

The logo for IRIS, featuring a red square followed by a blue vertical bar, and the word "IRIS" in white uppercase letters.

IRIS

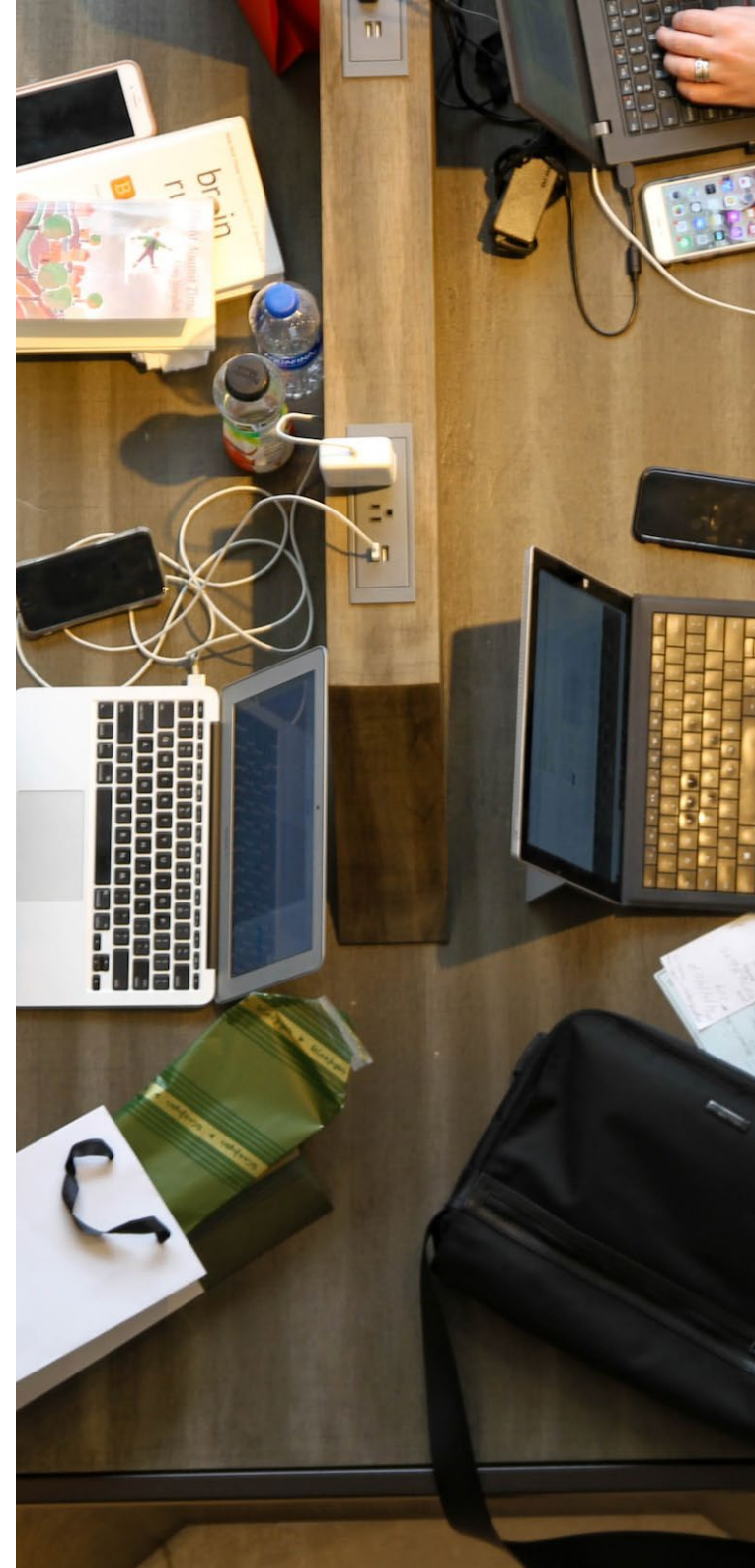
The State of Cybersecurity in 2023

How to protect your business in the face of
an ever-evolving threat landscape



Contents

Overview	3
Looking Ahead to Ongoing Risk Factors	5
Increasing Complexity of Technology Ecosystems.....	6
Changes to Ransomware Attacks and Payments.....	7
Scarcity of IT and Security Talent	8
Reliance on Less Mature Third Parties	9
Targeting the Weakest Link.....	10
How to Best Protect your Business	11
Reduce the Attack Surface	12
Dynamic Defence.....	13
A Combined Effort of AI, Automation and Human Intervention.....	14
Education and the Impact of Security Culture.....	15
Rely on the Assistance of a Trusted Provider	17
How We Can Help	18





Overview

When looking back at 2022, it was a turbulent year, full of macroeconomic and geopolitical risk. From the war in Ukraine to rapid inflation and supply chain failures, it has been the perfect storm of interlocked risks. This has had a profound effect on cybersecurity for businesses in the UK, Ireland and the rest of the world.

Now in 2023, cybersecurity is more important than ever, with all businesses, regardless of size or industry, being at risk of falling victim to a cyberattack or data breach.

In this eBook, we will break down the factors that are increasing cyber risk in 2023 and look into what steps you can take to protect your business.

2022 in Numbers



81%

of UK organisations experienced a successful cyberattack in 2022



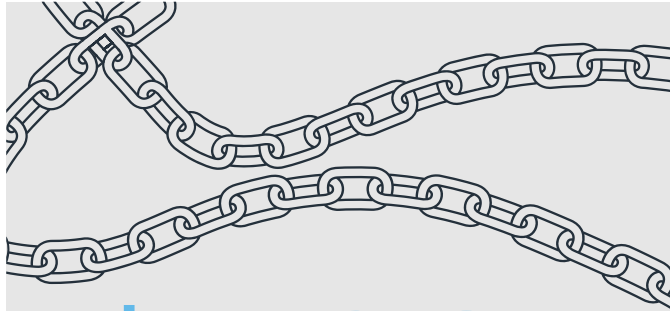
84%

of businesses can't find enough skilled security employees



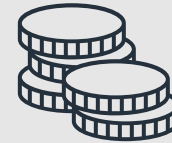
53%

of UK organisations experienced ransomware attacks in 2022



\$1.96_{mil}

The average cost of ransomware remediation in the UK



13%

of organisations pay the ransom after a cyberattack



77%

of employees reuse passwords across multiple services



93%

of employees update social media when they get a new job



80

The number of SaaS applications an average organisation uses

A dark, low-key photograph of a person wearing headphones and glasses, working at a computer. The person's hands are visible on a laptop keyboard. In the background, a computer monitor displays lines of code in various colors (green, blue, yellow) on a dark background. The overall scene is dimly lit, with the primary light source being the computer screen.

Looking Ahead to Ongoing Risk Factors

Increasing Complexity of Technology Ecosystems

Over the past decade, technology ecosystems have become increasingly complex. A relatively short time ago, a business would have a technology ecosystem comprised of a local area network, on-premises servers hosting applications, and endpoints such as PCs, laptops and printers. For most businesses, it was feasible for a single System Admin to manage this infrastructure.

Fast forward to 2023, most businesses have a complex ecosystem of cloud services, SaaS applications, data connectors, IoT devices and APIs that are working together. These technological advancements bring massive benefits to businesses, improving productivity whilst enabling communication and collaboration for remote and hybrid workers.

However, the sheer number of services being used makes managing complexity difficult. This is also the reason why a zero-trust security model is not feasible for most businesses. The complexity can also lead to security gaps, resulting in intrusion by bad actors being less likely to be detected, especially if organisations have issues with shadow IT.

This trend of added complexity is also mirrored in many organisations' security ecosystems. There is an increasing requirement for organisations to implement multiple security solutions from numerous vendors, making the management of alerts difficult. This is particularly a concern for businesses that have an IT team that has also been tasked with managing the business's security posture.

There is no sign of this trend slowing down, so it is important to take steps to manage this complexity and consider the security ramifications of implementing new technology solutions.

80

The number of SaaS applications an average organisation uses

Source: BetterCloud Inc.





Changes to Ransomware Attacks and Payments

Ransomware is no longer a novel form of cyberattack, especially as ransomware has been the most newsworthy form of attack for many years. You might believe that with ransomware being as common as it is, security solutions would be able to block all forms of this malware.

However, this is not the case as the methods that ransomware gangs use are constantly changing. Now, as most businesses have a comprehensive backup solution, ransomware gangs have pivoted to double extortion ransomware. This is where a bad actor exfiltrates data before encrypting it, giving them additional leverage to collect ransom payments, even if the business can restore data from a backup.

There are also other attack methods gaining popularity within the ransomware community, such as malvertising, which is particularly pertinent in 2023, with Google changing their extension manifest to stop adblocking plugins. Other ways that ransomware is changing include an increased prevalence of supply chain compromise and bad actors setting the ransom payment to the exact amount that can be claimed from the company's cyber insurance.

This risk is compounded by the simplicity of acquiring ransomware payloads, as they can easily be purchased from the dark web, for a low price.

These changes to ransomware can be difficult to keep up to date with, however, businesses need to do so, as the average cost of ransomware remediation is \$1.96 million.

www.ransomware.onion

Botnets & Malware Stampado Ransomware - FUD - CHEAPEST - ONLY \$39 - ...

All your files have been encrypted

Stampado Ransomware - FUD - CHEAPEST - ONLY \$39 - FULL LIFETIME LICENSE

Stampado Ransomware - You always wanted a Ransomware but never wanted to pay hundreds of dollars for it? - This list is for you! :) Stampado is a cheap and easy to manage ransomware, developed by me and my team. It...

Sold by **The_Rainmaker** - 2 sold since Jul 12, 2016 **Vendor Level 1** **Trust Level 5**

	Features	Origin country	Features
Product class	Digital goods		Worldwide
Quantity left	Unlimited	Ships to	Worldwide
Ends in	Never	Payment	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 39.00

Scarcity of IT and Security Talent

The skills shortage is affecting most industries, especially businesses looking for skilled IT and security professionals. This can be seen as 84% of businesses are unable to find skilled security employees.

With the lack of security talent, small and medium businesses are priced out of the market for hiring a cybersecurity or information security employee, even though they are still at risk. SMBs make attractive targets for cybercriminals as they typically lack security controls and are the path of least resistance. Unfortunately, due to the size of these businesses, they typically are unable to recover from a cyberattack.

Even for businesses with an in-house IT department, the skills shortage has meant that they have also been tasked with managing security, which is typically not sufficient.

Whilst the skills shortage commonly relates to hiring, with cybersecurity it also extends to the basic security skills of employees. As the cybersecurity threat landscape is constantly changing, many employees lack basic security awareness knowledge and are unable to accurately detect a potential social engineering attack.

84%

of businesses are unable to find a skilled security employees

Source: CyberEdge Group

It is important to note that the cybersecurity skills shortage does not only affect 'end-user' businesses but also vendors and service providers, which makes it even more important to work with trusted providers.





Reliance on Less Mature Third Parties

Over the past 3 years, we have seen more supply chain disruptions than ever before. From chip shortages to Brexit, it has affected all businesses. One of the reasons why supply chain disruptions are more common is due to an increased reliance on third parties, partly due to the abundance of SaaS solutions and the skill shortage.

This can increase the cyber risk of a business as working with a third party requires trust that they will handle data correctly. Some of these third parties that increase cyber risk include marketing agencies, SaaS application vendors, service providers, developers and hardware vendors. This can especially be seen with IoT device manufacturers, where novel devices are sold to businesses with multiple vulnerabilities.

This risk is made worse by the fact that legislation, such as GDPR and the European Banking Authority, places liability on the organisation that owns the data, which is typically the business, rather than the provider. This trend is likely to continue under the NIS2 directive.

It also makes auditing more difficult, as many businesses would struggle to complete a comprehensive internal audit due to the complexity of their supply chain.

Whilst there are security concerns with reliance on less mature third parties, there is also a business continuity concern, as downtime from higher in the supply chain can result in downtime for your business.

Targeting the Weakest Link

The goal of security vendors is to mitigate cyber risk and combat emerging threat vectors. Whilst it is true that they are doing a great job of this and constantly innovating to stay ahead of the curve, many security controls can be circumvented by a skilled social engineer, targeting an employee that lacks cybersecurity awareness training.

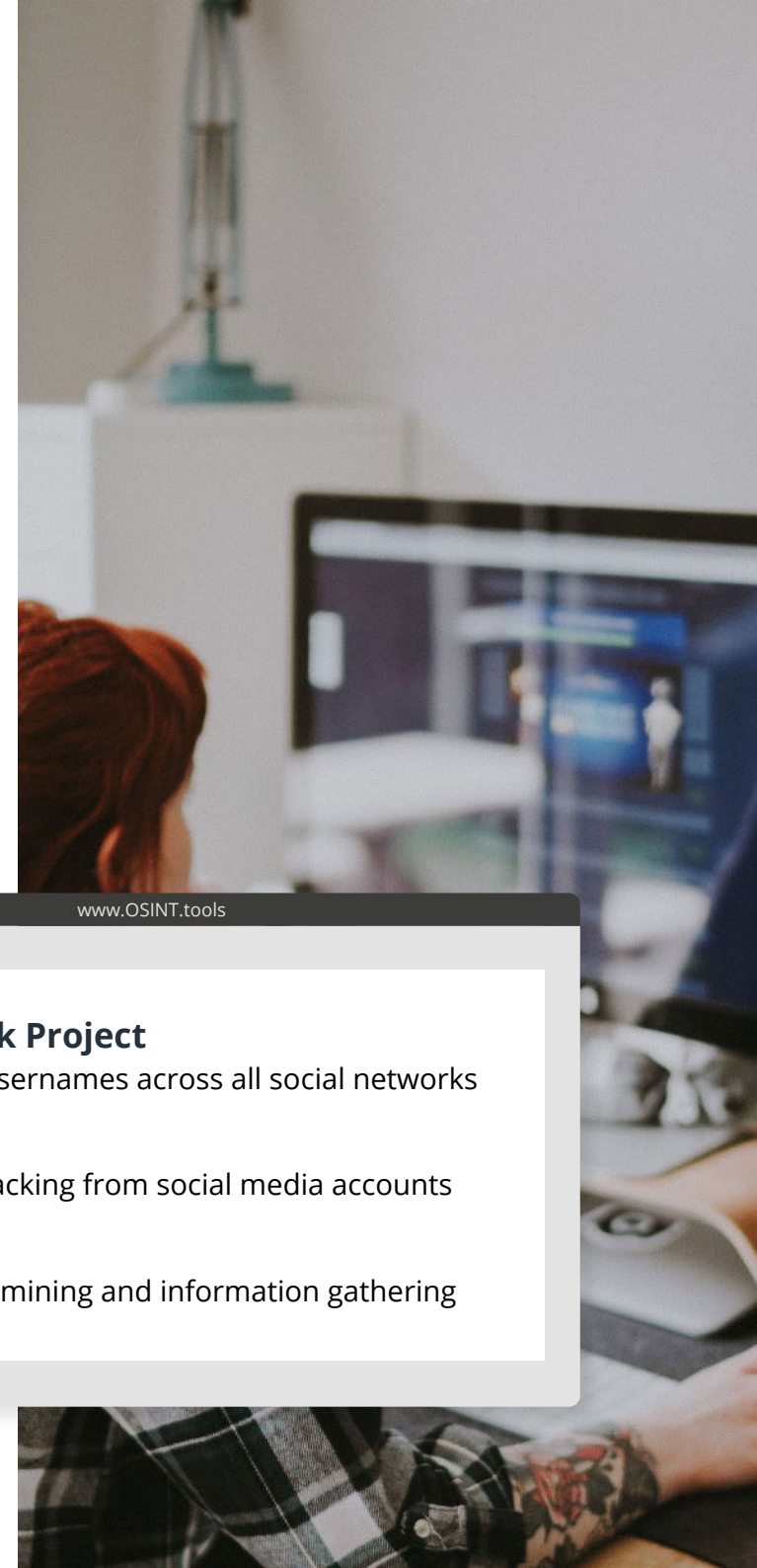
In 2022, the most common occurrence of this was SIM swapping. This is where an attacker transfers a victim's mobile phone account and phone number to a new SIM card, allowing them access to accounts, and giving them the ability to impersonate the victim. This form of attack is initiated by social engineering a mobile phone provider to transfer the phone number.

This risk is made worse by the fact that individuals have a vast digital footprint, that can be used by bad actors to craft spear phishing attacks. Some of the information that can be used includes the date of birth (from 'happy birthday' posts), names of children and pets, hobbies, spouse names, business travel information, EXIF data from images and out-of-office information.

Whilst this information seems innocuous, it is perfect for a spear phishing campaign, or smarter brute forcing of passwords.

Some of this information can be acquired through social networking sites, such as LinkedIn, Facebook and Twitter, but bad actors can use tools such as The Sherlock Project, Creepy and Maltego.

With this vast library of information, you can see how cybercriminals can easily craft targeted attacks that are difficult to detect by security solutions or individuals.



www.OSINT.tools

The Sherlock Project

A tool to find usernames across all social networks

Creepy

Geolocation tracking from social media accounts

Maltego

Real-time data mining and information gathering

A modern office interior with a mix of materials. The walls are a combination of light-colored wood paneling and red brick. The ceiling is exposed with wooden beams, silver ductwork, and long, white, rectangular light fixtures. In the foreground, there are several wooden tables with black metal legs. One table has a brown leather sofa and a grey armchair around it, with a potted plant on the sofa. In the background, there are more tables, office chairs, and a person sitting at a desk. A white door with an 'EXIT' sign is visible on the left side.

How to Best Protect your Business



Reduce the Attack Surface

One of the consequences of the ever-expanding complexity of technology ecosystems is that it also increases the available attack surfaces for bad actors. The attack surface now includes cloud services, IoT devices, servers, local networks, development environments and everything in between.

Reducing the attack surface makes it easier to manage the growing complexity of technology ecosystems. This can be achieved through a variety of methods. In regards to applications, businesses should remove any SaaS solutions and applications that are not used, and create a process for implementing new solutions to reduce the risks associated with shadow IT.

When considering networks, organisations should inspect all domains and DNS, segmenting networking where necessary. There are also solutions available to scan for open ports and close those that do not need to be open.

There are also solutions available to analyse the available attack surface, such as Weave Scope and Deep Fence Threat Mapper. If your business does not have the in-house expertise to use these solutions or act on the suggestions, a trusted third-party provider will be able to assist.

Businesses should strive for zero trust, where possible. Whilst this may be difficult, after following the previous steps to reduce the available attack surface, zero trust should become a more viable option.

Ideally, businesses should also monitor all network traffic to detect any potentially suspicious activities.





Dynamic Defence

As the cybersecurity threat landscape is constantly changing, your business needs defences that can dynamically adapt to these changes. If your business relies on static defences, you may be at risk of having a significant investment that is circumvented by a zero-day exploit.

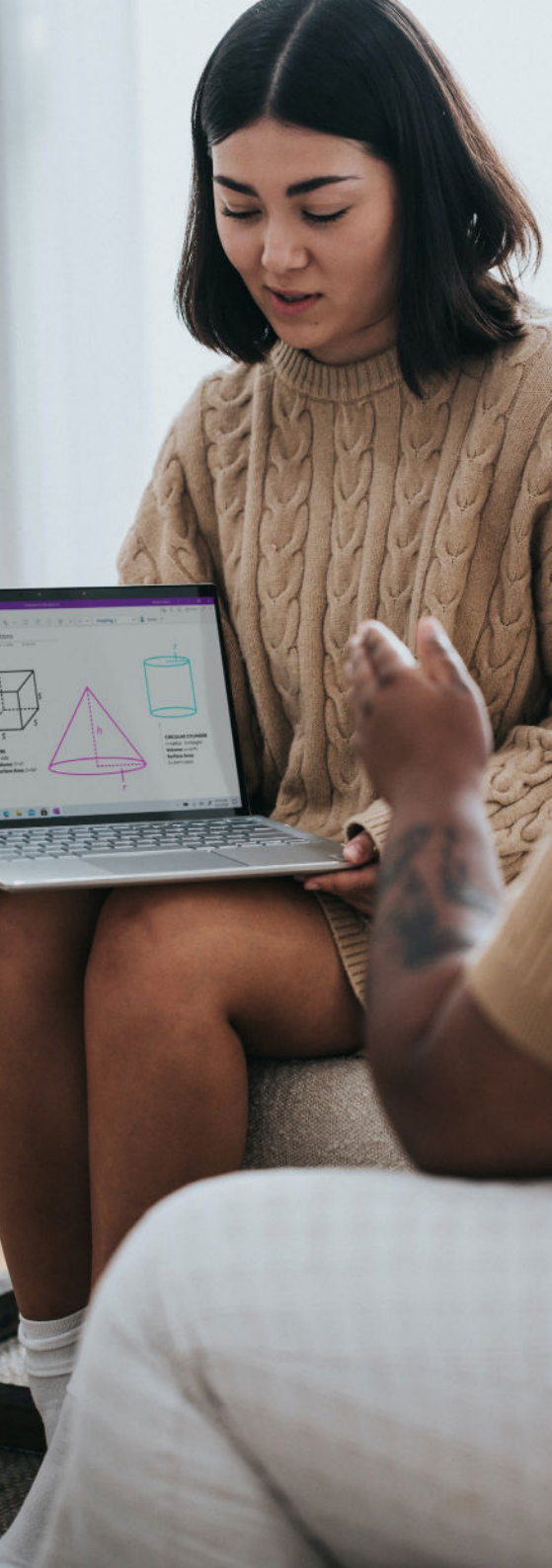
An example of how businesses have moved to dynamic defence is the change from a simple antivirus solution to endpoint detection and response (EDR). In the past, legacy antivirus solutions would scan for malicious code running or within files. This was made obsolete with the advent of fileless malware.

EDR solutions solve this issue as they collect data to form a baseline of 'normal' activities, through the use of artificial intelligence and machine learning. Therefore, an EDR solution can flag any 'abnormal' activity made by a user or endpoint. This means it can detect a compromised account or malware, regardless of whether it is a known exploit, zero day exploit or fileless malware.

However, an EDR solution only scans endpoints and does not solve the issue of a complex technology ecosystem. Thankfully, there is a new generation of security solutions that cover cloud services, IoT devices and networks, known as extended detection and response (XDR).

XDR solutions use the same behaviour mapping, but for additional services. This form of dynamic defence ensures that your business is ahead of the curve.





A Combined Effort of AI, Automation and Human Intervention

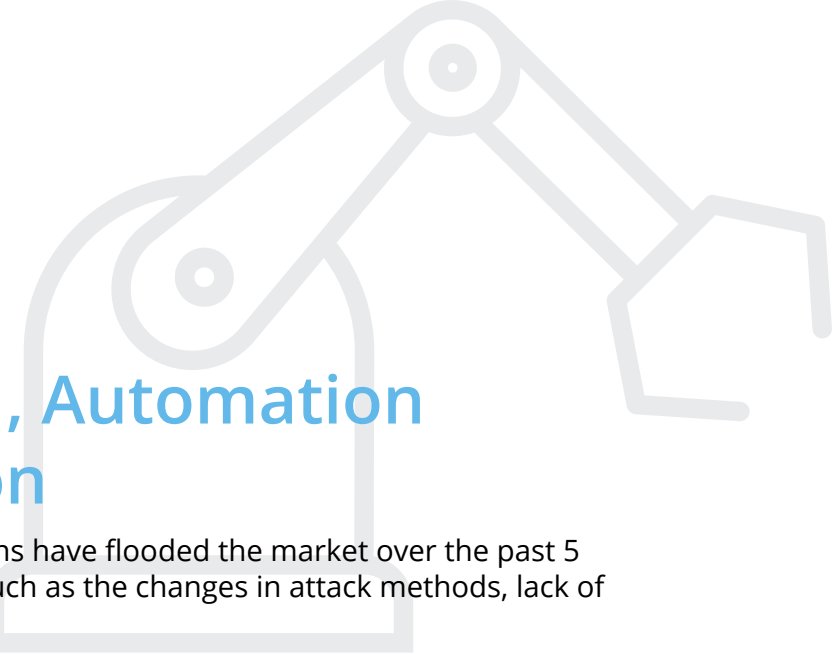
AI-based cybersecurity detection and response solutions have flooded the market over the past 5 years. They do solve many issues regarding security, such as the changes in attack methods, lack of dynamic defence and the complexity of IT ecosystems.

The latest wave of innovation within this space has extended the functionality of these solutions to include automated remediation. This saves time, as no action is required by a human, whilst improving security, as it addresses the vulnerability immediately. It also improves consistency, as the same workflow is followed every time, and aids with compliance, as details logs are recorded for every remediation action.

Most solutions have different levels of automation for remediation, to suit different use cases. For example, it is possible to simply notify a system admin of a potential breach, or it is possible to require the System Admin to approve any remediation action. Some solutions allow for full remediation, without input from the System Admin.

Whilst these solutions can provide immense benefits for organisations, unfortunately, we are not yet at a stage where all security controls and actions can be, or should be automated. It is still recommended that businesses protect themselves with the assistance of a security professional.

Therefore, businesses should rely on the combined effort of AI detection, with automated responses, approved by a trusted third-party advisor.





Education and the Impact of Security Culture

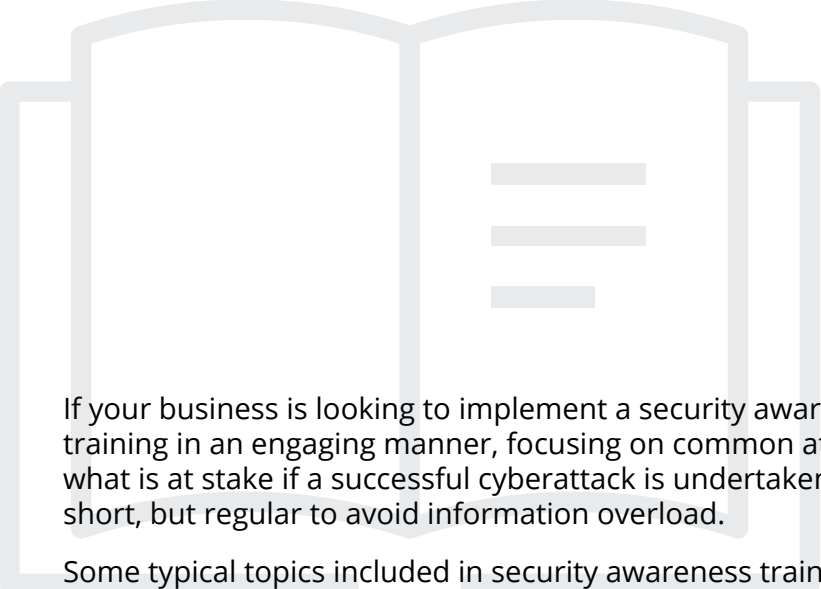
As cyber defences grow stronger, more bad actors will target individual employees, with advanced social engineering attacks, as it will reach a point where employees are easier to target than software or systems. Although many businesses invest in security solutions, some neglect security awareness training for employees, or do not complete training regularly to keep employees up to date with the current attack methods.

All employees within an organisation have a responsibility to maintain the security posture, so it is important to give employees the knowledge and tools to do so.

Security awareness training creates a strong security culture which can:

- Decrease the chance of success attacks
- Reduce human error
- Lead to behaviour changes to reduce cyber risk
- Help with security audits
- Lead to a more engaged work force in general



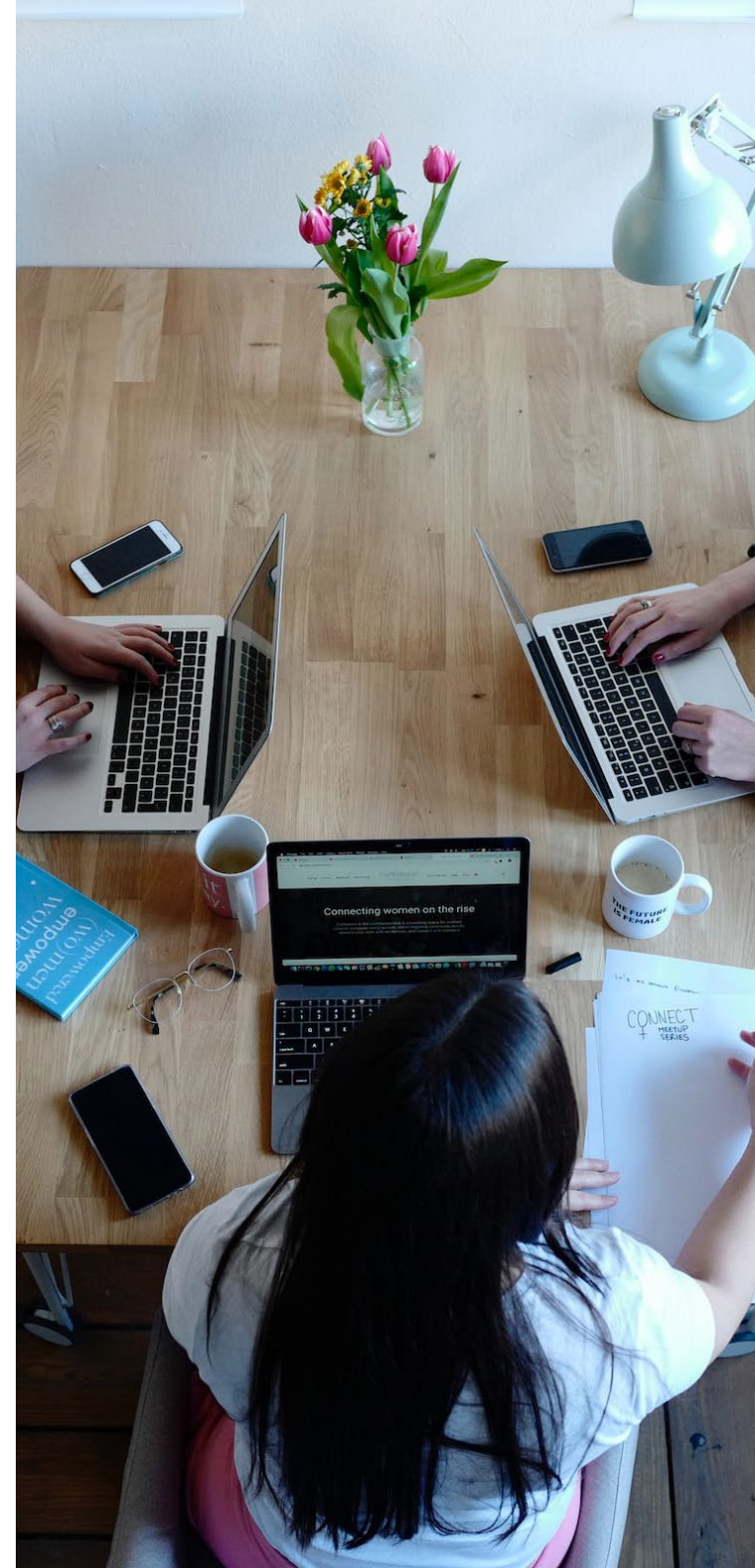


If your business is looking to implement a security awareness program, you should deliver the training in an engaging manner, focusing on common attack methods, how to spot them, and what is at stake if a successful cyberattack is undertaken. These training sessions should be short, but regular to avoid information overload.

Some typical topics included in security awareness training include:

- Phishing awareness
- Password security
- Privacy concerns
- Insider threats
- Physical security hygiene (entry passes, PII on screens and paper, entry to buildings, WFH privacy risk, etc.)
- Shadow IT
- CEO fraud
- Vulnerabilities of data in motion
- Social engineering techniques

Some businesses also implement phishing tests, if your business chooses to, the result should only be used for positive re-enforcement rather than punishing those that have less knowledge of security.





Rely on the Assistance of a Trusted Provider

With the way that the cybersecurity threat landscape is evolving, security is now an essential component of all businesses. For this reason, your security should be managed by a team of professionals.

A trusted provider will be able to create a bespoke security solution that meets your business needs, improve your security posture and reduce the chance of falling victim to a cyber attack.

They will also be able to monitor any alerts, making use of the latest innovations in AI and automation, whilst still handling human intervention when necessary.

This allows you to focus on running and growing your business, without having to worry about whether a cyberattack will lead to downtime or loss of business.

A trusted provider can also give you access to talent that would typically be too expensive for a business to hire an individual or team to manage. Many providers will have a team that includes experts on different areas of security, whilst also having experience in other technology solutions, enabling them to manage your entire IT ecosystem.

Moving to a security provider also can decrease your IT expenditure, with a simple monthly cost, allowing you to easily stick to your technology budget.



How We Can Help

The field of cybersecurity is constantly changing, and it can be difficult to keep up.

If your business is yet to truly take cybersecurity, make 2023 the year that you invest in security and take the necessary steps to protect your business. If your business already has a security solution in place, you should regularly review its effectiveness to ensure there are no gaps that could result in a cyberattack.

Thankfully, you don't need to go through the process alone, and we can help you implement controls and manage your security posture. To find out more, get in contact with us today and we will be happy to help.

 | Anywhere



iris.co.uk/products/iris-anywhere/



0344 815 5555

