stryke.

Navigating the Digital Frontier

A Cyber Security Retrospective and Outlook

Introduction

In the ever-evolving landscape of the digital age, the past year has seen unprecedented challenges and triumphs in the world of cyber security. With 2023 fast becoming a distant memory, for many it was a year marked by relentless cyber threats and ingenious defence strategies, with little time to reflect, learn and prepare for the year ahead.

It's critical that we keep an eye on the trends that will shape 2024 and beyond in the dynamic world of cyber security.

In this eBook, we'll take a look back at what happened in 2023 and share some of our thoughts for 2024. We will highlight the cutting-edge tools, solutions and strategies that will help empower businesses in the face of today's security challenges.

We'll close things off by showcasing the critical role played by Stryke, in defending organisations against the ever-growing array of digital threats.

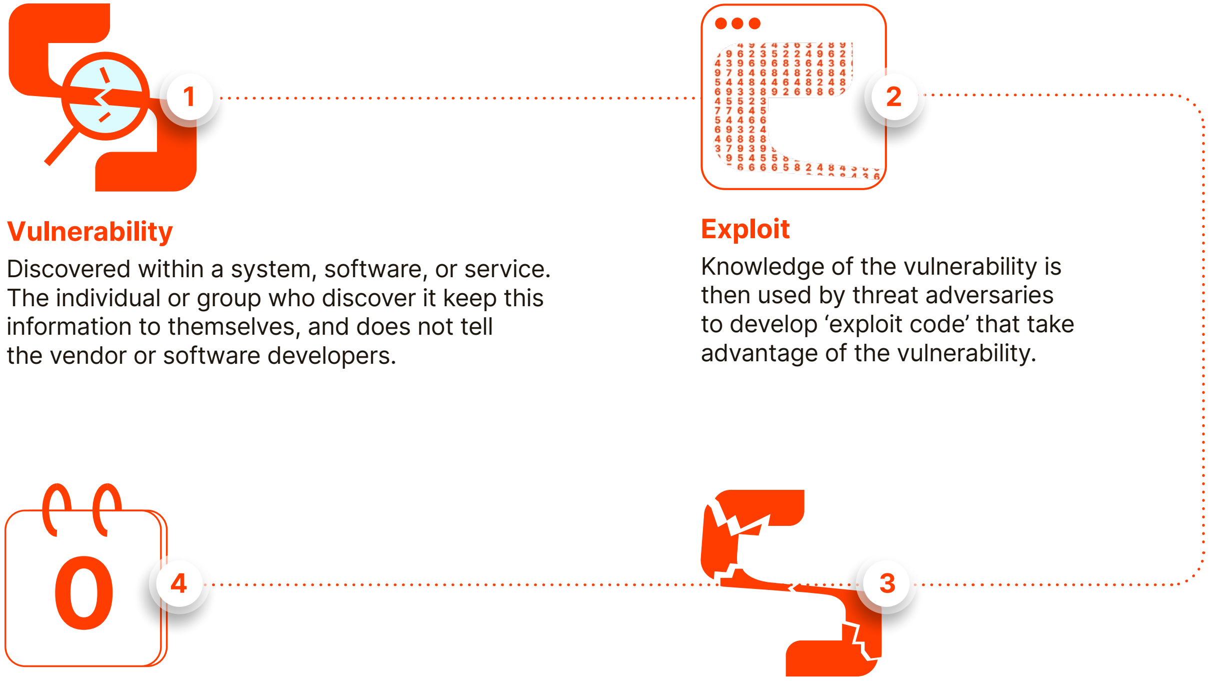
It's time to Stryke.

Contents

What happened in 2023?

Zero-Day vulnerabilities

Zero-day vulnerabilities in 2023 increased in a big way, but what are zero-day's? They are actually 4 individual events:



Vulnerability

Discovered within a system, software, or service. The individual or group who discover it keep this information to themselves, and does not tell the vendor or software developers.

Exploit

Knowledge of the vulnerability is then used by threat adversaries to develop 'exploit code' that take advantage of the vulnerability.

Attack

The exploit is used to perform a series of coordinated cyber attacks on the vulnerable system, software or service.

Day Zero

This is the day the vendor or software developer learns of the vulnerability, meaning they are already on the back foot and must act quickly to find a fix. This is what makes Zero Day attacks so harmful and damaging.

MOVEit

The 2023 MOVEit cyber attack was executed by CL0P, a Russian affiliated ransomware group, who exploited a zero-day vulnerability (CVE-2023-34362).

It impacted over **2,500 organizations** and **64 million individuals**, leading to financial damages of around **£10 billion**.

This breach was far reaching and affected entities globally, including significant organizations and government agencies across the US, UK, and Canada.

The attack was notable for its use of a SQL injection flaw allowing unauthorized access to MOVEit servers. In response, the MOVEit team collaborated with cybersecurity experts and agencies to issue patches and advisories, mitigating the breach's impact.

This incident highlights the critical importance of proactive vulnerability management and the need for rapid response mechanisms to address zero-day exploits effectively.

Evolution of cyber threats through AI adoption

Next, we saw the evolution of cyber threats through the adoption of AI. The threat landscape never stops changing, but in 2023 we saw first-hand how **AI technology** was used to enhance the sophistication of the techniques used by hackers. Whilst we know that AI is being applied in a positive way to solve real-world cyber problems, it is also being used in the opposite way by **hackers to cause harm**.

The target for these new types of attacks are users and employees. In particular, social engineering attacks which exploit gaps in the human security chain. We spoke to a well-known Global Cyber Advisor, who told a great story about these dangers. He was able, 'with permission', to use widely available voice cloning software to **pretend to be a CFO of a company**. Using this software, he managed to persuade an employee of said company to make a payment into his bank account.

Remote workforce challenges

The final observation in our retrospective is how remote working creates challenges for modern businesses. Today's workforce differs significantly from previous years, primarily due to the widespread adoption of remote and hybrid working. While this facilitates communication from any location, it introduces a number of new challenges for CISO's to deal with.

Social engineering attacks can exploit employee communications in hybrid or remote-first environments, and ransomware threats may target personal or insecure company-owned devices. Although these tactics are not new, the increased frequency of attacks highlight a persistent threat, particularly for less cyber-aware users. Encouraging employees to rethink cyber security in a remote work setting and become security advocates, is crucial for safeguarding this evolving threat vector.

While traditional security measures remain essential, the modern CISO must strike a balance to ensure employees are able to perform their jobs securely, while remaining productive. With **74% of cyber security breaches caused by human error**, security awareness training, with a focus on social engineering and ransomware, remains the most effective approach for securing remote workforces.

74% of cyber security breaches are caused by human error

Ever-Changing Regulatory Landscape

Why does the regulatory landscape always change?

Let's kick things off with the regulatory landscape and try to understand why cyber-regulation is having to continually evolve.

The regulatory landscape changes for many reasons – reflecting shifts in society, technology and the economy, but the primary driver has to be technology evolution, where rapid advancements often out-paces existing regulations. New technologies introduce novel risks and opportunities, prompting regulators to **update rules** to address these challenges, close **loop-holes** and ensure the responsible use of technology.

Another strong reason is to even-out the playing field across different geographies so that cyber security is harmonised, and everyone is subject to the same rules.

This is where NIS2 comes in.

NIS2 - What and Why?

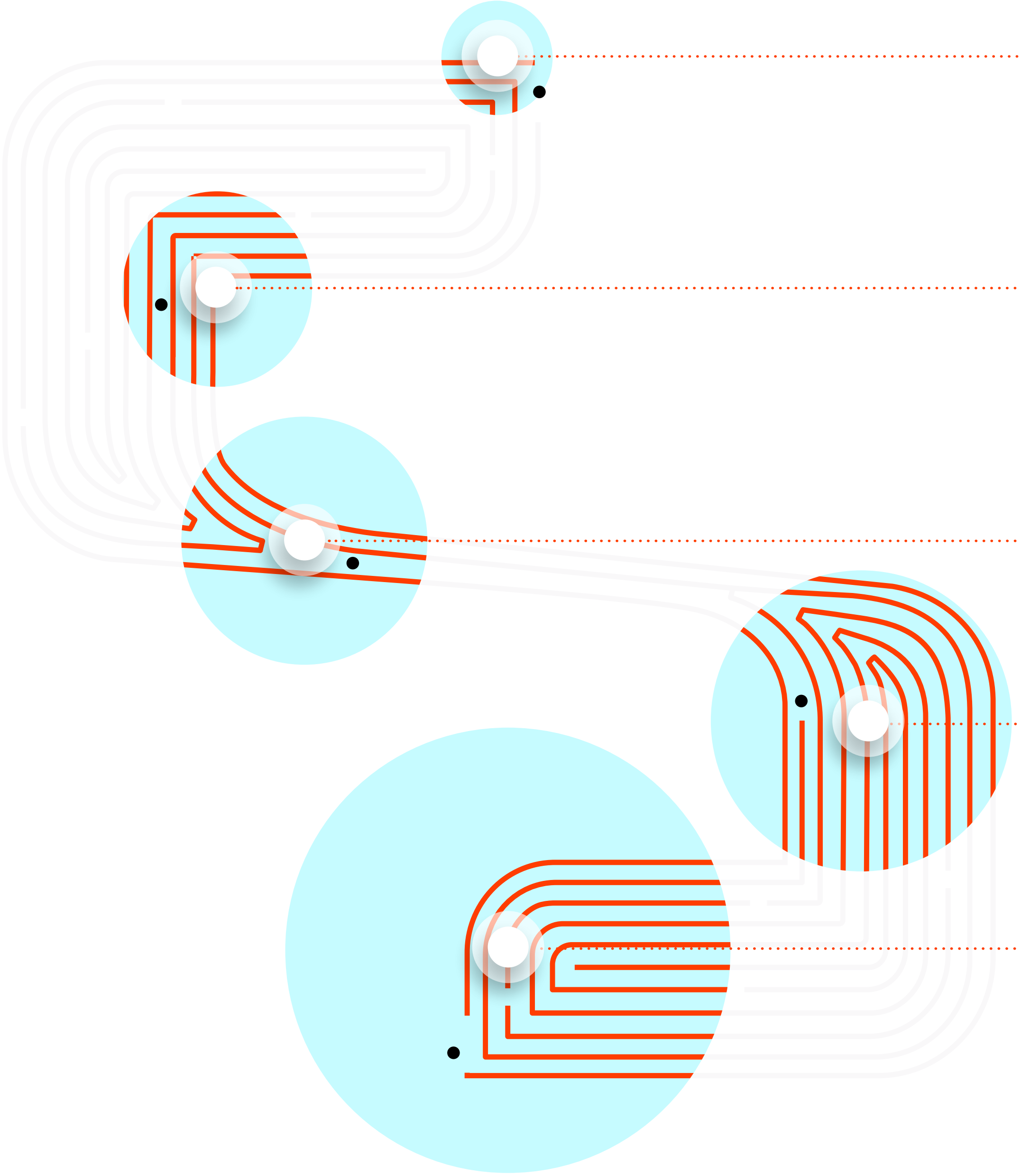
In short, NIS2 is a European Union directive aimed at **standardising and enhancing cyber security** across member states. It primarily impacts critical infrastructure operators in what we call Essential and Important sectors – think of industries like healthcare, water, utilities and transport. Its primary objective is to increase the **cyber resilience** of these sectors, and to standardise cyber security across member states over the long-term.

The directive includes requirements for security incident reporting, risk management, supply chain security, and training. NIS2 has already come into force, but all EU member states have until the 17th October 2024 to transpose NIS2 into their own national law.

Stryke is leading the charge in keeping our partners and customers up-to-date with all the changes. We will have a wealth of NIS2 resources available on our website, **sign up to access** to the latest information and steps you will need to take to achieve NIS2 compliance.

Sign up

NIS2 – What do I need to do?



Step 1: Understand the NIS2 Directive

The first step is to do your homework – to become a NIS2 champion and raise awareness within your organisation. The market needs to be educated on the impact of NIS2 and we anticipate this will be as disruptive as the General Data Protection Regulation (GDPR) which came into force back in May 2018.

Step 2: Determine if your Business is Affected

The NIS2 directive applies to organisations classed as Important or Essential sectors and that meet certain size criteria based on number of full-time employees, business turnover etc. Speak to Stryke to see if your business is affected, we will run through some basic qualifying questions with you.

Step 3: Choose a known Security Framework (ISO 27001)

We believe that with a tried and tested security framework such as ISO 27001, you'll get around 60% of the way there when it comes to demonstrating NIS2 compliance.

Step 4: Compliance Requirements and Implementation

To ensure compliance, it is important to develop and implement policies that align with the requirements of the NIS2 directive. The earlier you start planning and implementing these requirements, via a process change or cyber technology investment, the better.

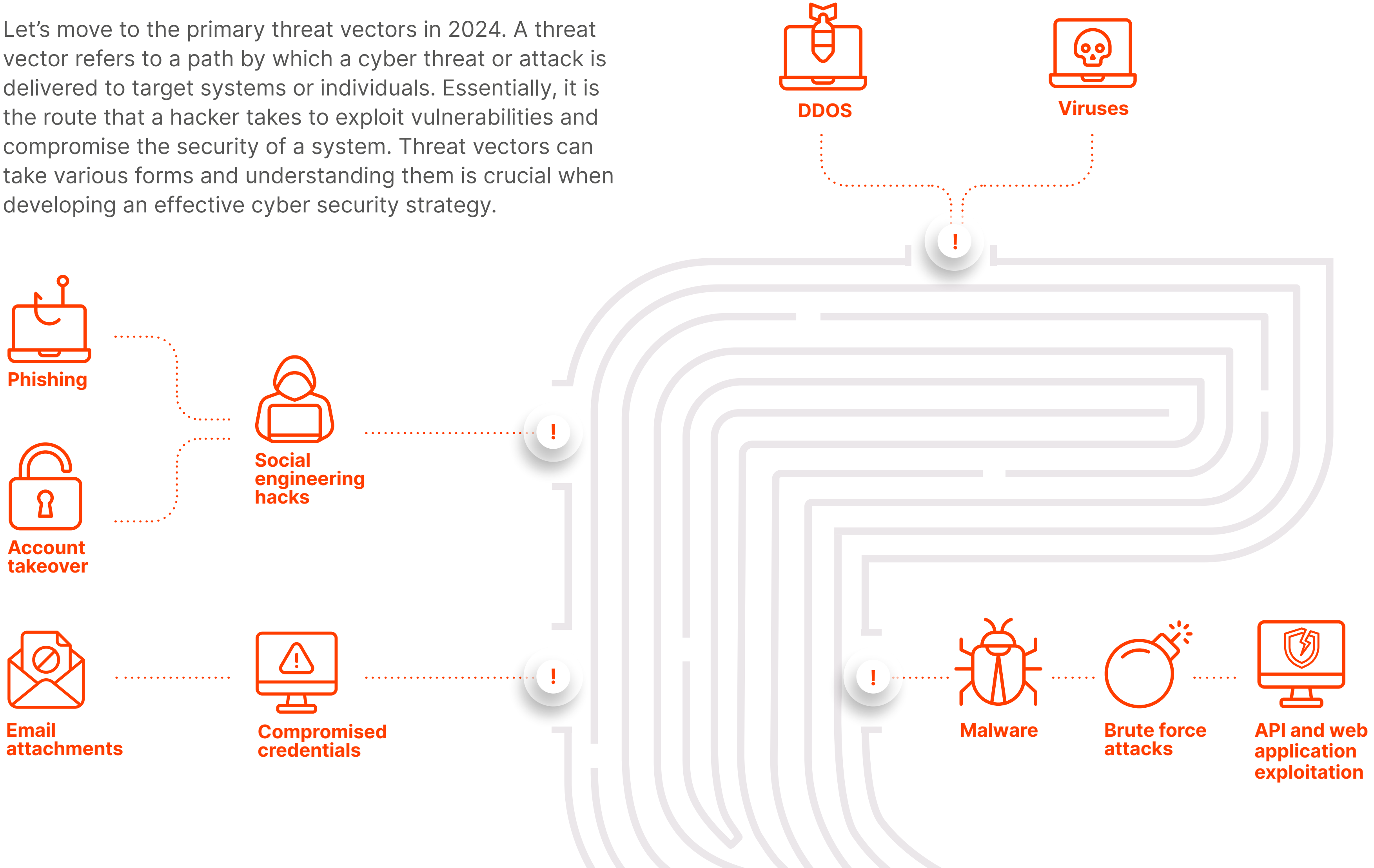
Step 5: Stay Informed and Compliant

NIS2 is in its infancy, and it is likely to undergo further changes, including the enforcement date. So, it is crucial to stay informed about the latest developments and requirements of the NIS2 directive. This may include updates on compliancy requirements, enforcement procedures, and potential penalties for non-compliance.

Sign up here to keep ahead

Predictions on the Primary Threat Vectors

Let’s move to the primary threat vectors in 2024. A threat vector refers to a path by which a cyber threat or attack is delivered to target systems or individuals. Essentially, it is the route that a hacker takes to exploit vulnerabilities and compromise the security of a system. Threat vectors can take various forms and understanding them is crucial when developing an effective cyber security strategy.



DDOS

Viruses

Phishing

Account takeover

Social engineering hacks

Email attachments

Compromised credentials

Malware

Brute force attacks

API and web application exploitation

Email

Organisations encounter a variety of email and phishing threats on a regular basis, ranging in complexity and volume. Beyond phishing, various categories of email threats exist, encompassing issues such as data infiltration, business email compromise, and even account takeover.

94% .... of malware is delivered by email
Verizon

57% .... of organisations see weekly or daily phishing attempts
GreatHorn

41% .... Phishing was the leading infection vector, identified in 41% of incidents, making it the most common initial threat vector
IBM

Email threats are not going away and it should be on your list of priorities for 2024.

Ransomware and DDos as-a-Service

Hacking as-a-Service is the commercialisation of hacking skills via software, making otherwise complex skills and techniques widely available to pretty much anyone who is willing to pay for them. While hacking as-a-Service is nothing new, there has been an increased rise in the use of these types of tools and services, particularly with ransomware and DDoS as-a-Service.

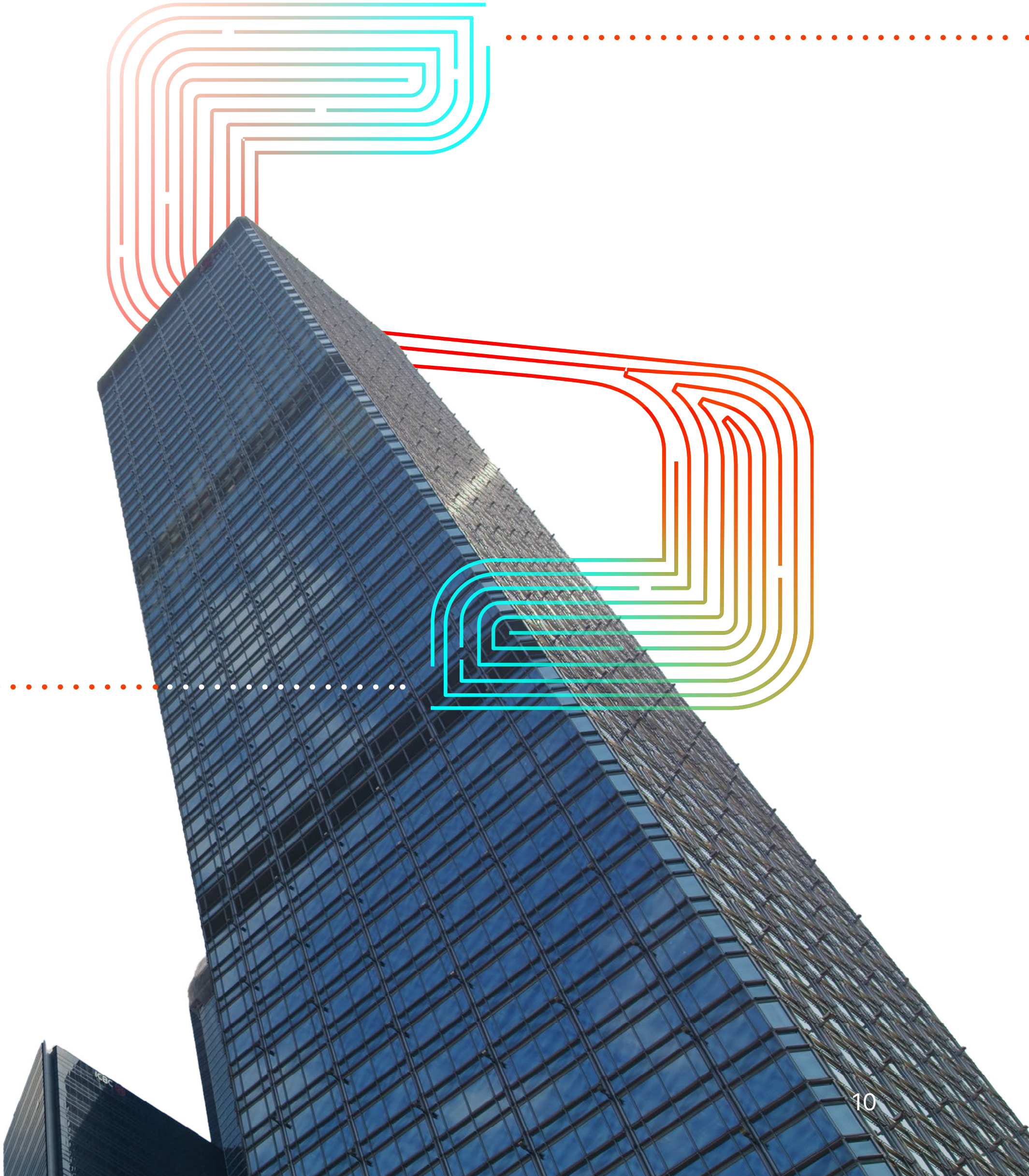
Over the course of 2023, eCrime adversaries continued to prove their ability to adapt, regroup and flourish, despite all of the defensive measures put in place. After some noteworthy ransomware attacks that shutdown businesses in 2023, these **ransomware affiliates have now moved to a new ransomware as-a-Service (RaaS) model** in light of the success they have been having. This means that more and more hackers can gain access to the tools and techniques required to continue this activity.

Cyber Security Insurance

Why should you consider cyber security insurance?

In straightforward terms, cyber insurance helps organisations to mitigate the financial impact of cyber attacks. Cover can encompass compensating for lost revenue caused by business interruption or managing claims arising from a data breach or cyber attacks against your company.

It is important you choose the right type of cover for your business, **based on your own requirements and attitude towards risk.**



Cyber Insurance premiums have surged in 2023 by

50%

Cyber security insurance is changing with the cyber landscape

Let's explore why the cyber security insurance is evolving with the cyber landscape and why certifications like ISO 27001 alone are **no longer good enough to protect your business**.

Given the size of the losses organisations experienced due to cyber attacks in 2022 and 2023, those with cyber insurance reported that their insurers have made substantial updates to their policies in the last year. This, combined with increased remote and hybrid workforce numbers, has meant that the cyber landscape is more complex. As a result, cyber insurance premiums surged, with a **50% increase in 2023** and look continue to rise throughout 2024.

To secure the levels of cover required, organisations are required to demonstrate robust cyber security practices, extending beyond security certification like SOC 2 and ISO 27001 or typical multi-factor authentication. Insurers are looking for controls around privileged access management, incident response, data encryption, cyber security awareness training, vulnerability management, and zero-trust network architecture.

Certifications such as ISO 27001 go a long way. However, it is fundamental to have the right security solutions in place, as organisations must demonstrate a commitment to security for insurance coverage in the first place.

Some food for thought

We recommend treating your **cyber insurance provider as a strategic partner**. Think of it this way – building a working relationship through consistent communication will only help when it comes to both renewals and claims procedures.

Those responsible for security in their organisations should take a proactive and transparent approach in the partnership, and openly share their cyber security strategy beyond the formal application processes or filling out rudimentary questionnaires. It's crucial to acknowledge that cyber insurance companies possess extensive data on cyber security risks and losses, so it is worthwhile paying attention and taking their advice!

Addressing the Cyber Security Skill Gap

Skills shortages and the talent density within cyber & information security teams

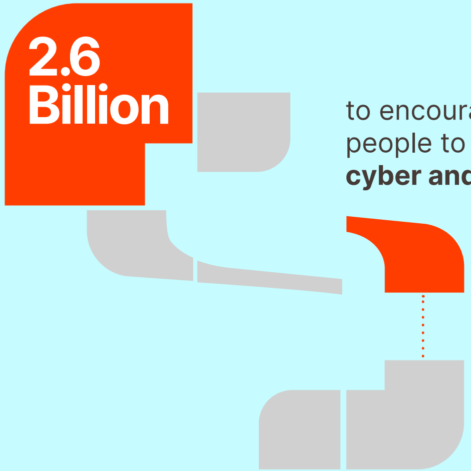
Research conducted in July 2023 by the Department for Science, Innovation and Technology gave some pretty good insights into the situation in the UK right now, highlighting that **50% of all UK businesses have a basic cyber security skills gap** and around **33% have an advanced cyber security skills gap**. These figures are similar to 2022 and 2021.

In the last 12 months alone, there were 160 thousand cyber security job postings. This is an **increase of 30%** compared to this time last year and of those 160 thousand, around 140 thousand were filled, leading to this biggest shortfall we have ever seen. But it isn't all doom and gloom. Having the right security partner is fundamental to success. With Stryke, we are your trusted Security Partner, providing as-a-service solutions which help you plug the security skill gap.

Humans have always been a notoriously weak link in the security chain due to things such as social engineering and lack of awareness. We are now seeing a whole new 'breed' of risk in the threat landscape driven by the **lack of professionals in the security space**. This trend promises to continue and we expect the skills-shortage gap to widen even further in 2024.

What is the UK doing to address the cyber security skills gap?

The government said it was working to increase the number and diversity of skilled people in the cyber security profession. It added that the **£2.6 Billion National Cyber Strategy** included plans to encourage young people to develop their cyber and technical skills, and to take subjects such as computer science at college and university level. National Cyber Strategy plans for 2024 are expected to be released by the UK government soon, sharing details on this initiative.



to encourage young people to develop their **cyber and technical skills**

Cyber Security Tools and Solutions

90%

of successful Malware attacks are delivered by email

In no particular order, we recommend you look at tools and solutions that directly tie in with some of the topics we've discussed today.

Phishing Simulation, including Security Awareness Training

Simulating phishing emails across your organisation (provided only a few key individuals know about the simulation) helps identify vulnerabilities. Clicking on a simulated phishing email highlights the need for cyber-security awareness training and to educate employees on what to watch out for in real scenarios and minimise risks. It's good practice to have these phishing simulation programmes running in the background that automatically send test-emails on a regular basis.

WAF

A Web Application Firewall or WAF, protects your website and other web apps by sitting between the user and the app. This not only allows filtering, monitoring and blocking of any malicious traffic, but also prevents any unauthorised data from leaving the app. The best part is that you can completely protect your web app or website against DDoS attacks.

Email Protection

With over **90% of successful Malware attacks being delivered by email**, having good email protection is critical.

Email protection refers to a set of measures and solutions implemented to secure email communication. We have already discussed a number of these but it includes Anti-Phishing Measures, Spam Filtering, Malware and Virus Detection, Email Encryption and Data loss prevention.

Effective email protection is a critical component of any comprehensive cyber security strategy, as it helps organisations and individuals to minimise the risks associated with cyber threats delivered through email channels.

Conclusion

As we conclude this exploration of the cyber security frontier, it is clear that the digital landscape is both a battleground and a playground (depending on your perspective!) – it's a place where cyber threats and innovation coexist. Stryke, with its portfolio of world-class technology partners, combine years of industry know-how to offer a comprehensive portfolio of Security Services to protect and support your business.

As we enter 2024, armed with insights from the past and a proactive vision for the future, **Stryke remains at the forefront** of all cyber developments. We are committed to working hard for our customers and help them navigate the landscape of cyber risk.

As this eBook presents, the digital security is everchanging and being one step ahead of cyber criminals is key to the success and longevity of your business.

At Stryke, we don't just implement a security solution and walk away, we become your trusted Partner. We will truly understand your business so we can support you in identifying and remediating risk, and putting the best security steps in place to secure your critical assets.

Get in touch today to see how we can help

Contact us today

www.stryke.com