methods
AN ALTEN COMPANY

# Top 5 Cyber Security Trends

In the ever-evolving landscape of cyber security, leveraging threat intelligence enables organisations to proactively address prevailing cyber threats. This document, crafted by our experts, illuminates the 'Top 5' cyber trends and threats we're observing, alongside our strategies at Methods to safeguard organisations from them.

May
2024

methods
AN ALTEN COMPANY

# Contents



methods
AN ALTEN COMPANY

Methods is a National Cyber Security Centre (NCSC) certified Cyber Security Consultancy. We craft advice and guidance tailored to the unique needs of our diverse clientele. Our approach is anchored in the principles of cost-effectiveness and pragmatic wisdom, guided by the gold standards of industry best practice.

Clients benefit from our team of experts, recognised by both the NCSC and the UK Cyber Security Council for their track record in delivering cyber security consultancy services.

Our Threat Intelligence team navigate the complex landscape of cyber threats with precision and foresight, serving our key clients including front-line MDR, offensive security, and cyber technical assurance. Our selection of the 'Top-5' threats is informed by extensive experience across various clients and comprehensive data analysis, focusing on the most prevalent threats in both the external landscape and our clients' environments.

With a collective experience exceeding 30 years in the cyber and intelligence sectors, our Threat Intelligence team ensures rigorous criteria are applied in identifying and prioritising the 'Top-5' areas of concern.

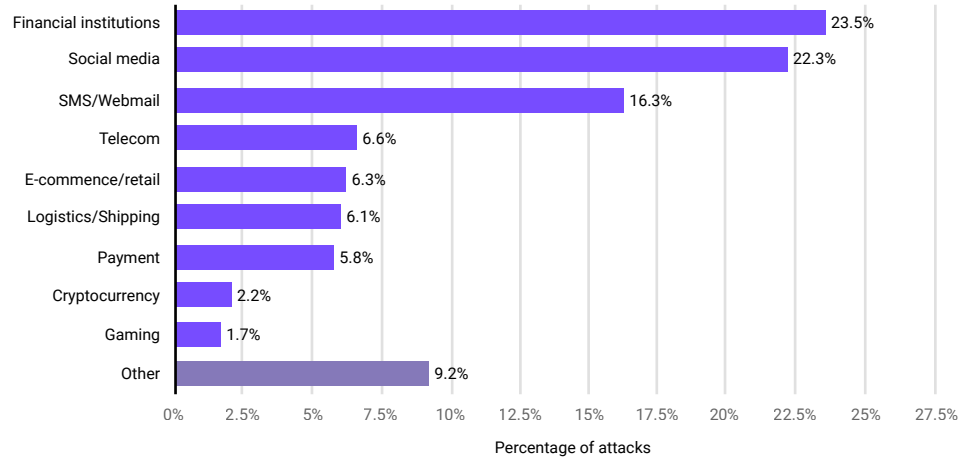
# 1. Phishing



Phishing occurs when attackers send scam emails (or text messages) that seem legitimate with the aim of gaining user credentials, or to get victims to access malicious websites.

The UK Government states that phishing attacks are commonly reported as the most disruptive types of attack that organisations face (by 61% of the businesses and 56% of the charities that identify any breaches or attacks).

## Phishing Industry Statistics (Statista)



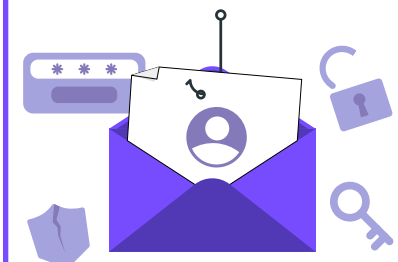

## Types of Phishing

### Spear Phishing

A targeted form of phishing where attackers conduct extensive research to craft personalised messages tailored to specific individuals or organisations. We see this more and more commonly with clients and employees targeted by these attacks.

### Smishing

Smishing uses fake mobile text messages to trick people into downloading malware, sharing sensitive information, or sending money to cyber criminals.



### Whaling

Targets high-profile individuals, such as senior executives, using fraudulent emails that masquerade as trusted colleagues or executives to manipulate lower-level employees into transferring funds or divulging sensitive information.

### QRishing

QR code phishing is a deceptive practice where cyber criminals create fraudulent QR codes that, when scanned, redirect users to malicious websites or prompt them to disclose sensitive information. These malicious QR codes can be disguised as legitimate ones, leading unsuspecting individuals to believe they are accessing genuine content or services.

### Vishing

Vishing perpetrators frequently employ VOIP to contact their victims, employing a combination of threats and psychological tactics over the phone to instill a sense of urgency or fear. They may assert that providing personal information is the sole means to resolve a supposed issue or avoid consequences.

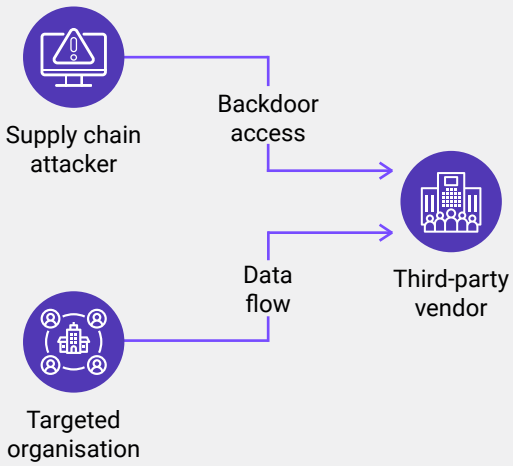
# 2. Supply Chain Attacks



A supply chain attack involves a cyber assault directed at a dependable third-party vendor providing crucial services or software within the supply chain.

In software supply chain attacks, malevolent code is inserted into an application to spread infection to all users of the app. Conversely, hardware supply chain attacks compromise physical components with the aim of achieving a similar outcome.

Often organisations fall victim to supply chain attacks due to suppliers' failure to consider supplier risks. This echoes the Government Cyber Breaches Survey 2024 where they state only 11% take into account their supplier risks.




## Common Supply Chain attacks

**Watering hole**
A watering hole attack targets a website that is used by employees or contractors of the targeted organisation. The website can be compromised to distribute malware to the users and then back to the target organisation after weaknesses have been identified in their cyber security.

**Cryptojacking**
These attacks allow attackers to use the computational resources of the targeted machines. It is done by distributing malware via email, website, or vulnerabilities, making the machines mine crypto-currency for the attackers.

**Open-source attacks**
Open-source software is a great way for businesses to develop products. However, the surge in cyber attacks exploiting vulnerabilities within such software poses a growing concern. To mitigate these risks, Microsoft offers a comprehensive repository of real-time open-source threats, enabling users to proactively safeguard their systems from potential breaches.

**Commercial software products**
Some software companies supply multiple organisations with the same solutions. If these are infiltrated by malicious actors, it can cause huge disruption in supply chains.

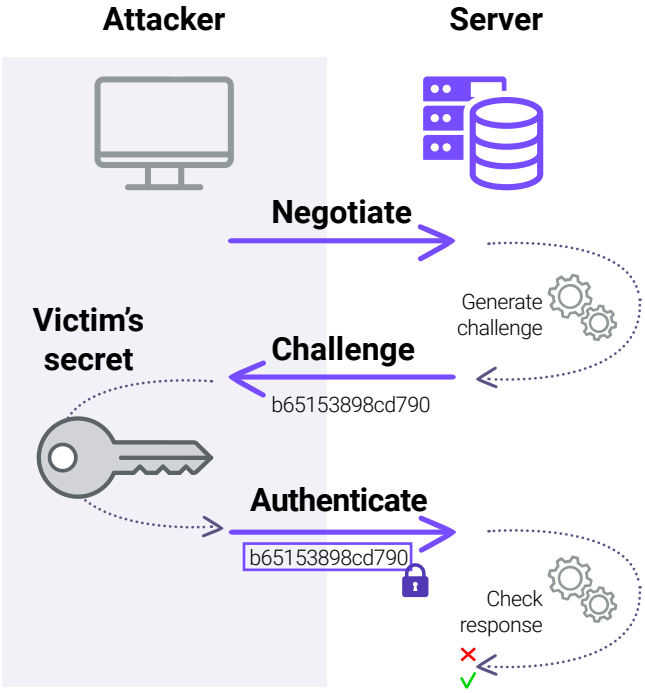
**Foreign-sourced threats**
In some countries where governments can exercise deep control over the production of private companies, some software may be infiltrated, and when overseas partners purchase the software, the malicious actors can execute the malware or code. These can be done by state actors or criminal organisations.

# 3. NTLM Relay



NTLM relay attacks allow attackers to steal hashed versions of user passwords and relay them to client creds to authenticate to a server. They use a 'Machine-in-the-Middle' method which intercepts and relays validated authentication requests gaining access to network resources.

Methods expert penetration testers state that there has been a significant increase of NTLM relay attacks due to the authentication protocol. Our team states that, "*NTLM Relays are a classic attack against Windows systems. Although proposed many years ago, it is still a hot topic among red teams, especially in Active Directory environments*".




## Leaking NTLM credentials through Windows themes

An Akamai researcher recently discovered a spoofing vulnerability in Microsoft Themes. It was assigned CVE-2024-21320 with a CVSS score of 6.5. The flaw has the potential to cause an authentication coercion attack, in which the victim is forced to transfer credentials to the attacker's computer over SMB (often in the form of NTLM hashes). The credentials can be cracked offline by the attacker later.

## Russian APT28 in the hunt with NTLM Relaying

High-profile organisations around the world have been targeted with NTLM v2 hash relay attacks by Russian state-backed threat operation APT28. APT28 exploited Microsoft Outlook privilege escalation vulnerability and WinRAR code execution flaw to launch NTLM relay attacks on organisations' mailboxes, according to Trend Micro researchers. The group also used various anonymisation layers, including data centre IP addresses, breached EdgeOS routers, and VPN servers.

## Windows Exchange Server

Microsoft updated their security advisory that a critical vulnerability in the Exchange Server was being exploited as a zero-day before being fixed. This vulnerability was identified as CVE-2024-21410, which allows the attacker from a remote unauthenticated standpoint to escalate privileges using an attack vector called NTLM relay.

| Threats | Real examples | Mitigation via OSS SSC Framework | Framework requirement reference |
|---|---|---|---|
| Accidental vulnerabilities in OSS code or Containers that we inherit | SaltStack | Automated patching, display OSS vulnerabilities as pull requests | UPD-2, UPD-3 |
| Intentional vulnerabilities/backdoors added to an OSS code base | phpMyAdmin | Perform proactive security review of OSS | SCA-5 |
| A malicious actor compromises a known good | ESLint incident | Ability to block ingestion via malware | ING-3, ENF-2, |

# 4. Artificial Intelligence and Large Language Models

In today's rapidly evolving technological landscape, the integration of Artificial Intelligence (AI) and Large Language Models (LLMs) has become ubiquitous. Data Scientists within Methods have seen a huge uptake in AI across organisations. While AI's applications span various domains, its impact on cyber security is particularly noteworthy.

## How adversaries can utilise AI and LLMs and the impact

Adversaries can leverage AI and LLMs to craft sophisticated cyber attacks, amplifying their capabilities, and potentially causing significant disruptions across various sectors. Microsoft compiled a list of LMM-themed TTPs that have been mapped to the MITRE ATT&CK framework. LLMs can be used to:

- Discover vulnerabilities
- Manipulate targets via social engineering
- Evade detection systems
- Even bypass security features like two-factor authentication

(Microsoft Threat Intelligence, 2024)

The NCSC spoke about the 'near-term impact of AI on the cyber threat':

"*Increases in the volume and heightened complexity and impact of cyber operations will indicate that threat actors have been able to effectively harness AI. This will highly likely intensify UK cyber resilience challenges in the near term for the UK government and the private sector.*" (NCSC, 2024)

AI and LLMs can enable all types of threat actors, lowering the skill barrier for individuals such as script kiddies to execute advanced attacks. Our threat researchers uncovered the simplicity with which ChatGPT can be employed to craft keyloggers, trojans, and worms.

## How AI and LLMs can empower organisations against cyber attacks

While AI and LLMs can potentially aid malicious actors in orchestrating sophisticated cyber attacks, their strategic implementation by organisations can significantly bolster defence mechanisms.

AI and LLMs can provide:

- Advanced threat detection capabilities
- Improved incident response efficiency
- Personalised security measures
- AI security Copilot (Microsoft Security Copilot)

Organisations utilising AI and LLMs can enhance their security posture, improve operational efficiency, and adeptly manage cyber risks, thereby safeguarding their digital assets and maintaining business resilience in an increasingly complex threat landscape.

**Copilot statistics from Microsoft:**

Analysts were up to 26% faster across all tasks

Novice analysts were 44% more accurate on tasks

More than 93% of users wanted to use Copilot again

# 5. Ransomware



### The definition of Ransomware from the NCSC states:

*"Ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption. The computer itself may become locked, or the data on it might be encrypted, stolen, or deleted. The attackers may also threaten to leak the data they steal."*

Methods' Cyber Analysts have observed an upward trend in the frequency of ransomware of late. Maintaining Security Operations Centres has shown the many varied ways in which the access portion of the ransomware could be enabled. The most common attack vector we have seen is through the medium of email, often spoofed to appear from a legitimate sender or regarding a common application like MFA .

### Threat trends from 2023:

84% increase in ransomware attacks

Total ransomware payments exceeded $1 billion

### Ransomware deployment process:

**Access**

Control is established and malicious encryption software is planted

**Activation**

Malware is activated, devices are locked, and the data upon them is encrypted

**Ransom Demand**

Usually an on-screen notification from the threat actor will appear, explaining what has happened, how to make the payment, and then instructions on how to regain access to your data

It is key to remember that 'ransomware' is an umbrella term for many different types of malware. There are variants that are designed to encrypt, these are historically the most common and certainly the most well-known. However, as commonality breeds innovative defence strategies, threat actors have to diversify and new variants emerge such as Scareware, Lockers, and Ransomware as a Service (RaaS).

At Methods, staying abreast of emerging threat actors, TTPs, and vulnerabilities is integral to maintaining cutting-edge defensive capabilities. Instances like the WannaCry malware attack on the NHS or the recent FBI and NCA takedown of LockBit underscore the significance of this proactive approach. In the most up-to-date reporting, however, Microsoft reports that DEV-0193, also called Trickbot LLC, is currently the most prolific ransomware organisation.

### The cost of ransomware

The trends gathered for the year ending 2023 make for some startling reading. It is estimated that there was a global increase of 84% in ransomware attacks and that for the first time since records began, the total ransomware payouts exceeded $1 billion!

It is estimated that global ransomware trends for damage will experience 30% year-over-year growth for the next decade. Financial damages from ransomware attacks are estimated to exceed a staggering $265 billion annually by 2031. Whilst these stats appear negative, there are a multitude of defensive options to combat these threats, see below to find out how Methods' can help secure your estate.

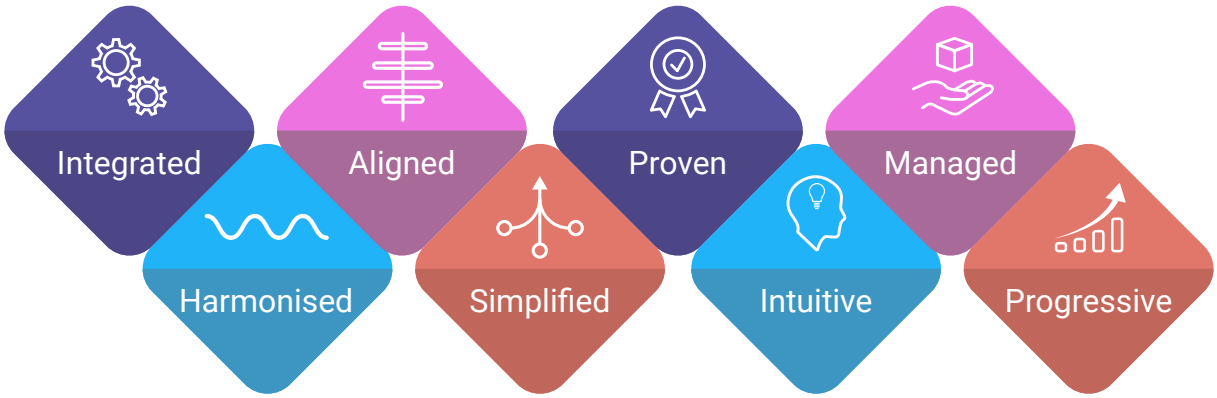
# How to protect yourself



**Methods are experts in delivering secure, resilient, cyber security services that keep your systems and data safe**

## Approach

We give expert independent and tailored advice, working towards cyber security that is:




## We understand your needs

### Maintain compliance

How do I maintain compliance in an ever-changing regulatory environment

### Security expertise

My organisation lacks in-house strategic security expertise

### Risk and compliance costs

We need to reduce risk and compliance costs

### Protect

How do I protect business-critical data

### Threats

We need to anticipate and identify threats, and have appropriate countermeasures in place

### Pragmatic approach

Pragmatic, business-focused approach to security

### Training and Awareness

Training and awareness play pivotal roles in the realm of cyber security, serving as crucial components in fortifying digital defences against evolving threats. Effective training equips individuals with the knowledge and skills necessary to identify, mitigate, and respond to cyber risks proactively. Whether it's recognising phishing attempts, practicing secure password management, or understanding the latest malware trends, a well-informed workforce can significantly reduce the likelihood of successful cyber attacks.

Furthermore, heightened awareness fosters a culture of vigilance, where every individual within an organisation becomes a frontline defender against cyber threats. By investing in comprehensive training programmes and promoting continuous awareness initiatives, businesses and institutions not only enhance their cyber security posture, but also cultivate a resilient and security-conscious environment capable of adapting to emerging challenges in the ever-changing digital landscape.

## Supply Chain Resilience

Securing organisations against supply chain attacks necessitates a multifaceted approach that encompasses proactive measures, robust partnerships, and continuous vigilance. Firstly, organisations should conduct thorough risk assessments to identify potential vulnerabilities within their supply chain network. Implementing stringent vendor due diligence processes, including rigorous background checks and security evaluations, is essential for vetting suppliers and mitigating risks. Tools such as Risk Ledger allow organisations to create resilient supply chains by identifying, measuring, and mitigating security risks.

Methods provide end-to-end services aimed at fortifying and securing complex, multi-layered supply chain networks. Please get in touch to discover how we can assist your organisation in identifying and mitigating threats to your supply chain.

You can find out more about supply chain resilience **here**.

## Patch Management

Software vendors regularly release updates to address bugs and vulnerabilities, ensuring the security of their products. Patch management is crucial for protecting endpoints against cyber threats while also enhancing system efficiency. It fosters organisational productivity by ensuring smooth software operation with timely patches.

Furthermore, effective patch management reduces device lifecycle management costs through remote management, thereby diminishing reliance on costly hardware shipments or on-site repairs. Moreover, it assists in meeting legal, regulatory, and compliance obligations, such as HIPAA and GDPR, by upholding data protection and privacy standards in accordance with relevant laws and regulations.

To find out how Methods can help your organisation achieve a robust cyber security programme, please visit **here** or get in touch with us at **cyber@methods.co.uk**.

# References



Cardillo, A. (2024, March 3). How Many Companies Use AI? Retrieved from Exploding Topics: https://explodingtopics.com/blog/companies-using-ai

Microsoft Threat Intelligence. (2024, February 14). Staying ahead of threat actors in the age of AI. Retrieved from Microsoft: https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/

NCSC. (2024, January 24). The near-term impact of AI on the cyber threat. Retrieved from https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat#:~:text=It%20is%20therefore%20likely%20that,making%20existing%20techniques%20more%20efficient

https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf

https://www.cynet.com/blog/rhysida-the-ransomware-gang-strikes-again/

https://www.cisa.gov/sites/default/files/2023-11/aa23-319a-stopransomware-rhysida-ransomware_1.pdf

https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/