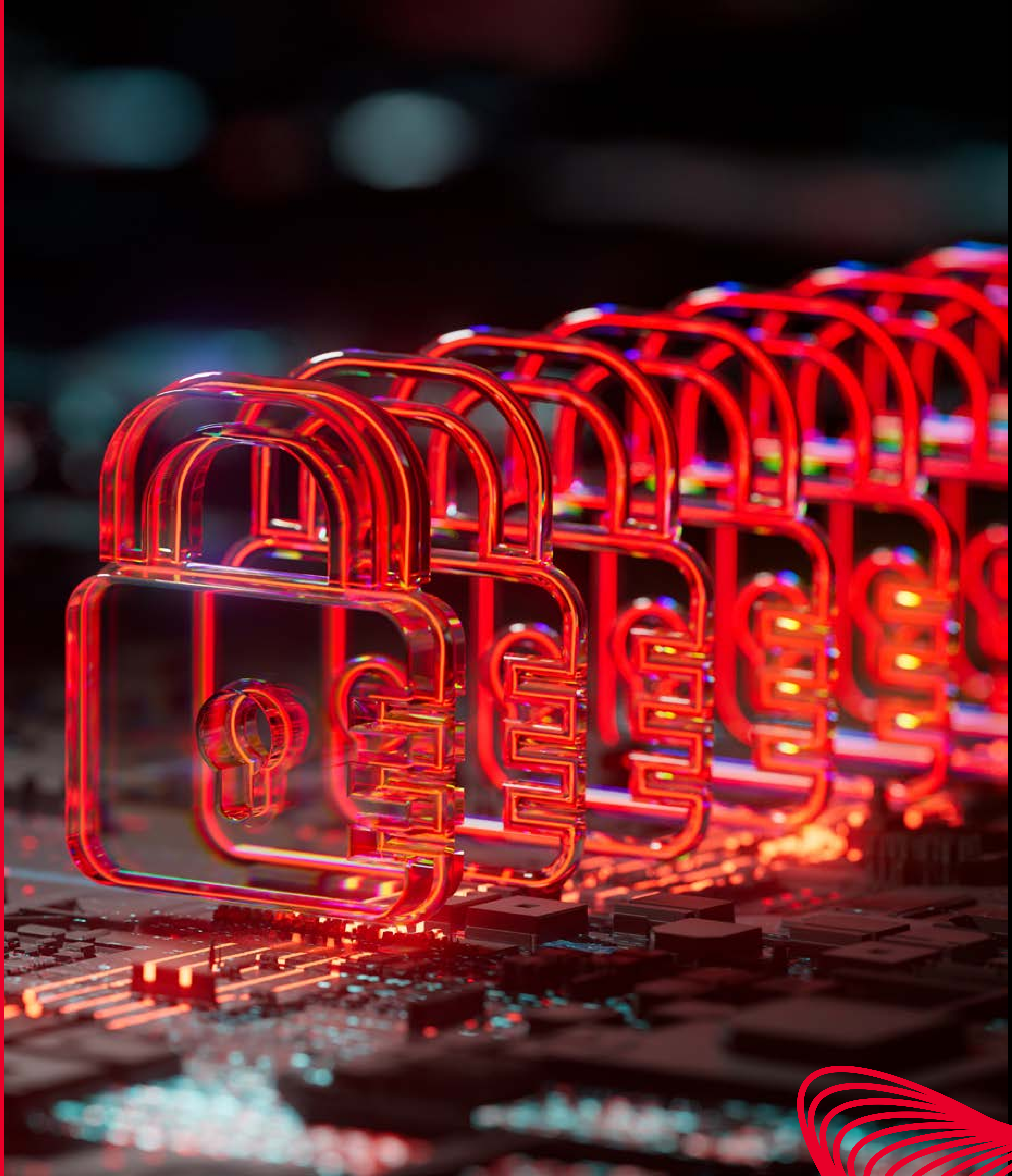


Red Helix

Holding Data Hostage: The Business Impact of Ransomware

CONTENTS

Understanding the Urgency of Today’s Most Disruptive Cyber Threat

Ransomware attacks have continued to plague businesses throughout 2025.

Marks & Spencer faced a ransomware attack that went viral earlier this year. The attack was pervasive, affecting the company’s IT systems and operations. The disruption meant that they were unable to accept online orders and with the BBC reporting that on average £3.8m is spent on clothing and home products on its website and apps every day, the profit loss is unimaginable.

After the viral Marks & Spencer’s attack, Harrods and Co-op were targeted with other ransomware attacks. Their online and onsite services were impacted with Co-op having to shut down parts of its IT system.

Public bodies face similarly persistent cyber-attacks. Though we are aware of many ransomware attacks on public bodies, we rarely learn the full details of the attack, but this is set to change. The introduction of the Cyber Security and Resilience Bil introduces tougher regulations on reporting cyber incidents to the government.

There is no doubt that ransomware is a serious threat. So, let’s explore the rise of ransomware, the widespread consequences, the challenges of ransomware attacks and the multi-layered solutions that are currently available.

The Rise of Ransomware

What is ransomware?

Ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. This is typically sent by a malicious group or actor who will then try to extort money from the company they have attacked in exchange for the data or decryption.

There are multiple reasons why the criminals will threaten to leak company data, violating customer privacy, or legal regulations, but primarily it is for financial gain, to humiliate a specific company, or for claimed altruistic reasons. Attackers most commonly access a company's networks via phishing emails, or through an unpatched vulnerability on a company's IT estate.

Ransomware is different from other cyber attacks because it is more invasive within a network. Ransomware attacks encrypt company data, giving the hackers sole access. This means that systems are debilitated with no method of re-operating without appeasing the malicious actor.

Ransomware has evolved into a sophisticated adversary. Attackers now use techniques such as encrypting malicious payloads, polymorphic malware, and multi-stage attacks that can lie dormant until triggered. These innovations make ransomware more elusive, often evading traditional detection systems.

Prevention against ransomware is more complex and demands a sophisticated, multi-layered approach to cyber security. Ensuring proper protection via encryption, firewalls, and access controls are not solely for preventative purposes. These security measures anticipate, detect, and remediate ransomware threats before they can cause harm to your networks.

The rise of ransomware

Ransomware attacks are here to stay. More than 40% of UK organisations experienced a cyber security breach or attack in the last 12 months.

The profitability of ransomware attacks makes them highly attractive to cyber criminals. When a business's operations halt, many choose to pay ransoms in exchange for quick restoration of services, reinforcing the incentive to continue these attacks. Even when companies refuse to pay ransoms, attackers can profit by selling stolen data or offering access to other malicious actors.

High-profile groups like REvil, DarkSide, and Conti have refined tactics like double extortion, where data is not only encrypted but also exfiltrated, with the threat of public release if the ransom is not paid. This has hit large organisations hard, with Maze ransomware making waves by targeting businesses like Canon and LG Electronics using this method.

The Ransomware-as-a-Service (RaaS) model further increases accessibility for less experienced hackers by allowing them to "rent" ransomware tools. This is something Conti famously used during its 2021 attack on Ireland's Health Service Executive (HSE), which crippled healthcare services across the country.

While attacks result in ransomware payments, they are going to continue to increase. Attackers don't need to be especially technical and benefit from anonymity while they can hide behind their screens. They can also send out a high volume of ransomware emails, increasing the likelihood that someone will fall for the attack by mistakenly clicking a malicious link.

This has solidified the existence of ransomware groups such as LockBit, Conti, DragonForce and Clop. All have taken responsibility for some of the biggest ransomware attacks within the last few years. Their targets have included government organisations, large technology companies, and manufacturing operators.

INSIGHT-2983 - CREDENTIAL ACCESS WITH EXECUTION AND INITIAL ACCESS
7/11/2021
0365 - Threat Intel Match

Consequences of Ransomware

Ransomware attacks are among the most disruptive and financially damaging threats that an organisation faces. As their sophistication and frequency increase, organisations across sectors are being forced to reckon with far-reaching consequences. These extend beyond the direct victims, impacting entire supply chains, stakeholders, and even national security. Understanding these ramifications is crucial for organisations aiming to bolster their cyber resilience.

Financial Impact

The financial toll of ransomware attacks is severe and multifaceted. According to the Guardian, the average ransomware payment made by UK organisations is £870,000 with some organisations admitting they have paid £10-£20 million. However, ransom payments are only the tip of the iceberg.

The true cost of an attack includes expenses associated with forensic investigations, system recovery, legal fees, regulatory fines, customer notification obligations, and investments in upgraded security infrastructure. Cyber insurance may offset some costs, but it often falls short of covering the total damages, particularly in prolonged attacks.

A report by Infosecurity magazine reported that 58% of organisations hit by ransomware shut down operations in order to recover. The financial impact for a business shutting down for potentially weeks is unparalleled and can be detrimental.

Supply Chain Risks

Ransomware's reach often extends well beyond the initially targeted organisation, particularly when third-party vendors, suppliers, or partners are connected through digital infrastructure. A single compromised entity can become a gateway to a broader network, triggering cascading failures across the supply chain. This interdependence makes it essential for companies to assess the cyber maturity not only of their internal systems but also of their entire ecosystem.

Operational Disruption

Beyond monetary losses, the operational disruption caused by ransomware is the most immediate and tangible consequence. These attacks can freeze entire IT systems, halting production lines, disrupting logistics, and preventing access to vital business applications. For hospitals, it might mean the unavailability of patient records or critical equipment. For manufacturers, it can lead to costly delays and missed contract deadlines. In November 2024, a ransomware attack on a major supply chain technology firm resulted in a range of disrupted logistics for companies such as Starbucks and Morrisons.

In another high-profile incident, faced by Redcar and Cleveland Council a cyber attack in February 2020 disrupted all of their systems from bin collections to social services. Mr Martin who was the Chief Executive at the NCSC said, "If a council are telling you they are worried about their ability to run services for vulnerable children, you take that very seriously." The systems took 10 months to be fully restored, as many of the systems had to be rebuilt from scratch.

Reputational Damage

One of the most immediate and enduring effects of a ransomware incident is reputational harm. When a company's systems are compromised, it signals to customers, partners, and the broader market that its data and infrastructure were not adequately secured. This erosion of trust can lead to customer attrition, difficulties acquiring new clients, and strained business partnerships. In highly regulated industries such as finance or healthcare, this perception of vulnerability can be especially damaging, potentially leading to loss of accreditation or stricter oversight.

Surveys indicate that if consumers found out their personal information was breached by a provider; 46% said they would switch insurance companies, 35% would switch hospitals, and 39% said they would get a new lawyer. Thus, the reputational cost is not just theoretical it translates directly into lost revenue and business opportunities.

Legal and Regulatory Consequences

Increasingly, organisations are facing legal repercussions following a ransomware breach. Data protection laws such as the UK GDPR impose strict obligations on companies to safeguard personal data. Failure to do so can result in regulatory investigations, fines, and class-action lawsuits.

For example, the Information Commissioner's Office (ICO) fined a software services provider £3.07 million after a ransomware incident impacted critical services such as the NHS with healthcare professionals unable to access patient records. The investigation found that the attacker had gained access to 79,404 people's personal information including details of how to gain entry into the homes of those receiving care.

The consequences of ransomware are profound and multifaceted ranging from financial devastation and operational paralysis to reputational harm and legal exposure. In today's digital economy, the question is not if, but when an organisation will face such a threat. Preparing for that eventuality through robust multi-layered security, incident response planning, and supply chain risk management is no longer optional, it is essential.

Challenges of Defending Against Ransomware

Despite increasing awareness, and the devastating impact of ransomware attacks, effective and foolproof protection remains elusive. The challenges are multifaceted, encompassing technical, strategic, and human factors.

Widespread Attack Vectors

Ransomware can infiltrate organisations through a multitude of attack vectors, with phishing attacks remaining the most common. 83% of businesses identified phishing as the primary method used by attackers to deploy a cyber attack. These phishing campaigns are often highly targeted and sophisticated, using social engineering tactics to impersonate trusted brands, executives, or vendors. Employees may be tricked into clicking malicious links or downloading infected attachments, unknowingly opening the door to an attack.

The emotional manipulation inherent in phishing schemes makes them particularly difficult to combat. Even experienced professionals can be fooled when emails appear to come from known contacts or exploit urgent scenarios like payment processing or account compromise. The rise of generative AI tools has made phishing attacks more sophisticated, enabling attackers to create highly convincing messages at scale. Often without the usual warning signs like spelling errors or poor grammar.

Defending against these threats requires a layered approach. Robust email filtering systems, real-time threat intelligence, and multi-factor authentication are essential. However, technological solutions must be paired with consistent employee training. Regular simulated phishing exercises and awareness campaigns can dramatically improve an organisations resilience. A 2024 report by KnowBe4 found that companies conducting monthly phishing simulations saw a 60% reduction in click-through rates over six months.

The weaknesses of complex digital infrastructures

While phishing dominates, it is far from the only entry point for ransomware. Attackers also exploit vulnerabilities in outdated software, misconfigured cloud services, weak remote desktop protocol (RDP) settings, and exposed APIs. Domain spoofing, watering hole attacks, and malicious browser extensions are also used to gain a foothold in organisational networks.

As organisations adopt more complex digital infrastructures including hybrid work models and cloud-first strategies the attack surface grows. Each new device, user, or service introduced into the network can become a potential vulnerability if not properly secured. Maintaining strong cyber hygiene including prompt patch management, network segmentation, and strict access controls is more critical than ever.

Inadequate Incident Response and Recovery

Despite the prevalence of ransomware, many organisations remain unprepared for an attack. One of the most significant challenges is the lack of a well-defined, regularly tested incident response plan.

Without clear procedures for detection, containment, and recovery, organisations may face extended downtime, higher ransom demands, and greater data loss. The absence of secure, regularly updated backups further exacerbates this issue. Many victims are forced to pay ransoms simply because they lack an alternative path to recovery.

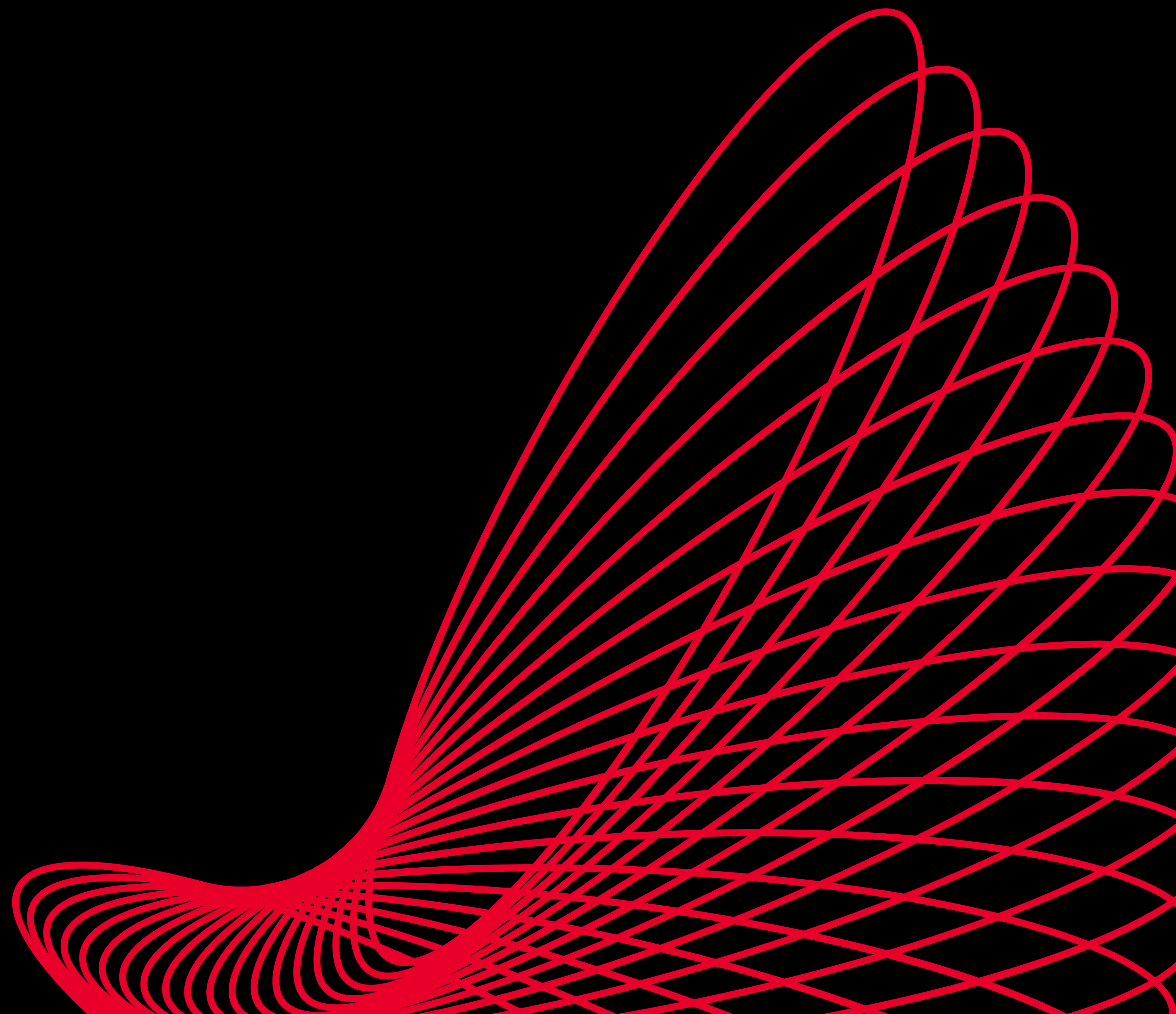
It is important to note that, the response shouldn't end once the immediate threat is resolved. Post-incident analysis and remediation are essential to close the gaps that allowed the attack in the first place.

Alarmingly, only 31% of companies have conducted a cyber security risk assessment in the past year.

The Role of AI and Emerging Technologies

Artificial intelligence and machine learning offer promising avenues to enhance ransomware defence. AI-driven threat detection can identify suspicious behaviour faster than traditional methods, flagging anomalies such as unexpected file encryption or unusual login activity. AI can also bolster phishing detection, analysing email metadata, content, and patterns to identify threats in real time.

However, the same tools are being weaponised by cyber criminals to automate attacks, personalise phishing emails, and evade detection. This arms race underscores the need for proactive, adaptive defences, combining technology with strong policy enforcement and human awareness.



The Ransomware Solution

Once a malicious file is activated, often via a phishing email, it can begin encrypting data across a company's network, rendering systems inaccessible. Attackers then demand payment in exchange for decryption keys. The impact is swift and significant, affecting not only internal operations but also external stakeholders across the supply chain.

While backup systems offer a means of recovery, restoring systems from backups can be time-consuming and complex. In many cases, organisations require the assistance of a specialist incident response provider to investigate the breach, contain the damage, and support recovery efforts. This process may take days or weeks, during which time business operations are severely disrupted.

In response to the growing threat, the UK Government has proposed a reporting framework requiring victims to notify authorities before making ransom payments. This reflects growing concerns about the long-term effectiveness of paying attackers, particularly given that payment does not guarantee that stolen data will be returned or that systems won't be targeted again.

How to protect your company

Defending against ransomware requires a multi-layered cyber security strategy. A holistic approach will allow you to evolve alongside constant technological advancements, whilst remaining compliant with regulatory frameworks.

If ransomware criminals can infiltrate an endpoint, they can encrypt it with ransomware and spread throughout your estate. An Endpoint Detection & Response (EDR) solution will identify the threat and allow you to isolate an affected endpoint before the issue spreads. Combine this with Network Detection & Response (NDR) and any threats on your network will be similarly identified and your security team alerted. Layering both together and ingesting all alerts into a Security Information & Event Management (SIEM) will give you full visibility and allow your Security Operations Centre (SOC) to identify and respond to anomalies immediately.

Previous solutions, such as VPNs are almost redundant against ransomware attackers. If your network has implemented a VPN solution, attackers can gain visibility into the entire network. Instead, Zero Trust Network Access (ZTNA) ensures that in the worst-case scenario that a hacker has infiltrated your system, they are prevented from accessing the entire network. By implementing specific and contextual access policies, access is only granted into specific areas. This ensures that the inflicted damage is minimised. In conjunction with other layers of defence, this is more effective.

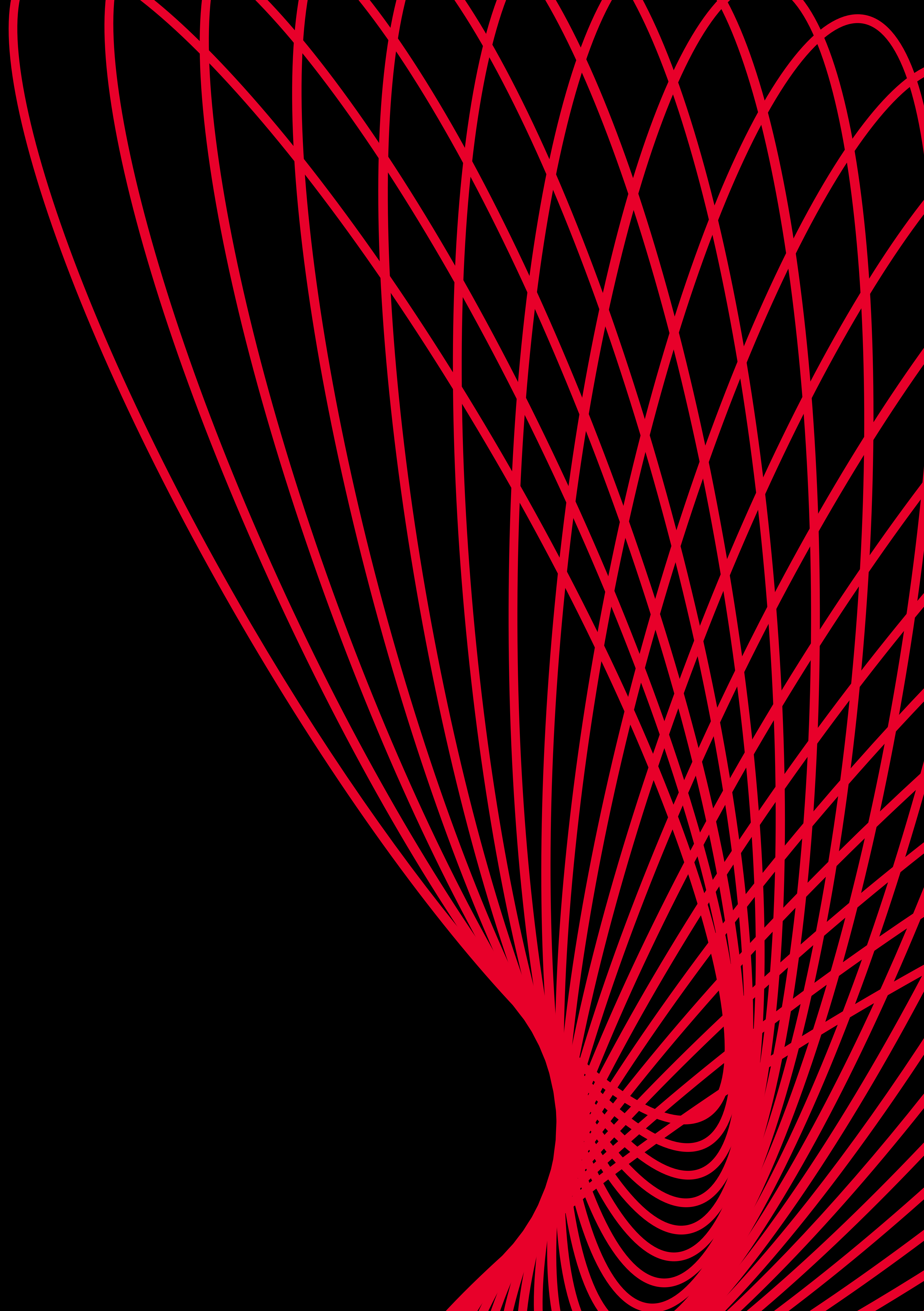
Additionally, good cyber hygiene will reduce the likelihood of a successful attack. This includes comprehensive patch management and educating your employees on common ransomware techniques to help them identify red flags. This decreases the likelihood of people clicking links and reinforces your first line of defence.

Halcyon's Anti-Ransomware Solution

For organisations seeking to further strengthen their defences, advanced anti-ransomware solutions provide additional safeguards. Halcyon's anti-ransomware solution provides an intelligent agent that captures the encryption event, shuttles the keys into a secure enclave and, after the malicious process is blocked, automatically decrypts any impacted files on the endpoint. This eliminates any need for your organisation to even consider paying a ransom.

Importantly, such platforms are designed to integrate with existing endpoint security solutions, offering additional layers of defence without requiring wholesale changes to security architecture.

Cyber criminals target everyone either directly or indirectly. By creating a multi-layered defence, you will build a truly secure security infrastructure.



Contact Red Helix
today and revolutionise
your IT security.

☎ +44 (0)1296 397711

✉ info@redhelix.co.uk

Phoenix House
Smeaton Close
Aylesbury
Buckinghamshire

Red
Helix

redhelix.com