audits — just send over your system logs and I'll run a scan."

Threat: The attacker offers a service or benefit in exchange for access to sensitive data or systems.

SHARP

Increasing AI Risks

While Artificial Intelligence (AI) is delivering significant benefits in areas such as customer engagement, data analysis, and cyber security, on the flip side it also poses certain risks.

The rise of generative AI has dramatically magnified the impact of social engineering tactics. What were once plausible phishing attempts or impersonation scams are now hyper-realistic, AI-powered deceptions that are far harder to detect—and easier to fall for.

Social media platforms are increasingly saturated with AI-generated content, blurring the lines between what's real and what's synthetic. This uncertainty fuels anxiety and self-doubt among users, the question "Is this real?" Which although is not great, it's good that people are questioning these things.

According to the NCSC, the cyber threat posed by AI will intensify significantly between now and 2027. The ability to keep pace with 'frontier AI'—the most advanced and rapidly evolving AI capabilities—will be critical to maintaining cyber resilience over the next decade.

AI's Role in Social Engineering

Cyber attackers are now leveraging generative AI to:

- Craft highly convincing phishing emails and messages
- Automate scams at scale with minimal human oversight
- Clone voices for fraudulent calls and voice-based authentication
- Deploy deepfake technology to impersonate executives and manipulate victims

AI-driven tactics are undermining trust in digital communications and disrupting traditional identity verification. For businesses, the stakes are high: without strong cyber defences and informed employees, organisations are increasingly vulnerable to sophisticated threats that evade standard security protocols. While AI is amplifying risks, it's important to remember that most breaches still stem from basic phishing and poor cyber hygiene.

Speak with one of our experts today or explore our Copilot Consulting Services to see how we can help you harness AI with confidence.

SHARP

Supply Chain Risks

A single cyber attack on a supplier can trigger widespread disruption — delaying deliveries, inflating costs, and even halting production altogether. This is especially critical in sectors like manufacturing, logistics, and retail, where timing and coordination are everything.

Even major organisations like M&S, are not immune. The reality is that cyber criminals are increasingly bypassing technical defences and targeting people — using sophisticated social engineering tactics to trick employees into giving up access, credentials, or sensitive data. It only takes one click on a malicious link or one misplaced trust in a fraudulent email to open the door to a breach.

When a company like M&S is compromised, the ripple effects are immediate and far-reaching. Orders are suspended, operations stall, and suppliers — from farmers to food processors — face unsold stock, wasted resources, and unpaid invoices. For SMEs, these knock-on effects can be financially devastating.

Yet despite the risks, supplier cyber resilience remains dangerously overlooked. According to GOV.UK, only 14% of UK businesses review the cyber risks posed by their immediate suppliers — and this drops to just 7% when considering the wider supply chain.

When assessing your current suppliers or partners on as part of the onboarding process, we suggest you conduct the following:

- Audit supplier cyber policies and ensure minimum standards are met.
- Include cyber clauses in contracts to protect against third-party risks.
- Use monitoring tools to track vulnerabilities across the supply chain.

02: Staying Secure

With threats evolving faster than ever, businesses must take proactive steps to protect their data, systems, and reputation. Yet despite the growing risks, many UK organisations still fall short on basic cyber hygiene.

According to the UK Government's 2025 Cyber Security Breaches Survey, only 40% of businesses use multi-factor authentication, and just 31% have VPNs in place for remote staff. These are basic security defences that every business should be implementing as standard.

From financial loss and reputational damage to regulatory fines and insurance complications, the impact of a breach can be severe. Prioritising cyber security at leadership level ensures that the right investments are made, risks are properly assessed, and resilience becomes part of your company culture.

Three Reasons Why Cyber Security Should Be a Business Priority

1. Rising Threat Landscape

Cyber attacks are increasing in frequency, sophistication, and cost. According to the Cyber Security Breaches Survey 2025, 43% of businesses reported a cyber breach or attack in the past year. These threats range from phishing and ransomware to supply chain vulnerabilities — and no sector is immune.

Why it matters: A single breach can disrupt operations, damage brand reputation, and lead to significant financial loss.

2. Compliance & Insurance

Businesses must follow data protection laws like GDPR to keep personal and customer data safe. If they don't, they could face fines of up to £17.5 million or 4% of global turnover. Insurance companies also expect strong cyber security — without it, you'll struggle to get cover or make a claim.

Why it matters: Cyber security isn't just about keeping data safe. It shows your business takes responsibility, builds trust, and helps avoid legal and financial trouble.

3. Customer Trust and Brand Reputation

A breach can erode trust overnight. Research from CBI shows that 84% of consumers check a business for good data security hygiene before making a purchase.

Why it matters: Strong cyber security is a competitive advantage. It reassures customers, partners, and stakeholders that your brand is resilient and responsible.

SHARP

The Power of a Multi-Layered Approach

A multi-layered approach protects your business across every touchpoint — from your network and devices to your data and users.

Here's how it strengthens your resilience:

Prevention: Firewalls, email filters, and endpoint protection stop threats before they enter.

Detection: Intrusion detection systems and monitoring tools spot suspicious activity early.

Response: Incident response plans and backup systems help you recover quickly and minimise damage.

Education: Team training and awareness reduce human error — still the leading cause of breaches.

To help keep your data and your systems SECURE, here are some essential best practices to follow:

S – Strong, unique passwords for every account

E – Enable two-factor authentication (2FA) wherever possible

C – Connect via VPN when working remotely

U – Use caution with links and attachments

R – Refrain from reusing passwords across platforms

E – Ensure safe practices by following company guidelines

Our Top Five Tips

The key to resilience isn't just technology — it's education. Every member of your team, from the warehouse floor to the boardroom, needs to understand the role they play in protecting your business.

Cyber awareness must be embedded into company culture, with regular training, clear policies, and practical guidance on how to spot and respond to threats. We believe that when people understand the risks, they become your strongest defence.

SHARP

If In Doubt...

When you're faced with an email or phone call and you're unsure if it's legitimate — trust your instincts and follow our five steps:

1. Pause and Verify

Social engineering thrives on urgency. AI-generated content can mimic tone and style, but often lacks context. Take a moment to assess:

- Does the message feel out of character?
- Is the timing unusual?
- Would this person normally communicate this way?

2. Use Trusted Channels

Never rely solely on the medium used to deliver the message. If it appears to come from a colleague or executive:

- Confirm via a known channel—such as a direct phone call, internal messaging platform, or face-to-face conversation.
- Avoid replying directly to suspicious emails or messages.
- If it's a link, find the website via a Google search and avoid clicking on sponsored ads.

3. Check for Red Flags

AI-generated scams often include subtle but telling signs:

- Unusual phrasing or grammar
- Generic greetings or sign-offs
- Requests for urgency or secrecy
- Unexpected links or attachments

4. Report Suspicious Activity

Whether it's a phishing email, a voice deepfake, or a suspicious video:

- Report it immediately to your IT team.
- Early reporting helps prevent wider exposure and strengthens organisational resilience.

5. Stay Informed

Cyber threats evolve rapidly. Stay up to date with the latest guidance from trusted sources like the National Cyber Security Centre (NCSC).

Awareness is your first line of defence against both AI-driven and socially engineered attacks.

SHARP

03: Compliance & Insurance

As businesses increasingly rely on technology to manage data, transactions, and communications, ensuring compliance with cyber security regulations protects not only sensitive information but also brand reputation and customer trust.

Cyber Compliance

What is the Cyber Security and Resilience Bill?

The Cyber Security and Resilience Bill is a proposed UK legislation designed to strengthen the country's digital defences. It aims to improve security standards and mandate increased cyber incident reporting.

We've seen essential services in the firing line of large-scale cyber attacks, such as the attack on NHS hospitals that resulted in sensitive data to be leaked and disruption to service. The bill is aimed at strengthening our essential services, such as healthcare, power and water to address the growing threat.

UK data centres are also classified as critical national infrastructure, which puts them into the same category as water, energy and emergency services systems. Data centres will also be required to meet enhanced cyber security protocols, which means stronger protection for your data and greater accountability from providers, giving you more confidence in the partners you choose.

How does the Cyber Security and Resilience Bill affect your organisation?

Although it has not yet been outlined in the Cyber Security and Resilience Bill exactly how it will affect organisations, it could follow in the footsteps of the NIS2 legislation in Europe.

The bill could mean the following for organisations:

- **Increased Security:** Organisations could expect improved cyber security protection and measures for their data, reducing the risk of cyber attacks. This is particularly crucial for sectors that rely heavily on data, such as healthcare and finance.
- **Regulatory Compliance:** Organisations might need to comply with stricter cyber security protocols and regulations, which may require additional investments in security infrastructure and training.
- **Operational Resilience:** With data centres due to receive more robust support, organisations might expect greater operational resilience, minimising disruptions to their services and operations.
- **Stronger Supply Chain Oversight:** The bill may drive regulators and organisations to better manage supply chain risks, ensuring third-party providers meet robust cyber standards
- **Streamlined Incident Reporting:** Reporting requirements could be enhanced, with faster timelines and greater transparency.

Cyber Insurance

To successfully claim on a cyber insurance policy, insurers increasingly require businesses to provide tangible proof of robust cyber security practices.

This includes evidence of:

- Multi-Factor Authentication (MFA) across critical systems
- Endpoint Detection and Response (EDR) solutions to monitor and contain threats
- Regular, secure backups to ensure business continuity
- Incident response rehearsals to demonstrate preparedness for real-world breaches

These measures are no longer optional. They form part of a growing checklist insurers use to assess risk and validate claims. Without them, organisations may face reduced coverage, higher premiums, or even denied claims.

To meet these expectations, aligning with recognised frameworks such as the NIST Cybersecurity Framework and Cyber Essentials is strongly recommended. These standards not only strengthen your organisation's security posture but also serve as clear evidence of due diligence — a critical factor in underwriting decisions.

Looking ahead, the Cyber Security Resilience Act, will require UK organisations to meet minimum cyber security standards. Compliance will be essential not just for regulatory reasons, but also to maintain insurability. Insurers are increasingly factoring in resilience measures when underwriting policies, and failure to comply could result in reduced coverage or denied claims.

04 How We Can Help

We help businesses build strong, multi-layered cyber security strategies tailored to their industry and risk profile.

Whether you're aiming to boost resilience, meet compliance or achieve cyber accreditations, our Cyber Security Packages ensure you have the fundamental security measures in place. Aligned to the trusted NIST framework and government-backed Cyber Essentials scheme, you will have peace of mind that you have the essentials covered.

SHARP

We'll Give You Peace of Mind

Our Cyber Security Packages are built around the essential layers every business needs:

Perimeter Protection: Firewalls and email filters that stop threats before they reach your network.

Endpoint Security: Antivirus and device controls that keep your hardware safe and compliant.

Access Management: Secure login protocols and multi-factor authentication to prevent unauthorised access.

Data Protection: Encryption and backup solutions that safeguard your sensitive information.

User Awareness Training: Clear, jargon-free education that empowers your team to spot and respond to threats.

Ongoing Support & Monitoring: Expert help and real-time alerts to keep your defences strong and responsive.

Why Partner With Us?

- Over 30 years of experience
- Microsoft Solutions Partner for Security
- Cyber Essentials Plus Certified
- ISO 27001 accredited

Speak with one of our experts today or explore our Cyber Security Packages to discover how our team can help you.

SHARP

www.sharp.co.uk

SHARP