CYBER ALCHEMY
ASSESS - PROTECT - ENABLE

The Essential Guide to Cyber Threats in 2024

cyberalchemy.co.uk

Foreword

Worried about cyber security? You're not alone.

A business is hacked every 37 seconds.

That means that, in the time it takes you to read this foreword, four CEOs are dealing with the fallout of a data breach.

You're probably aware of the cyber threats facing your business - phishing, ransomware, DDoS attacks similar have plagued workplaces for years.

Unfortunately, while many businesses are worried about these threats, they lack the understanding or support to actively defend against evolving attack methods.

Equally, many IT teams are aware of the risks, but lack the infrastructure and support to ensure the business is adequately defended.

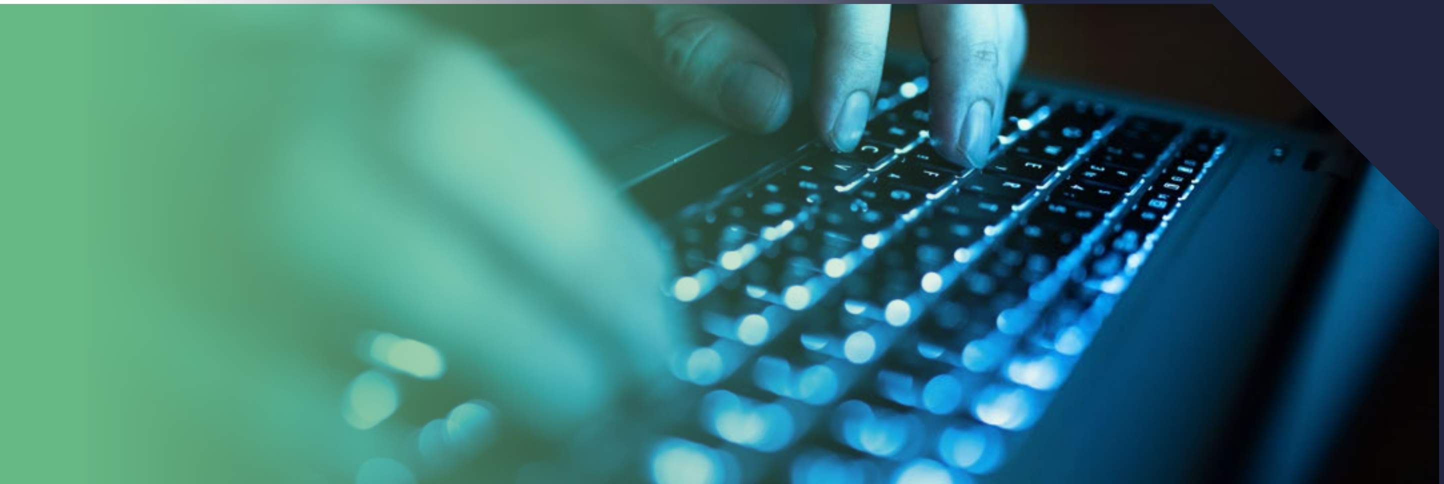
If you lack robust cyber security, a 'breach' isn't an arbitrary risk. Data protection laws are stricter than ever, and a breach could lead to heavy fines and reputational damage. Sophisticated cyber criminals work extremely hard to bring businesses like yours to a stand-still.

Downloading this guide is your first step to a more secure future.

By the end of it, you'll have a comprehensive understanding of the current cybersecurity landscape. You'll know what emerging trends threaten your business, and most importantly, have actionable strategies for effectively safeguarding your business.

Whether you own the business, or you're responsible for the IT within it, downloading this guide gives you a roadmap for ensuring your organisation is well-equipped to handle an ever-evolving cyber threat landscape.

Neil Richardson
Founder



Contents

The stakes

It's difficult to overstate the importance of cyber security. Every business needs to be cyber secure. Even if that business is one person working from a laptop at home.

The truth is, many businesses don't actively develop their cyber security strategy. They may not have the knowledge, or the budget, or they simply don't see it as a priority. Whatever the reason, hackers take advantage of this to devastating effect.

Why? Because hackers are opportunistic. Most cyber attacks exploit basic vulnerabilities in the target infrastructure. That might involve taking advantage of a lack of staff training, or brute force hacking a business email without multi-factor authentication.

That's why phishing remains the most common cyber threat. Although the emails have become easier to detect, it doesn't require any specialist IT knowledge and beyond that Phishing is not just a technical problem, but a human one. Its possible to send out thousands of emails and wait for an unwitting victim, or even specifically target a range of individual with an Phishing campaign bespoke to that specific individual.

So what's at stake?

- **Reputational damage:**
  Cyber attacks can tarnish a company's reputation, leading to a loss of trust. This damaged reputation can hinder the adoption of new services or products, impacting your company's growth and market position. Imagine having to inform customers, stakeholders and partners that their data may have been accessed by a malicious third party.
- **Your defences:**
  The cyber threat environment is constantly changing, with new vulnerabilities and attack methodologies emerging regularly. Businesses that don't update their cyber security strategy accordingly leave themselves more exposed to attacks.
- **Innovation and future growth:**
  Cyber attacks risk more than current operations; they threaten the heart of business innovation. Intellectual property theft and the diversion of resources in response to breaches can severely impede the development of new products and services, eroding competitive advantage. Effective cybersecurity protects not only current assets but also future innovation and market leadership.
- **Regulatory compliance:**
  Many industries are subject to stringent regulatory requirements regarding data protection. Data breaches threaten a business's compliance status, especially if they are found to be at fault for the attack.
- **Business continuity:**
  Cyber attacks can lead to lengthy downtime and large financial losses if the business isn't prepared. Proactive cybersecurity measures help maintain operational continuity and minimise the impact of any breaches.
- **Customer trust:**
  Demonstrating a commitment to cybersecurity strengthens customer trust and confidence - vital in an era where customers are increasingly aware and concerned about their data privacy. Especially as a number of attacks now target supply chains and look to leverage trust relationships between existing organisations.
- **Competitive advantage:**
  Demonstrating robust measures is becoming increasingly important in a more security-conscious world. For instance, Cyber Essentials certification is now a requirement for bidding on many government contracts and many third parties require the adoption of robust frameworks such as NIST2, 27001 and CIS18.
- **Mitigating financial risks:**
  Cybersecurity breaches can be financially devastating. Investing in proactive security measures is far more cost-effective than the expenses incurred from a breach, which can range from remediation costs, legal fees, and loss of business.
- **Securely integrating new technology:**
  As businesses increasingly adopt new technologies (like cloud services, IoT, and AI), understanding the security risks is essential. Implementing new technology securely minimises the risk of creating new vulnerabilities whilst being able to take advantage of the benefits this technology brings.

The threat landscape in 2024

Whether you work in education or entertainment, cyber crime is a constant threat. In today's digital age, attacks have become more sophisticated and prevalent - from bored teenagers to state-sponsored groups, anyone with a computer and some basic IT knowledge can launch an attack.

This new threat landscape is constantly evolving, but trends have emerged:

Ransomware's continued rise

Data is the backbone of modern business. It's therefore a valuable target for cyber criminals.

Ransomware encrypts an organisation's data, with the attacker demanding payment for its release. This can cripple operations, and is especially disruptive in sectors like healthcare and local government. Attacks that shut down operations here don't just cause financial losses; they can significantly disrupt critical services.

The evolution of ransomware into double extortion tactics (threatening both data encryption and public release) amplifies its danger. Organisations might recover from the operational impact of data encryption, but the reputational damage and breach of trust from leaked data can be irrecoverable, posing an existential threat.

Phishing scams

Gone are the days where phishing emails were characterised by obvious scams and riddled with grammatical errors.Cyber criminals are now more adept at crafting convincing phishing emails, making these attacks more dangerous than ever.

Personalised messages, official-looking links and logos, and sophisticated social engineering techniques have made it more challenging for individuals to distinguish between legitimate communication and malicious attempts. Once the victim has followed the instructions (usually clicking a download link or entering information on a spoof website) the scam serves as an entry point for more destructive attacks.

Phishing is also evolving, with techniques like spear phishing and whaling. These more targeted attacks involve attackers extensively researching their targets for more convincing fraud attempts.

The Threat Landscape in 2024
Continued

Credential theft and reuse

This involves stealing usernames and passwords to access many accounts, especially when the same password is used more than once. Thieves often use tricks like phishing, recording keystrokes via malware, or third party breaches to get these details. The impact can be huge, including stolen identity and financial loss.

Social engineering – adapting and evolving

As technical security measures improve, attackers increasingly rely on social engineering to sidestep these defences. They adapt to new technologies and communication trends, using them to craft more convincing scams. Techniques like phishing, pretexting, the use of tools like WhatsApp and MS Teams evolve with societal changes. Attackers exploit current events and technological advancements to manipulate victims into giving away sensitive information or granting access to secure systems.

Supply chain vulnerabilities

Attackers are exploiting weaknesses in the supply chain to access larger networks. By targeting less secure elements in the supply chain, they can compromise the security of major organisations by exploiting existing trust relationships, both technical and human.

Remote work vulnerabilities

The shift to remote work has expanded the attack surface for many companies, with cybercriminals exploiting weak home networks and unsecured devices, especially where the line between corporate devices and personal devices becomes blurred. The ability of a user to access key company accounts and data from their unsecured devices increases the risk and likelihood considerably.

Advanced Persistent Threats (APTs)

These are sophisticated, prolonged attacks typically sponsored by state actors or major criminal organisations, aiming to steal information or disrupt operations - and they're becoming a tool in global politics, affecting not just governments but businesses of all sizes. With tensions rising internationally, especially between the West, China, and Russia, APTs target a broad range of sectors, including those seen as 'insignificant.' No organisation is too small; as larger entities fortify their defences, attackers turn to smaller, less protected ones as entry points or targets of opportunity.

The Threat Landscape in 2024
Continued

AI-powered attacks

Artificial Intelligence (AI) has not only revolutionised many industries but also opened a new frontier for cyber threats. AI-powered cyberattacks are more sophisticated, faster, and harder to detect than traditional methods. These attacks include:

- **Adaptive malware:** AI-driven malware that changes its behaviour to avoid detection.
- **Automated hacking:** AI systems that automate the process of finding and exploiting vulnerabilities.
- **Targeted phishing attacks:** AI-crafted phishing emails that convincingly mimic trusted sources.

Internet of Things (IoT) vulnerabilities

The proliferation of IoT devices, often lacking robust security, presents a growing risk. Vulnerabilities in these devices can provide hackers with access to broader networks.

Deepfakes

Deepfakes involve synthetic media where a person in an existing image or video is replaced with someone else's likeness. They pose unique threats, such as:

- **Impersonating executives:** Creating videos or audio recordings mimicking company executives.
- **Manipulating stock markets:** Using fake announcements to influence stock prices.
- **Undermining trust:** Eroding trust in legitimate communications by creating convincing fake content.

Cloud jacking via misconfigurations

The migration to cloud services increases risks such as misconfigured cloud settings and targeted attacks on cloud infrastructures. This includes everything from Microsoft 365 and AWS (Amazon Web Service) implementations to smaller niche and bespoke providers. Ultimately having part or even your entire IT infrastructure fall under the control of a malicious operator.

Mobile device vulnerabilities

The widespread use of mobile devices in business operations makes them prime targets for targeting individuals in an organisation, this includes threats like malicious apps, attacks on unsecured Wi-Fi networks, and SIM swapping.

Lack of preparedness for a cyber security incident

Generally, there is a big difference demonstrated from those companies who have considered and prepared for a cyber security incident to those who haven't. Those who have prepared possess robust incident response plans, conduct regular security training for employees, and implement advanced detection systems. This preparation enables them to quickly identify breaches, effectively contain the damage, and recover with minimal operational impact. Their readiness often results in reduced financial losses and safeguards their reputation.

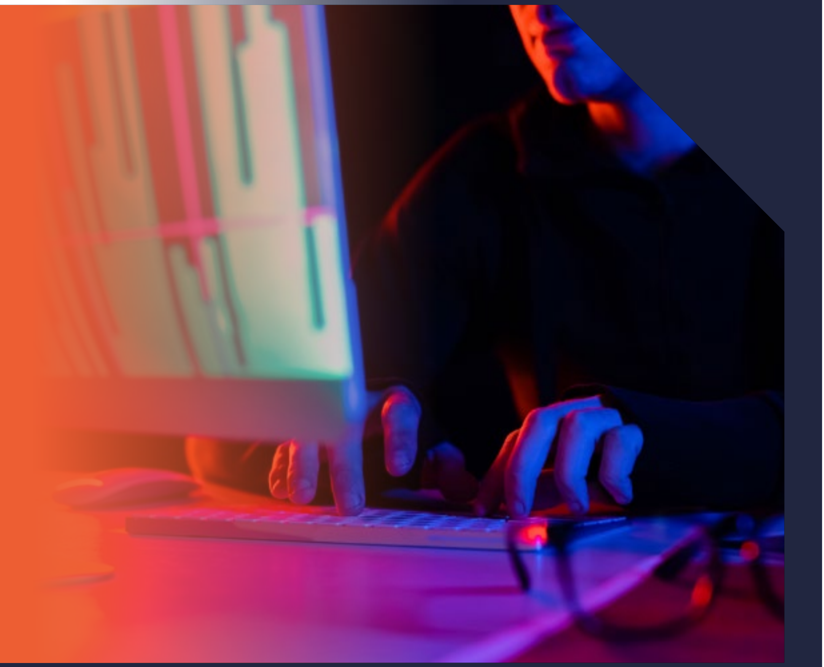
On the other hand, companies without a preparedness plan face longer recovery times, exacerbated financial and reputational damage, and a higher likelihood of severe data breaches.

Recent major cyber security incidents

Understanding the real-world implications of these threats highlights their seriousness, where even simple oversights can have catastrophic consequences. Here are a few notable incidents from 2023 [source]:

Victim (Data Identified)	What happened?	Result and impact	Result and impact
23andMe - October 2023	20,000,000 breached records Currently facing a class action lawsuit. Under the basis the ethnicity-specific groupings could amount to a "hit list". For example; Terrorist llooking to identify people of Jewish heritage. It was also stated Chinese intelligence agencies, which have a history of surveilling and intimidating dissidents abroad, could use the data to target people critical of the government or even nation states.	Credential Stuffing Attack (Involves attackers using stolen usernames and passwords from one breach to gain unauthorised access to accounts on other platforms, exploiting the common practice of password reuse.)	23andMe initially reported that 14,000 users' personal information was hacked. However, nearly 7 million users had some profile information exposed in the data breach.
KidSecurity - September 2023	Configuration oversight.	Over 300 million records exposed. Impact - This placed KidSecuriy in a very precarious situation, one where it is not beyond possibility that multiple parents would sue the organisation.	Security, which allows parents to monitor and control their children's online safety, exposed user activity logs to the Internet for more than a month via misconfigured Elasticsearch and Logstash (tools used for logs and events data analysis) instances.
SAP SE Bulgaria - (November 2023)	Human error.	95,592,696 records/ artefacts exposed.	SAP SE Bulgaria was one of the main organisations affected when Kubernetes Secrets – objects that contain small amounts of sensitive data, such as passwords, tokens or keys – relating to hundreds of organisations were exposed to the Internet in public GitHub repositories.

Recent major cyber security incidents Continued



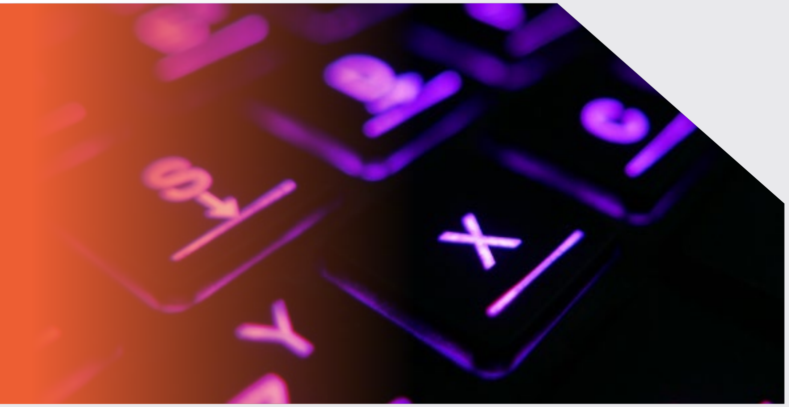
Victim (Data Identified)	What happened?	Result and impact	Result and impact
TmaxSoft (Initially June 2021, but real impact in January 2023)	Internal leak.	2 TB of data - more than 56 million records	TmaxSoft, an IT company in South Korea, exposed data to the Internet via a Kibana dashboard for over two years.
ICMR Indian Council of Medical Research (September 2023)	Likely multiple attack vectors taking advantage of vulnerabilities in the ICMR's Covid-testing database.	815,000,000 breached records With the data being sold on the dark web this places both the organisation and individuals affected at great risk.	The personal data, including names, passport details and contact information, was offered for sale on the dark web in October.
Redcliffe Labs (October 2023)	Non-password protected database left unsecured for an unknown period of time.	7TB of data breached, comprising 12,347,297 records.	The data included medical test results, doctors' names and other sensitive medical information.
MOVEit (Compromised May 2023, Detected June 2023)	SQL Injection	The scale of the breach remains unquantified, but estimates put the number of affected organisations at over 2,000 and the number of individual victims at over 60 million.	The managed file transfer software company suffered a series of cyber attacks over a number of months, affecting potentially millions of users.
UK Electoral Commission (Compromised Aug 2021, Detected Oct 2022).	Zero-Day Flaw. (ProxyNotShell – CVE-2022-41040).	The personal information of around 40 million people may have been affected. The Information Commissioner's Office (ICO) launched an investigation into the incident and the Electoral Commission faced scrutiny over its data retention policies and the delay in notifying data subjects. The breach underscored the need for effective cyber detection measures, data retention policies that stand up to scrutiny, and timely notifications to data subjects.	This was a sophisticated attack that may have exploited a zero-day flaw in the software in their Exchange server. The personal information breached was considered 'low-grade' - names and home addresses.

Recent major cyber security incidents Continued

Victim (Data Identified)	What happened?	Result and impact	Result and impact
University of Minnesota (Compromised 2021, Detected July 2023).	Unknown	Information relating to around 7 million people who attended or worked at the university between 1989-2021. The long-term impacts of the breach for the University of Minnesota include facing multiple lawsuits from individuals whose personal information was compromised.	The potential data that was accessed included Social Security numbers, names, addresses, demographic information and employment information.
Tigo Business - January 2024.	Ransomware.	Over 700,000 people's data may have been affected. Over 330 servers were encrypted. The attack on Tigo Business is attributed to the Black Hunt ransomware group, known for breaching victims via unsecured RDP connections and for stealing files for secondary extortion attempts.	Tigo is the largest mobile carrier in Paraguay, with its 'Tigo Business' division offering services like cloud hosting and cybersecurity consulting. It's likely Tigo Business was the victim of Black Hunt ransomware.

How much does a cyber incident/breach cost?

There are many statistics on how much a breach costs, the average cost as stated by IBM is around £3.42 million. Unfortunately for many organisations that figure can feel quite arbitrary. Below we attempt to break down some of the more tangible costs. These will vary from one organisation to another but should give an overview of the stacked costs involved in a serious Cyber Breach.



Immediate costs

- **Investigation costs:**
  £15,000 to £100,000 (approx. $20,000 to $100,000). Costs for hiring external cybersecurity experts to analyse the cause and scope of the breach.
- **Remediation costs:**
  £40,000 to several hundred thousand pounds (approx. $50,000+). This includes upgrading software, enhancing network security, and employee training.
- **Notification costs:**
  £8 to £16 per record (approx. $10 to $20). Involves informing affected customers about the breach, communication costs, and possibly offering credit monitoring services.

Immediate costs

- **Legal fees:**
  Easily exceeding £75,000 (approx. $100,000). For consulting legal experts on compliance issues, lawsuits, or regulatory inquiries.
- **Regulatory fines:**
  Can range from thousands to millions of pounds, depending on jurisdiction and the nature of the data compromised. Under GDPR, fines can be up to 4% of the company's annual global turnover.

Indirect costs

- **Reputational damage:**
  Significant percentage loss in annual turnover due to the loss of customer trust, leading to declines in new business and customer churn.
- **Increased insurance premiums:**
  Cybersecurity insurance premiums may significantly increase post-breach.
- **Operational disruption:**
  Leads to productivity loss and potentially lost revenue.

Long-term costs

- **Litigation:**
  Costs can run into millions of pounds if customers or shareholders sue the company.
- **Long-term security upgrades:**
  Ongoing costs for maintaining enhanced security measures.
- **Decreased market value:**
  Potential drop in the company's valuation.

Intangible impacts

- **Employee morale:**
  Internal stress and lowered morale post-breach can impact productivity.
- **Customer relationships:**
  Potential years required to rebuild damaged customer relationships.

Where does cyber security add value?

We've discussed many examples where a lack of Cyber Security resilience introduces risk and significant costs. But there are many instances where Cyber Security can add value to both the business and the products and services which those businesses provide.

Enhancing trust and reputation

Building Customer Confidence: In today's digital landscape, where data breaches are rampant, a demonstrated commitment to cybersecurity significantly boosts customer trust. Consumers, investors and other businesses are more inclined to engage with businesses that show diligence in protecting personal and financial information.

This can be demonstrated by;

Using cybersecurity as a brand differentiator: In crowded markets, cybersecurity can be a unique selling proposition (USP), especially in markets where data breaches are increasingly common, an organisation's commitment to cybersecurity can set it apart from competitors.

Cybersecurity Certifications as Trust Badges: Obtaining industry-recognised cybersecurity certifications can serve as a "trust badge" for organisations. Displaying these certifications on websites and marketing materials signals to customers and partners that an organisation meets high security standards. These can assist with high value contracts and tenders.

Supporting business growth

Investing in cybersecurity is not just a defensive measure against cyber threats; it's a strategic investment that can significantly support and drive business growth. Here are creative reasons why investing in cybersecurity can enhance business growth and encourage more engagement from customers and businesses alike:

- **Regulatory compliance as a growth lever:** For many industries, regulatory compliance around data protection is not just a legal requirement but a strategic advantage. Businesses that go beyond the minimum compliance requirements can use their superior cybersecurity posture as a marketing tool, attracting customers and partners who value data privacy and security.

Where does cyber security add value?
Continued

Attracting investment

Investors are increasingly aware of the financial and reputational risks associated with cyber threats. Companies that can demonstrate a strong cybersecurity posture are more likely to attract investment, as they are perceived as less risky. This is especially true for startups and tech companies, for whom data and intellectual property are often their most valuable assets.

Innovating securely

Investing in cybersecurity enables companies to adopt new technologies and business models safely. This secure innovation can lead to the development of new products and services that can open up untapped markets or create new revenue streams, all while maintaining the integrity and confidentiality of sensitive information.

Accelerating time to market

For companies launching apps or digital services, integrating cybersecurity from the development phase can significantly reduce delays associated with security breaches or compliance issues. By ensuring that the product is secure from the outset, companies can avoid the costly setbacks of addressing security flaws post-launch, thereby getting to market faster and gaining a competitive edge.

What threats (and defences) are on the horizon?

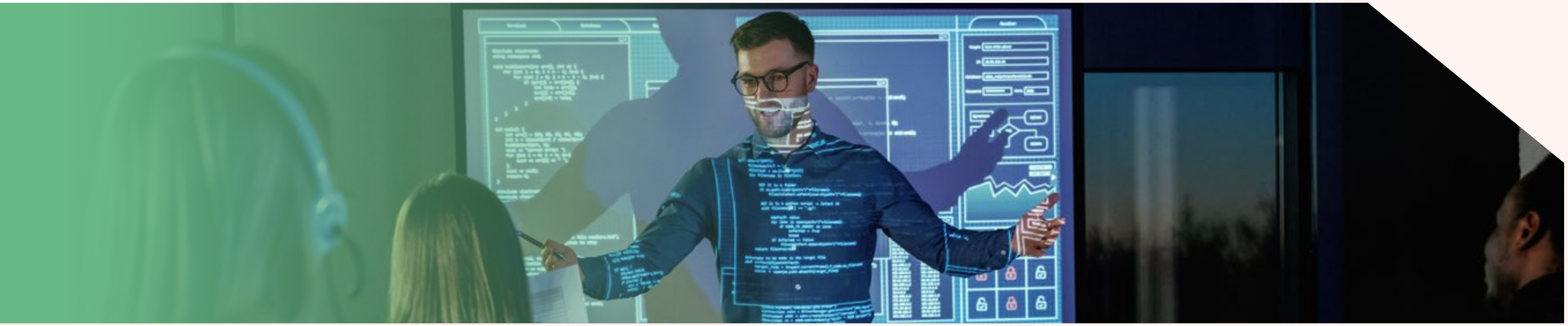
The current threat landscape is serious. Businesses need to regularly educate their employees about risks like phishing and ensure that remote staff can connect to internal networks securely. But technology is constantly evolving.

New technologies can be used by good and bad actors, increasing the complexity of the threat landscape. Here's a breakdown of some double-edged-sword technologies:

Machine learning and artificial intelligence (AI)

Machine learning and AI have transformed modern workplaces. The computing power of AI-powered systems makes them a robust tool in cyber defence, but that same power can be exploited by cyber criminals and unfortunately already is.

This ranges from malicious actors tricking ChatGPT and other language models to create malware, social engineering campaigns and other nefarious activities or to the existence of models created for nefarious purposes such as FraudGPT and WormGPT. These tools give attackers even more capability and reach.

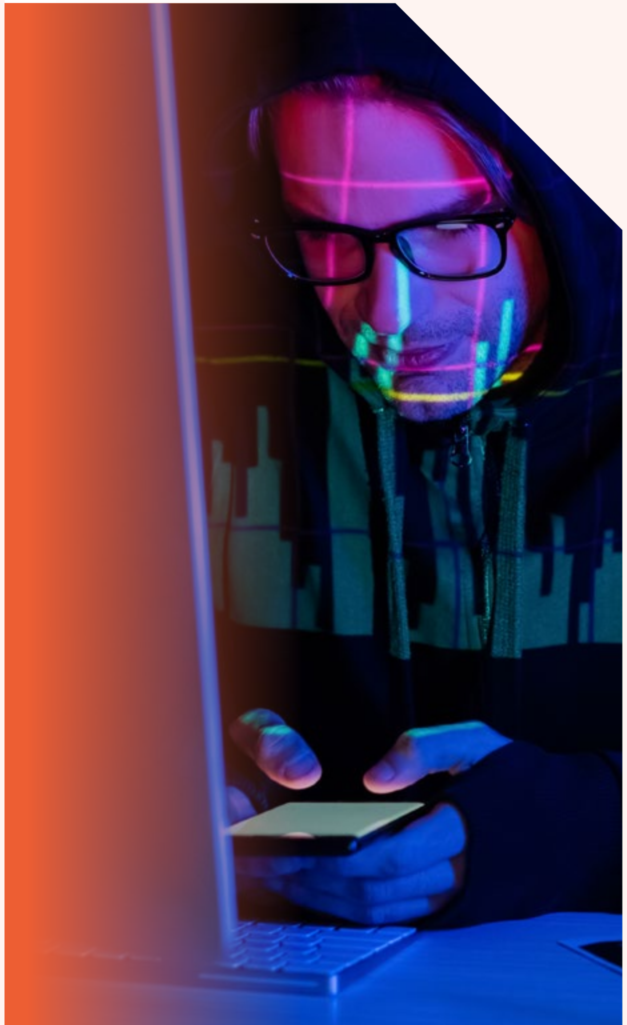


What threats (and defences) are on the horizon? Continued

The Threats

Machine learning and artificial intelligence (AI)

- **Adversarial attacks:**
As AI systems become more sophisticated, so do the methods used to deceive them. Adversarial attacks involve feeding malicious input data to trick AI algorithms into making incorrect decisions or classifications. This could lead to false positives or, allow threats to go undetected or provide bad and incorrect information which is acted upon to cause damage or harm.
- **Lack of transparency:**
The complex nature of AI algorithms can make it difficult to understand how they arrive at decisions. This lack of transparency, often referred to as the "black box" problem, can obscure potential biases or errors in the system. In a cybersecurity context, this could mean missing critical threats or incorrectly identifying benign activity as malicious.
- **Data privacy concerns:**
AI systems require vast amounts of data to learn and improve. In the process of collecting and analysing this data, there is a risk of exposing sensitive information or violating privacy regulations. Cybercriminals may also target these data troves, potentially gaining access to a wealth of valuable information.
- **Overreliance and complacency:**
As AI becomes more capable of handling cybersecurity tasks, there is a danger of over-relying on these systems and becoming complacent. This can lead to a false sense of security and a failure to keep human expertise sharp. In the event of an AI failure or a novel threat that the AI is not equipped to handle, human intervention may be necessar
- **Potential for misuse:**
Just as AI can be used to defend against cyber threats, it can also be weaponized by malicious actors. AI-powered attacks, such as intelligent malware or automated social engineering, could be more difficult to detect and counter. As AI continues to advance, the cybersecurity landscape may shift in favour of those who can harness its power for nefarious purposes.



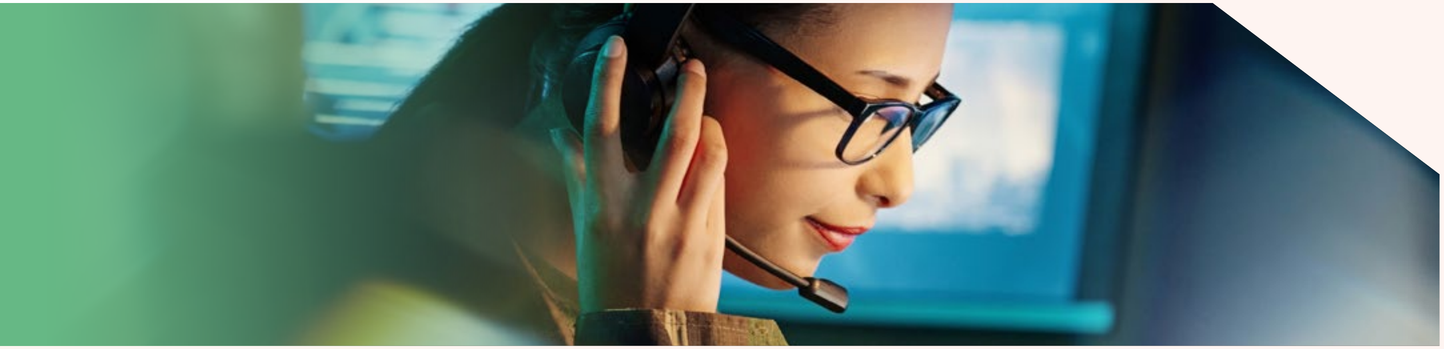
What threats (and defences) are on the horizon? Continued

Defences

- **Adaptive threat detection:** AI algorithms are increasingly capable of identifying and responding to cyber threats in real-time. Unlike traditional security software, these systems learn from each interaction, enabling them to anticipate and neutralise even the most sophisticated attacks.
- **Automated security protocols:** Machine learning can automate routine cybersecurity tasks, such as monitoring network traffic or scanning for vulnerabilities. This not only increases efficiency but also frees up valuable human resources for more complex tasks.
- **Prediction and prevention:** AI's predictive analytics are revolutionising how businesses foresee and prevent potential security incidents. By analysing vast amounts of data, AI can identify patterns that may indicate a looming threat, so countermeasures can be deployed before serious harm is done.
- **Assistance for humans:** AI could also be used to assist humans in making more informed decisions about cybersecurity. By collating complex data into actionable insights, AI systems can guide cybersecurity professionals to prioritise threats and optimise their response strategies. In addition it could assist with human decisions on social engineering threats.

Overall

Like any technology it's a double edged sword, each technological leap has brought both opportunity and risk just as the internet did and continues to do. The main difference though is the rapid speed of change, this amplifies the risks and opportunities as both legitimate organisations, criminal organisations and nations attempt to navigate these changes.



Supply chain attacks – business to business compromise

A supply chain attack targets a trusted third-party vendor who offers services or software vital to the end user or organisation. These attacks can be either software-based, where malicious code is injected into an application to infect all users of the app, or hardware-based, where physical components are compromised to achieve a similar goal.

Threats

- **Targeting vendors:** Attackers focus on software vendors and hardware manufacturers, searching for unsafe code, infrastructure practices, and network procedures that allow the injection of malicious components.
- **Exploiting trust:** These attacks exploit the trust relationship between a manufacturer or supplier and their customers. By breaching one supplier, attackers can potentially gain access to thousands of unsuspecting victims.
- **Widespread impact:** Due to the interconnected nature of supply chains, a single compromised component can affect numerous organisations across different sectors.

Business Email Compromise (BEC)

BEC is a form of phishing attack where a criminal attempts to trick a senior executive or budget holder into transferring funds or revealing sensitive information. Unlike standard phishing, BEC attacks are highly targeted and crafted to appeal to specific individuals within an organisation.

- **BEC as an entry into a supply chain:** BEC attacks can also serve as a precursor or entry point to supply chain attacks. By compromising the email accounts of senior executives or key personnel within a vendor organisation, attackers can manipulate communication to insert malicious links or attachments into regular supply chain correspondence.
- **Exploiting trust:** These attacks exploit the trust relationship between a manufacturer or supplier and their customers. By breaching one supplier, attackers can potentially gain acc

Supply chain attacks – business to business compromise Continued

Defences

Organisations can mitigate the risk of supply chain attacks and BEC by implementing robust security measures, including:

- **Vendor risk management:** Assessing and monitoring the security practices of all suppliers and vendors.
- **Employee education:** Training employees to recognize and respond to phishing attempts and suspicious emails.
- **Multi-factor authentication (MFA):** Using MFA for all business email accounts to add an extra layer of security.
- **Regular security audits:** Conducting regular security audits and vulnerability assessments to identify and address potential weaknesses.

What to look out for

Other examples of supply chain attacks that are similar in nature to BEC, where the attack vector is through trusted business relationships or communication channels, include:

- **Invoice manipulation:** Attackers can intercept and alter invoices from a legitimate supplier to redirect payments to their own accounts. This often involves changing bank account details on the invoice before it reaches the customer.
- **Software update compromise:** A notorious example is the SolarWinds Orion attack, where malicious code was inserted into a legitimate software update, which was then distributed to customers as part of regular update processes.
- **Third-party service providers:** Attackers may target managed service providers (MSPs) that have access to their clients' IT systems. By compromising the MSP, attackers can potentially gain access to the networks of all their clients.
- **Vendor email spoofing:** Similar to BEC, attackers may spoof emails from a trusted vendor to initiate fraudulent transactions or to deliver malware to an unsuspecting client.
- **Compromised hardware:** Attackers can implant backdoors or vulnerabilities in hardware components which are then shipped to customers. This can occur at any point in the manufacturing or distribution process.
- **Cloud storage hacks:** If a business uses a third-party cloud storage provider, attackers might breach the provider's systems to gain access to sensitive data belonging to multiple businesses.
- **Open source code tampering:** Attackers can contribute malicious code to open-source projects, which, when integrated into commercial products, can lead to widespread compromise.
- **Legal and professional services:** Law firms and accounting services, which handle sensitive information for businesses, can be compromised to gain insider information or to facilitate BEC schemes.

Supply chain attacks – business to business compromise Continued

Cloud computing

In 2024, the landscape of cloud computing continues to evolve, bringing forth a myriad of benefits such as scalability, flexibility, and cost-efficiency. However, this evolution also introduces several significant threats and challenges that organisations must navigate. Especially as more organisations are moving entirely to cloud based operations due to many of the operational benefits cloud environments provide. Whilst Cloud computing has now been around for over a decade the continued growth with offerings such as Microsoft 365, Salesforce, AWS and a multiple other large and small providers the threats continue to evolve and develop

These threats stem from various factors, including the inherent trust placed in cloud providers, potential misconfigurations, complacency, and the complexities associated with many Software as a Service (SaaS) platforms offered by cloud providers. Below, we delve into these concerns, highlighting the critical areas that organisations need to address to ensure a secure cloud computing environment.

Supply chain attacks – business to business compromise Continued

Threats

Trust in cloud providers

The reliance on cloud providers for securing and managing data and applications places a significant amount of trust in these entities. This trust, however, introduces risks related to data breaches, loss of data control, and potential misuse of data by the cloud provider. To mitigate these risks, organisations must conduct thorough due diligence, ensuring that their cloud provider adheres to stringent security standards and compliances. Additionally, implementing a shared responsibility model for cloud security can help delineate the security obligations of both the provider and the customer.

Misconfigurations

Misconfigurations in cloud environments are one of the leading causes of security incidents and data breaches. These misconfigurations can occur due to the complexity of cloud settings, lack of visibility, and human error. To combat this, organisations need to understand how to properly configure these environments, as many require configuration and work to fin Microsoft 365 is a great example where many companies tend to score below 50% for their secure scores due to a lack of understanding and knowledge of what settings and configurations need to be modified and managed.

Complacency and human error

The ease of use and management of cloud services can lead to complacency and human errors, such as inadequate access controls, weak password policies, and failure to regularly update or patch cloud-based applications. A leading cause of this is a lack of understanding and communication from cloud providers on what security standards and practices users are required to adhere to. To bridge these gaps, it's essential for organisations to implement comprehensive training programmes that educate all users on security best practices and the specific requirements of their cloud services.

SaaS challenges

The adoption of SaaS (Software as a service) platforms introduces unique challenges, including data privacy concerns, lack of control over the security posture of the SaaS application, and potential data leakage between tenants in a multi-tenant architecture. To address these issues, organisations should carefully evaluate SaaS providers. This entails verifying their security and compliance certifications, understanding their data management policies, implementing strong access controls, and ensuring tenant data is effectively isolated. Additionally, establishing clear incident response protocols and considering the use of third-party assessments and Cloud Access Security Brokers (CASBs) can further safeguard data and maintain privacy.

Cloud-native threats

As organisations increasingly adopt cloud-native technologies, they face threats such as container vulnerabilities, serverless function misconfigurations, and insecure APIs. Embracing a DevSecOps approach, where security is integrated into the development and deployment processes, can help mitigate these threats. Additionally, employing cloud-native security tools designed to protect containerized applications and serverless functions is crucial.

Supply chain attacks – business to business compromise Continued

Defences

Establishing strong governance and compliance

- **Implement a shared responsibility model:** Clearly define and understand the security responsibilities that lie with the cloud provider versus those that are the organisation's obligation. This clarity ensures comprehensive coverage of security controls.
- **Conduct regular security assessments and audits:** Perform continuous security assessments and compliance audits of cloud environments to ensure adherence to industry standards and regulations.

Enforce strong access controls and identity management

Apply multi-factor authentication, least privilege access policies, and regular access reviews to minimise the risk of unauthorised access.

Bolstering data protection and privacy

- **Encrypt data in-transit and at-rest:** Use strong encryption standards to protect sensitive data stored in the cloud and during transmission over networks.
- **Implement data loss prevention (DLP) strategies:** Use DLP tools to monitor and control data movement, preventing unauthorised data leaks or exposure.

Cultivating a culture of security awareness

- **Provide ongoing security training:** Educate employees about cloud security risks and best practices, focusing on the prevention of phishing attacks, safe handling of data, and secure use of cloud services.
- **Promote a culture of security vigilance:** Encourage employees to be proactive in reporting suspicious activities and to stay informed about the latest cybersecurity threats.

Integrating DevSecOps practices

- **Incorporate security early in the development lifecycle:** Embed security practices and tools from the initial stages of application development, promoting a security-by-design approach.
- **Automate security testing and compliance checks:** Integrate automated security testing and compliance verification into the continuous integration/continuous deployment (CI/CD) pipeline.

Leveraging Advanced security technologies

- **Deploy threat detection and response solutions:** Utilise advanced threat detection technologies, such as Security Information and Event Management (SIEM) systems and Endpoint Detection and Response (EDR) solutions, to identify and respond to threats swiftly.
- **Use Cloud Access Security Brokers (CASBs):** Implement CASBs to gain visibility into cloud application usage, enforce security policies, and protect against threats across cloud environments.

Edge computing (smart devices)

Edge computing is a distributed computing paradigm that brings computation and data storage closer to the ***sources*** of data, (such as IoT devices / sensors), instead of relying on a central location thousands of miles away. By processing data closer to where it's generated, edge computing can improve response times and save bandwidth.

For our cyber-security needs, edge computing can reduce the risk of data exposure by minimising the amount of sensitive data that needs to be transmitted over networks. It can also enable faster response to security threats, as data can be analysed and acted upon locally rather than having to be sent to a central server for processing.

Threats

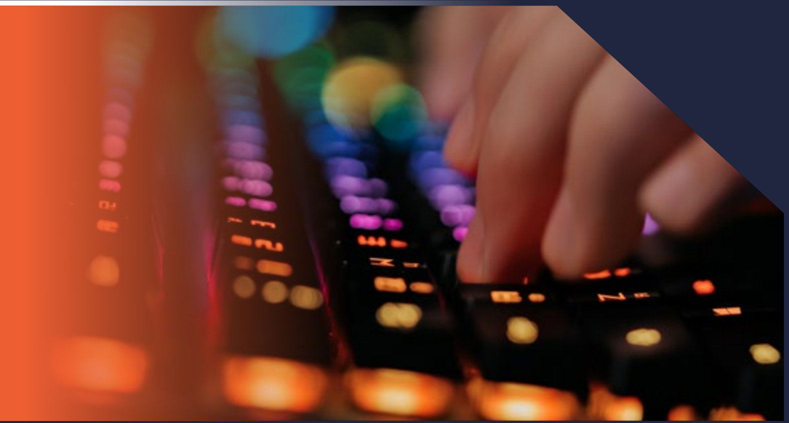
- **Expanded attack surface:** Edge computing involves a distributed network of edge devices, each of which represents a potential entry point for attackers. As the number of edge devices grows, so does the attack surface. Each device needs to be secured, patched, and monitored, which can be challenging in a distributed environment.
- **Physical security risks:** Unlike centralised data centers, which are typically well-protected, edge devices are often in public spaces or remote locations. This makes them more vulnerable to physical tampering or theft. If an attacker gains physical access to an edge device, they could potentially access sensitive data or use the device as an entry point to the broader network.
- **Device constraints:** Edge devices, such as IoT sensors or smartphones, often have limited computational power, memory, and energy resources. This can make it difficult to implement robust security measures, such as advanced encryption or real-time threat monitoring, on these devices.
- **Software and firmware vulnerabilities:** Edge devices often rely on embedded software or firmware, which can contain vulnerabilities. As edge computing becomes more prevalent, attackers are likely to focus more on exploiting these vulnerabilities. Keeping all edge devices updated with the latest security patches can be a significant challenge.
- **Data privacy concerns:** Edge computing often involves processing sensitive data, such as personal information or health data, at the edge of the network. Ensuring this data is processed in compliance with privacy regulations and is protected from unauthorised access can be challenging in a distributed edge environment.

Defences

- **Localised data processing:** By processing data closer to where it's generated (at the "edge" of the network), edge computing reduces the risk associated with data transit and centralised storage.
- **Improved response times:** Edge computing enables faster response to security breaches, as data does not have to travel to a centralised data centre for processing.

What to do next?

Hopefully this section has given you some interesting insights into the complex and ever-changing world of cyber security. As much as new technology improves our ability to defend ourselves from would-be attackers, it doesn't happen automatically. You (and your organisation) need to be empowered to understand the risks and how to stay on top of them.



The key is a proactive, rather than reactive, approach. Here's how businesses can prepare for future threats:

1. Stay informed about emerging threats

- **Regular briefings:** Subscribe to cybersecurity newsletters and bulletins from trusted sources to stay updated on new threats and vulnerabilities.
- **Attend industry conferences and webinars:** These events are invaluable for gaining insights into future trends and networking with cybersecurity experts.

2. Invest in continuous learning

- **Staff training:** Regular training sessions for your team ensure they are aware of the latest threats and know how to respond.
- **Learning from incidents:** Analyse cybersecurity incidents within and outside your industry to learn from others' experiences.

3. Adopt a forward-thinking mindset

- **Scenario planning:** Conduct regular risk assessments and develop scenarios for potential cyber threats. This helps in creating a robust response strategy.
- **Innovative solutions:** Keep an eye on technological advancements, like AI and machine learning, and consider how they can bolster your cybersecurity measures.

4. Foster strong industry partnerships

- **Collaborate and share information:** Engaging with industry peers and participating in information-sharing forums can provide early warnings about emerging threats.

5. Regularly update and test your cybersecurity plan

- **Periodic reviews:** Cybersecurity strategies should be reviewed and updated regularly to adapt to the changing threat landscape.
- **Testing and drills:** Regularly test your systems and conduct drills to ensure your team is prepared for a real incident.

Developing a future-proof cybersecurity plan

Creating a robust cybersecurity plan is crucial for protecting your business from threats in the digital world. A good plan not only safeguards your data and systems but also enhances your credibility with customers and partners. Here's a step-by-step guide to help you develop a comprehensive cybersecurity plan.

The key is a proactive, rather than reactive, approach. Here's how businesses can prepare for future threats:

1. Assess your current cybersecurity status

- **Conduct a risk assessment:** Start by identifying your valuable assets, such as customer data, intellectual property, and financial information. Assess the vulnerabilities and potential threats to these assets.
- **Audit existing security measures:** Review your current security protocols and technologies. Determine if they are adequate and identify areas for improvement.

2. Define your cybersecurity goals

- **Set clear objectives:** Your goals might include protecting customer data, ensuring operational continuity, or complying with industry regulations. Make these goals specific, measurable, and achievable.

3. Develop policies and procedures

- **Create comprehensive policies:** Develop policies for data protection, acceptable use, remote work, incident response, and more. Ensure these policies are clear and accessible to all employees.
- **Establish response protocols:** Develop an incident response plan that details the steps to take in the event of a security breach, including communication strategies and recovery processes.

4. Implement security measures

- **Invest in technology:** Provide ongoing cybersecurity training for your staff. This should include awareness of current cyber threats and best practices for avoiding them.
- **Focus on human factors:** Implement robust password policies, regular software updates, and two-factor authentication. Educate employees about phishing, social engineering, and other common threats.

Developing a future-proof cybersecurity plan Continued

5. Regular training and awareness

- **Conduct regular training:** Provide ongoing cybersecurity training for your staff. This should include awareness of current cyber threats and best practices for avoiding them.
- **Promote a security-conscious culture:** Encourage employees to be vigilant and proactive in reporting potential security threats.

6. Monitor, review, and update your plan

- **Continuous monitoring:** Regularly monitor your systems and networks for unusual activity. Use this data to refine your approach to cybersecurity.
- **Regular reviews:** Cyber threats are constantly evolving. Schedule periodic reviews of your cybersecurity plan to ensure it remains effective against new threats.
- **Update and adapt:** Be prepared to update your security measures and policies as needed. This may involve investing in new technology or revising employee training.

7. Create a business continuity plan

- **Plan for the worst:** In the event of a major cyberattack, have a business continuity plan that outlines how your operations will continue. This includes data backups and alternative communication channels.

8. Engage with cybersecurity professionals

- **Seek expert advice:** Consider consulting with cybersecurity professionals to review your plan and provide insights. They can offer expertise in areas you may not have considered.

You don't have to face cyber security alone...

At Cyber Alchemy, we believe that privacy, security and trust are a fundamental right. Every individual and organisation should be able to operate online without fear.

Jamie Kelly
CEO
EVie:
"Working with Cyber Alchemy was a fantastic experience. Their responsiveness and depth of expertise significantly aided our application's launch."

Yannick Van Der Bergen
Owner
iWebDevelopment:
"Cyber Alchemy's comprehensive testing of our main application was invaluable. Their advice greatly enhanced our security. Highly recommended."

Sam W,
DLSHealth:
"Cyber Alchemy stands out with their direct approach and hacker mindset. They're more than a provider; they're integral to our platform's integrity and overall security posture."

CREST

Crown Commercial Service *Supplier*

CYBER ESSENTIALS

CYBER RUNWAY

Your bespoke route to cyber security empowerment

1. **ASSESS**
   A full, process-led vulnerability assessment. We will uncover any risks in your infrastructure.
2. **PROTECT**
   Find peace of mind and alleviate anxiety with our dependable cyber protection.
3. **ENABLE**
   We'll help you build an empowered, knowledgeable organisation, ready to prevent attacks.

If you're ready to embrace cyber security for your organisation, we're ready to help.

[Contact Us Now] Details please

CYBER ALCHEMY

ASSESS - PROTECT - ENABLE

Cyber Alchemy
Unit G1
Advanced Manufacturing Park
Brunel Way,
Catcliffe
Rotherham S60 5W

Email: sales@cyberalchemy.co.uk
Call: 0114 4000377

cyberalchemy.co.uk