Humans are the weakest link

Net-Defence
Ogilvie House, Princes Park, Team Valley Trading Estate, Gateshead NE11 0NF • Ogilvie House, 200 Glasgow Road, Stirling FK7 SES
Tel: 03300 241 666 • Web: net-defence.com

Verizon reported that 68% of all attacks that occurred globally involved a non-malicious human element. In the same period, the ICO reported that 60% of UK data breaches were due to insider action.

We all employ smart people with strong skill sets, whether they be problem solvers, critical thinkers, leaders or decision-makers, so how can the percentage be so high?

In this blog post, we'll look at why people are the weakest link in your security and how you can reduce the likelihood of an attack due to human error.

First, let's take a look at the common types of cyber attacks.

The Stats (SotP and Cyber Breaches survey)

In the past 12 months, 50% of businesses and 32% of charities experienced a cyberattack or breach. This figure rises to 70% of medium-sized businesses and 66% of high-income charities.

Email remains the most common method of attack, with phishing affecting 84% of businesses and 83% of charities. Email (and online) impersonation/spoofing is the second most common method, affecting 35% of businesses and 37% of charities, followed by malware and ransomware, which affects 17% of businesses and 14% of charities.

Our employees make choices and decisions that ultimately determine whether a cyber attack is successful.

Cybercriminals use psychological manipulation to get the target to react, engage and ultimately perform an action for an illegitimate purpose. They only need to be lucky once and use every tool at their disposal to improve their chances.

Spear phishing

A method that is becoming increasingly popular is spear phishing. Instead of casting a wide net, the attacker will target one individual. They will spend time researching and gathering information, mostly from open sources (social media, google etc) before designing a tailored attack to acquire the data they want. They will often mimic a trusted person to make it seem even more legitimate and add a sense of urgency to push the victim into taking action.

Spear phishing has become the most popular method of phishing among attackers. In 2023, UK companies reported that spear fishing had a 53% success rate, compared to an 18% success rate for phishing attacks.

AI & deepfakes

In the age of artificial intelligence, attackers are using AI-powered techniques to breach even the most robust cyber defences. Attackers can use AI to create highly convincing voice or video messages that impersonate a trusted person, tricking unsuspecting victims into giving them access to sensitive data or authorising fraudulent transactions.

A recent example is the successful cyberattack on the ARUP Group, a UK multinational company, using a deepfake video call. In January 2024, an employee in Hong Kong, believing he was on a video call with an ARUP senior officer, was tricked into transferring £20 million to cybercriminals.

BEC

Business email compromise (BEC) occurs when a criminal uses an email to trick employees into transferring money or disclosing sensitive company information. These attacks are often directed at senior executives or those who can approve financial transactions.

In late 2022, a new threat group emerged: the Crimson Kingsnake. They were specifically conducting large-scale BEC attacks using blind third-party impersonation tactics to defraud companies all over the world. The group impersonated professional law firms and real solicitors in order to trick accounting professionals into transferring funds.

They aimed to intercept and divert funds by registering hundreds of domains similar to well-known law firms and sending out mass emails chasing up payments on false invoices. They used legal language to add legitimacy while also conveying a sense of threat and urgency, allowing the process to be completed before anyone understood what was going on.

Supply Chain Risk

Attacks on the business supply chain are a current and growing risk that companies must be aware of in 2024. Supply chain risk relies heavily on the chances of human error. Through this method, cybercriminals look for weaknesses within the UK supply chain to infiltrate particular organisations and use them as a stepping stone to attack larger, more high-profile targets.

Once inside your supply chain, an attack can take many forms, including service disruption, data theft, infrastructure breach, or a direct cyber attack. The attack can come by direct target or chance, which we have differentiated below.

A direct attack occurs when cybercriminals have identified you as their primary target and have determined that your defences are too strong to overcome, requiring them to take a different approach. They will review your supply chain to find a weakness and exploit this.

A chance attack occurs when the supply chain has been successfully compromised, and the attacker then casts a wide net throughout the chain to see where else they can get lucky.

Whether you are a direct target or have become a target by chance, these attacks can be extremely difficult, and sometimes impossible, for employees to detect.

It has long been recognised that email is the biggest threat and the most common method of launching an attack in the UK. The type of attack can vary significantly, and email scanning, antivirus technology and firewall controls have been doing a pretty good job of keeping these attacks out.

However, if someone in your supply chain (customer or supplier) has been compromised and the criminal has access to their email, standard prevention and detection controls may be ineffective.

When authentication, authorisation, and signature-based detection are all compromised, combined with the insider knowledge that a hacked email account can provide an attacker, communication patterns will fail to flag anomalies.

Consider this: if you received an email from a trusted source with who you communicate on a regular basis, would you hesitate to open a document, click a link, or enter your user credentials to access a file? This is what the attacker is counting on.

Insider Action / Threat

Not every threat comes from outside your organisation. Insider threat refers to employees who can unintentionally or intentionally jeopardise business security. There are two types of insider threats: human error and malicious action.

Unintentional insider threats often occur due to human error or a mistake leading to information or data being disclosed, whereas intentional insider threats involve a malicious action conducted purposely, such as intentional data theft or data destruction.

In 2015, a disgruntled Morrisons supermarket employee who had been subject to disciplinary procedures leaked payroll data for approximately 100,000 employees (past and current). He received an eight-year prison sentence for his actions, and the supermarket was also found to be at fault.

Morrisons fought for 5 years to demonstrate that this was a personal vendetta by the ex-employee and that they should not be held vicariously liable. In 2020, the UK Supreme Court overturned the original findings, exonerating the supermarket of all responsibility.

According to data collected from businesses across the UK, 71% of employees said they had taken a risky action that could jeopardise the company's security, with 96% of those participants aware they were doing so. 60% of those polled thought they were not responsible for security (8%), or were unsure of their responsibilities (52%).

Those who took risky actions stated that they did so for a variety of reasons that would benefit their organisation, including saving time, meeting an urgent deadline, saving money, achieving a revenue target, and meeting performance goals. Even if they intended to help the organisation, their actions could have been extremely detrimental.

The top five risky actions for employees within an organisation are as follows:

- Using a work device for personal use
- Reusing or sharing a password
- Connecting without a VPN
- Responding to a message from an unknown person
- Accessing inappropriate websites

What else do we need to consider?

We are already aware that cybercriminals play a psychological game with our employees in order to manipulate our human reactions. However, are you aware that they use their unconscious bias to increase their chances of success?

Let's take a closer look at some of these methods and how they're exploited:

Curiosity effect

Curiosity is one of the most powerful human characteristics that hackers can exploit. Attackers frequently use a false promise to pique a victim's interest, leading them into a trap that steals information or infects their system with malware. We're all a little nosy, so it's no surprise that secrets, gossip, and limited offers can give hackers a psychological advantage over their victims.

Authority bias

An attacker who uses authority bias may impersonate a senior manager or even a CEO and send an email to an employee requesting payment for an unauthorised invoice. The employee may ignore major red flags because the request is made by what appears to be an authoritative figure. This method takes advantage of the trust between employees and senior employees in order to gain access to accounts or sensitive data.

Optimism bias

Optimism bias is the tendency to overestimate the likelihood of positive outcomes while underestimating the risk of negative results. Although cyber criminals target specific individuals and businesses based on their worth and what they can gain, no individual or business should assume they are immune from being chosen as a target.

Recency effect

The recency effect causes individuals to place undue importance on recent events while ignoring historical or contextual information. Cyber attackers use this bias to launch targeted attacks immediately after a high-profile event, diverting attention and resources away from standard security protocols.

Hyperbolic discounting

Everyone enjoys a special offer or a deal that seems too good to be true, which is why hackers frequently use hyperbolic discounting. This method capitalises on the human tendency to prefer smaller, immediate rewards over larger, future rewards. For example, most of us fall for 'free trials' or 'free coupons' and are willing to give away our credit card information without considering the potential long-term negative consequences.

Halo effect

Hackers are not angels, but they do enjoy using the halo effect to attack. The halo effect is based on the victim's likelihood of having a positive impression of a person, company, brand, product, or service. Cybercriminals frequently impersonate trusted entities such as banks or reputable organisations, to trick people into clicking on malicious attachments or URLs.

Loss aversion

We all want to avoid suffering a loss or engaging in negative behaviour. Cybercriminals use this to their advantage by threatening the loss of something, usually money, in front of their potential victim, clouding their judgement and making them more likely to cooperate and share valuable information or send funds to hackers.

Ostrich effect

The ostrich effect describes people's tendency to avoid difficult situations rather than deal with them. When dealing with an overwhelming or complicated situation, people may prefer to take an out-of-sight, out-of-mind approach, which could benefit an attacker. For many organisations, an attack is unavoidable, and the only way to protect yourself is to take precautions to ensure that you are prepared rather than ignoring the possibility of one occurring.

Habit

This bias takes advantage of users' tendency for recurring habits, constructing social engineering attacks that are received around the same time as expected regular emails or other communications. For example, they may be aware of a specific time when emails regarding deliveries are sent out and send a phishing email at the same time, increasing the likelihood of an individual clicking on a malicious link.

How do we reduce the human risk?

Human behaviour and personality also play a significant role in the likelihood of a successful cyber attack. If we went deep here, it would take us days, weeks, or even months to fully explore everything. However, it is an aspect that should not be ignored, so we are going to give you a brief overview.

When it comes to cyber attacks, people's personalities influence how they feel about the subject. Some people are already well-versed in how to avoid an attack, some are terrified and refuse to discuss the subject, some believe they will never be a target, and some are hungry for knowledge and insight into how to do so.

Let's look at how to reduce risk and balance/address the personalities and behaviours of those you work with.

The first thing to consider is unsurprisingly, training! We must be mindful of not overloading and overwhelming our employees as this can lead to them not participating in training, being put off due to fear or hiding behind other priorities.

We wouldn't let any employee begin work without proper training, so how can you expect them to protect your company from cyber attacks without it?

To ensure cybersecurity is drilled into the mind of employees, organisations should:

Provide phishing simulation exercises

The simulations are proven to be extremely effective in providing cyber security training to employees and can be hidden amongst their day-to-day emails.

You should begin by sending simple phishing exercises and gradually progress to more difficult ones as employees become accustomed to them. Your employees want to be seen as doing an excellent job; if they are aware that these types of emails are being sent, they will pay closer attention to ALL emails.

This type of training is also beneficial for employees who are arrogant about cybersecurity and believe that you can't catch them out! This is a win-win situation; either you catch them or they work even harder to avoid being caught.

Share organisational results and statistics

You should share statistics that demonstrate how your organisation is being targeted, as well as near misses and successful attacks. If we are subjected to a successful attack, we forget that we are victims of crime and will try to hide this from the rest of the world. However, this should not be the case. Shared knowledge and wisdom can help mitigate the chances of a similar situation happening again.

By sharing this information such as email filter results and details of how attacks happened and were avoided, you can increase engagement from those employees who believe they and your organisation would never be a target. Sharing how these attacks present themselves will help employees to be better prepared.

Operate with a no-blame culture

If you want an organisation that openly reports everything, including mistakes, a no-blame culture is essential. Blaming users for security mistakes can be both unfair and counterproductive. Fostering a culture in which employees can communicate openly about security issues without fear of repercussions means they are much more likely to speak up about something they don't think looks right or to report a mistake before it becomes serious.

Motivate employees to make security a priority

Even if employees attend awareness courses, a lack of practical application can cause them to lose interest and reduce awareness levels. It is critical to continue motivating employees to prioritise cyber security, which can be accomplished through a variety of methods such as providing ongoing personalised, interactive training, implementing a reward and recognition programme, or reinforcing its importance with regular reminders.

Other ways you can defend

There are numerous other ways to protect your business from the threat of a cyberattack. These include methods to reduce the human and technical error, as well as certifications and training for your employees, which are detailed below.

Human

- Add a report phishing button on your email system to enable fast reporting.
- Limit access to your data on a need-to-know basis.
- Implement timing limits when large or wide access is required for a short period of time.

Technical

- Implement email filtering that requires approval to release high-risk emails
- Ensure you have implemented authentication email protection (DMARC, DKIM and SPF).
- Activate MFA (multi-factor authentication) or 2FA.
- Implement continuous patch management
- Ensure your data is backed up and stored away from your operational infrastructure to stop the attacker from accessing these.
- Ensure you test your backup to ensure you can recover if the worst happens.

Certifications

- Cyber Essentials - aimed to safeguard your organisation from the most common cyber threats, focussing on your technical controls and systems.
- Cyber Assurance - designed to implement an Information Security Management System (ISMS) which is a risk-based approach, assessing your; people, processes, technology, and assets demonstrating your level of cyber security, privacy, and data protection.
- ISO27001 - the international standard for information security, cyber security, privacy protection. This is governed by the independent International Organization for Standardization and is recognised globally as the highest-level certification in the industry.

Contact us today to learn more about how you can reduce the likelihood of a human error-based attack on your business.