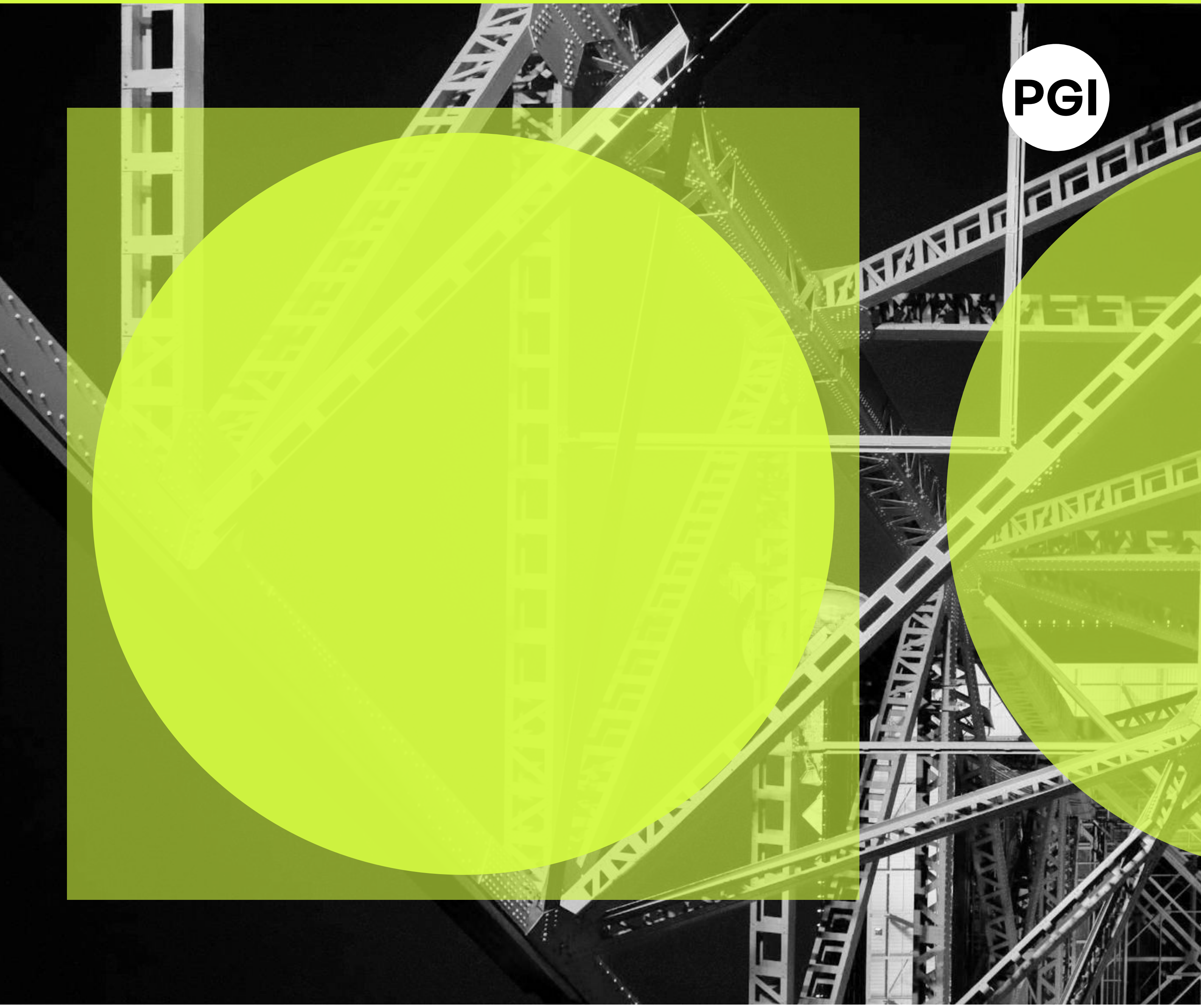

How SMEs can protect themselves against the surge in social engineering attacks

Insights from PGI's Head of Penetration Testing, Barry Sadler & Senior Digital Investigations Analyst, Shawn Gillooly

Visit: www.pgitl.com
Email: findoutmore@pgitl.com

Phone: +44 (0) 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT, UK

PGI - Protection Group International Ltd.
Registered in England & Wales. 07967865

Will we be next?

Social engineering attacks are on the rise, and today, small and medium enterprises (SMEs) are at a higher risk of being targeted.

For SMEs, it's tempting to think, "It won't happen to us", but the consequences of a successful attack can be severe, and can far outweigh the cost of preventative measures. These attacks often result in unauthorised access to systems, fraudulent payments, data theft, operational disruption, and reputational damage. In some cases, a single mistake made by an employee is enough to impact customers, suppliers, and the wider supply chain.

> " attackers often follow the path of least resistance "

Attackers often follow the path of least resistance, and SMEs are frequently targeted because their defences tend to be less mature than those of larger enterprises. As a result, these organisations require less effort and resources to bypass security measures. This lower barrier of entry increases the likelihood of a successful attack.

Understanding how these attacks work and investing in practical defences is essential for strengthening protective capabilities. Even with limited budget or resources, SMEs can still take a strategic approach to mitigating social engineering risks. By incorporating intelligence and proactive measures into your security strategy, you can better identify potential threats, close gaps and build resilience across your organisation.

In this whitepaper, we'll go into detail about practical steps SMEs can take to reduce exposure to social engineering attacks and enhance their overall security posture.

What is social engineering?

Social engineering is a **psychological manipulation technique** used by threat actors to trick individuals into revealing confidential information or granting access to secure systems. It **exploits human behaviour** by leveraging fear, urgency, or authority to trick individuals into compromising security. It covers all forms of communication, including email, phone, social media and face-to-face.

A social engineering attack could be anything from an email impersonating a supplier requesting a change in bank details, to an attempt to recruit an insider through manipulation. Essentially, if the attack involves communication with a human, it falls under the social engineering umbrella.

Why SMEs should care about social engineering

Social engineering attacks are increasingly common because it's low-risk and high-reward. It requires very little technical skill, and large groups can be targeted with low effort.

Crowdstrike's 2024 annual global threat report revealed a **442% increase in voice phishing** between the first and second half of 2024, highlighting that **as technical defences get stronger, threat actors are increasingly targeting human vulnerability.**

Attackers today are exploiting trusted third-party vendors or partners to gain inside access to their target organisations. There are also increasing numbers of threat actors using AI generated video and language tools to trick hiring managers into onboarding malicious insiders.

> “No organisation is immune”

In recent news, even large, high-profile companies like Jaguar and Heathrow have fallen victim to these types of attacks. This highlights how **no organisation is immune** and demonstrates the true scale and sophistication of modern social engineering attacks today.

While large organisations may seem like the more enticing targets due to the potential payoff, attackers are aware that they're likely to be up against strict security controls and multiple layers of approval. In practice, **attackers often follow the path of least resistance**, targeting SMEs because defences tend to be less mature, and may be more straightforward to infiltrate.

For SMEs with a limited budget for cybersecurity, the focus should be on using resources effectively. Regular Digital Risk Assessments on key personnel, combined with internal control frameworks like ISO 27001, can raise defences enough to remove your organisation out of attackers' pathway.

Why social engineering attacks are so successful

Exploiting human nature

Training related to social engineering is often focused more on the technical elements as opposed to the core understanding of how social engineering works. This can pull people away from understanding what social engineering actually is – a manipulation of human behaviour. Just focusing defences on technical risks can overlook the primary method of attack.

Employees juggling multiple tasks might click on an email that appears legitimate or inadvertently share information online. Small oversights due to stress or distraction make organisations susceptible to these campaigns, particularly if they believe the contact is from a trusted individual or authority figure.

The key element in these attacks isn't the novelty or sophistication, but rather the exploitation of common human behaviours, leaving vulnerabilities in an organisation's defences. These types of attacks are relatively low effort, require less skill, and bypass the highly technical barriers of cybersecurity software, making them a very common and favourable method of attack.

> “human error contributes to **up to 95%** of data breaches”

Technical vs non-technical controls

Protective controls surrounding employees are not usually considered as thoroughly as technical controls, such as firewalls. Although **human error contributes to up to 95% of data breaches** (according to a 2024 study by Mimecast), the vast amount of time is often still spent on developing and refining only technical controls, which ultimately alone will not help to prevent social engineering attacks.

Policies

Policies related to social engineering, such as the sharing of information, don't always consider important questions such as:

- **Who should I provide access to this information?**
- **How do I determine if someone is who they say they are?**

Digital footprint

Some threat actors use information found online to blackmail individuals and businesses. By leveraging publicly available information (such as employee or supplier details), attackers can execute much more convincing attacks that seem legitimate. They often impersonate people of authority within an organisation to bypass security measures – sometimes using multiple layers of compromised personas to trick decision-makers.

AI technology

AI is one of the most common talking points within the cybersecurity space today, fuelling both hope and fear for the future. The reality is actually far more nuanced.

AI tools have the capability to act as a powerful 'admin assistant' for threat actors, automating tasks, generating copy, gathering information on targets and executing campaigns at a larger scale. This has lowered the bar for the level of effort required, so even unskilled threat actors can easily start launching campaigns. It's also easier for attackers to execute more legitimate-seeming attacks by creating deepfake videos and voice calls to impersonate a trusted or authoritative individual.

Although there's limited data so far to show how extensively threat actors use AI today, it's clear that it can enhance the effectiveness of these attacks. This underscores the need for organisations to stay informed and prepared. But, fundamentally AI has not 'revolutionised' social engineering- it's simply added new tools that can be leveraged by threat actors.

Practical steps for SMEs to defend against social engineering

The good news is that when it comes to practical steps to protect against social engineering, you don't need to reinvent the wheel as they have stayed largely consistent over time. In some cases, it only adds another layer of defence to the security measures and controls that organisations already have in place.

1 Improve identification of social engineering attacks within your team

Training employees to recognise social engineering techniques and understand the potential consequences is essential to strengthening your defences. Providing real-life examples can increase awareness and preparedness. While this doesn't guarantee every attack will be spotted, it improves resistance, making it more difficult for attackers to succeed.

Some practical approaches that help improve people's understanding of social engineering include:

a. **Ensuring all employees have a good understanding of what social engineering is, beyond the technical elements.**
Educate staff on the human psychology element and how to recognise manipulation techniques. This encourages people to think more about the context and content of messages and provides them with the tools to question and appropriately respond to suspicious communications.

b. **Sharing personal stories and case studies of social engineering attacks.**
Use these as a starting point to discuss how people could have detected it, and appropriate actions. Where possible, make these discussions frequent to keep awareness high.

2 Invest in proactive intelligence

Adding a layer of intelligence to your strategy will help strengthen proactive defences and make your organisation more difficult to target. Proactively understanding your protective capabilities means you will have more confidence in where your current limitations are.

Targeted services can help you identify and mitigate weaknesses in your protective controls:

a. **Digital risk assessments**
provide insight into publicly available information of key personnel and suppliers to identify weak points and mitigate them

b. **Policy reviews**
Ensuring policies cover different elements of social engineering and how to protect against it.

c. **Social engineering assessments**
Ideal for identifying who may struggle to identify specific social engineering attacks to give you a starting point for how to resolve it.

d. **Strategy Development**
Working on a long-term approach to developing your protective capabilities will make it easier to know what challenges you need to overcome in areas related to social engineering attacks.

3 Develop a layered security strategy

Establishing your core security strategy

The concept of ‘strategy’ may have started as a military concept, later adopted in business, but it’s equally relevant to building long-term protective capabilities. The first step is to clearly define the space you are protecting. In the context of social engineering, this primarily focuses on **users and the controls surrounding them.**

From this, a core security strategy can be developed, serving as the foundation for subsequent decision making. This core strategy will cover your business goals and represents your main focus where you can **demonstrate long-term value to the business.**

As your business matures, you can build your sub-strategies that address specific areas, like protection, monitoring and testing.

Some key concepts for social engineering-focused strategies could include:

a. **Protection strategy:** How do we protect our people, operations and data from social engineering attacks to ensure the continuity of our business?

b. **Monitoring and response strategy:** How do we identify and respond to social engineering incidents?

c. **Security testing strategy:** How do we assess the effectiveness of our defences against social engineering attacks?

A strong security strategy should be focused and realistic, ensuring it addresses threats within the defined space, and is adaptable to emerging threats.

Building layers of defence

A layered strategy goes beyond technical defences and includes proactive engagement with both your people and your wider information environment. For example, training staff to recognise manipulation complements technical systems designed to protect data from attackers. These layers can also extend to outside of your organisation to see how attacks might develop and using what information.

Social engineering attacks often rely on Personally Identifiable Information (PII) such as social media posts or photos, home addresses, telephone numbers, old email addresses and more to build trust, intimidate, or even outright blackmail key personnel within your company.

A layered defensive strategy not only recognises the need to find technical solutions and mould behaviour through training, but also **proactively identifies potential risk vectors and takes action to mitigate them** e.g., conducting investigations into their own key principals to get a 'lay of the land' regarding potential PII.

Oftentimes, the identification of PII can lead to immediate, direct security-improving actions; like taking down posts or accounts, identifying potentially compromised personal and professional accounts, and strengthening the overall operational security of key principals and their families to make them less appealing as a target.

> “An effective layered defence strategy will achieve three key objectives”

An effective layered defence strategy will achieve three key objectives:

a. Mitigate attacks as they emerge and before they reach critical targets.

b. Ensure that if an attack occurs, individuals within the organisation are prepared and can respond appropriately.

c. Reduce the volume and likelihood of potential attacks that could be directed at the organisation in the first place by limiting exposure and risk vectors.

Implement a strong internal control framework

Human risk management should form a key element of your overall risk management strategy. A structured framework will help you to standardise security practices across your organisation and reduce the likelihood of breaches.

- **Cyber Essentials (Basic or Plus)**
  A UK government-backed certification ensuring the most fundamental IT security measures are in place.

- **Conducting a Gap Analysis**
  An assessment of your existing information security measures to identify areas for improvement.

- **Implementing ISO 27001**
  A globally recognised standard for more mature organisations needing an advanced information security management system

The value of your policies and controls

Policies

To achieve your long-term security strategy, you also need to drive behavioural change across the business. This is where security policies come in. Like your other policies, their purpose is to guide actions and decision-making, but the focus is on protecting that defined space covered in your core security strategy. When security policies are well-defined and consistently reinforced, they can be used to influence behaviour around security. This shift towards a security-first culture can reduce the likelihood of human error or negligent behaviour.

In the case of social engineering, clear policies ensure employees understand what's acceptable, how to verify requests, and how to recognise and respond effectively to suspicious activity.

Policies surrounding social engineering should take into account different types of social engineering attacks, including:

- How to identify social engineering attempts
- What questions to ask yourself before responding
- How to determine if the person you are speaking to is who they say they are? How do you know whether or not it is someone pretending to be them (e.g., a deepfake)?

It should be made clear to employees what data can be shared both internally and externally to your organisation. Employees should also understand how to verify someone's identity and be able to discern legitimate requests from phishing scams or other social engineering attacks.

Controls

Social engineering attacks exploit human behaviour, so a combination of both technical and non-technical controls is the most effective approach to reducing the risk of a successful attack.

Evaluate your current controls to understand your baseline:

a. What controls do we currently have in place?

b. How effective are they in practice?

c. Are there gaps in one control that another control can compensate for?

Non-technical controls are essential for effective defence:

a. **Employee training** helps your team to recognise manipulation, respond appropriately and understand the consequences of a successful attack.

b. **Digital Risk Assessments (DRA)** identify and mitigate publicly exposed information about your organisation and key personnel, reducing the opportunities for attackers to exploit it.

c. **Formalised verification processes** ensure that high-risk actions, like access requests, payment changes, or data sharing, are verified through approved channels. All staff should be aware and trained to follow these processes consistently.

Technical controls make attacks more difficult to execute:

a. **Limiting user privileges** so employees only have access to the systems and data that's necessary for their role

b. **Email filtering** for commonly used phishing terms and suspicious messages

c. **Alerts** to flag emails from outside of your organisation

The final word: It's not impossible

SMEs don't need to invest millions to protect themselves against social engineering attacks. Implementing even just a few of the steps below can raise your defences high enough above the baseline to place you out of the attacker's path of least resistance and improving your overall security posture.

- **Clearly define your scope of protection** and what types of threat you're protecting it from.
- **Develop and implement policies** related to social engineering that provide clarity on what behaviour is expected and what an appropriate response looks like.
- **Implement practical procedural and technical controls** that support your policies.
- **Build awareness:** Ensure staff understand why social engineering attacks work and how they exploit human behaviour.
- **Share and discuss real-life examples** of social engineering attacks, highlighting how they could have been detected.
- **Leverage intelligence** related to deliberately harmful behaviour and assess what information about your organisation or people can be used against you.

Get in touch with our team today to find out how we can help protect your organisation against sophisticated modern threats like social engineering.