NBS Nottingham Business School

Cybersecurity in the Modern World

Dr. Olga Khon

olga.khon@ntu.ac.uk

Learning Outcomes

- Cybersecurity and Cyberattacks
- Cybersecurity Threats (Cyberthreats)
- Cybersecurity Myths
- Cybersecurity: Best Practicies and Technologies
- Cyberthreats vs IT Outages: Regional and Global Incidents
- Cybersecurity Trends in 2025
- **Case Study 1**. The Near-Term impact of AI on the Cyberthreat in the UK
- **Research Activity 3. [** Brainstorming: Cyberthreats in the Modern World on the Regional and International Levels]

Cybersecurity

Cybersecrity refers to any technologies, practices and policies for preventing cyberattacks or mitigating their impact *.

Cybersecurity aims to protect computer systems, applications, devices, data, financial assets and people against ransomware and other malware, phishing scams, data theft and other cyberthreats *.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity;
** Image source: Cisco, 2025, https://www.cisco.com/site/uk/en/learn/topics/security/what-is-cybersecurity.html

Cyberattack

A **cyberattack** is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device.

Threat actors start cyberattacks for **all sorts of reasons**: from petty theft to acts of war. They use **various tactics**, like malware attacks, social engineering scams, and password theft, to gain unauthorized access to their target systems.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity

Cybersecurity: Cost of a Data Breach *

2024:

The average cost of a data breach

jumped to

USD 4.88 million from

USD 4.45 million in 2023 -

a **10% spike** and the highest increase since the pandemic *

2024:

Business losses (revenue loss due to system downtime, lost customers and reputational damage) **and post-breach response costs (**costs to set up call centers and credit monitoring services for affected customers or to pay regulatory fines), **rose nearly 11%** over the previous year *

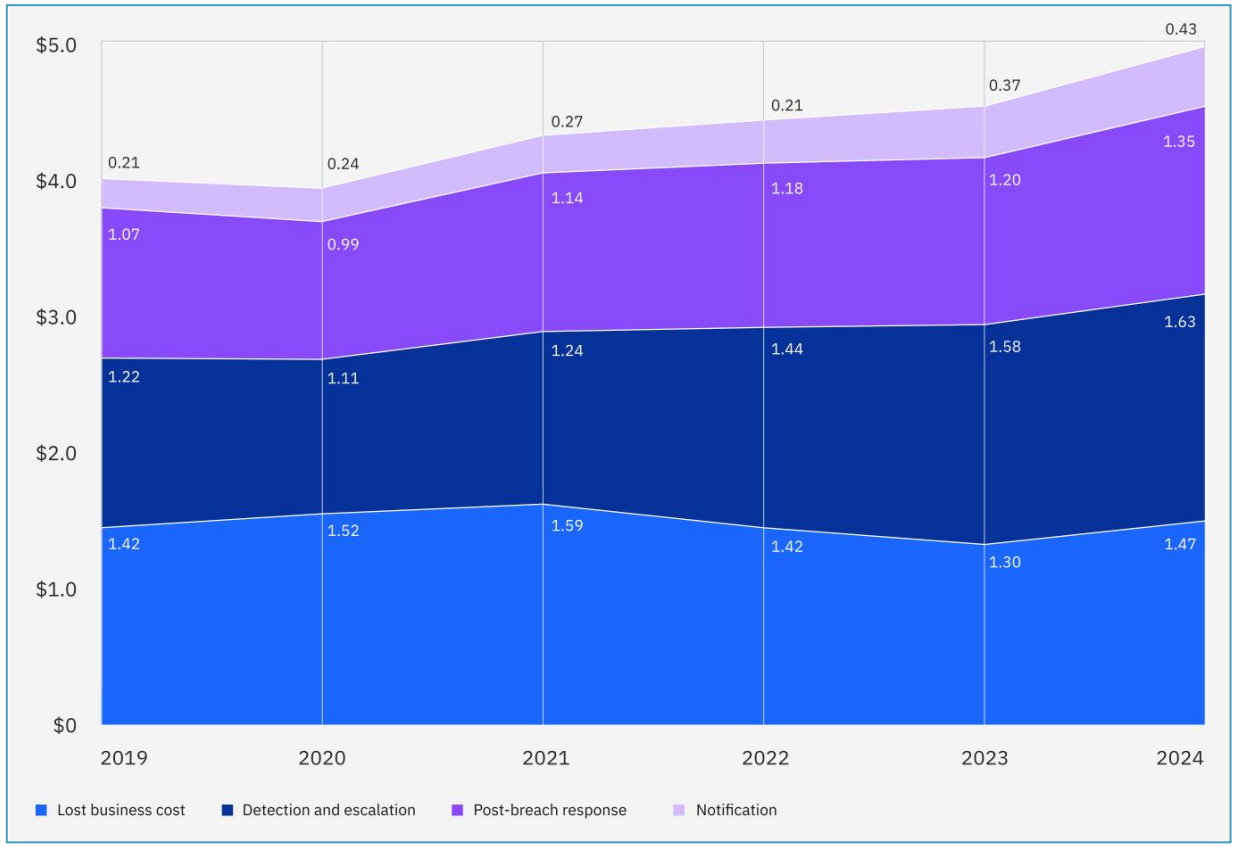
2024:

The number of organizations paying **more than USD 50,000 in regulatory fines** as a result of a data breach **rose 22.7%** over the previous year; those paying **more than USD 100,000 rose 19.5%** *

* Source: IBM Cost of a Data Breach 2024 Report, available at https://www.ibm.com/think/topics/cybersecurity

Cybersecurity: Cost of a Data Breach (2) *

Fig. 1. Average Cost of a Data Breach in Four Components *



Lost business costs and post-breach response costs soared

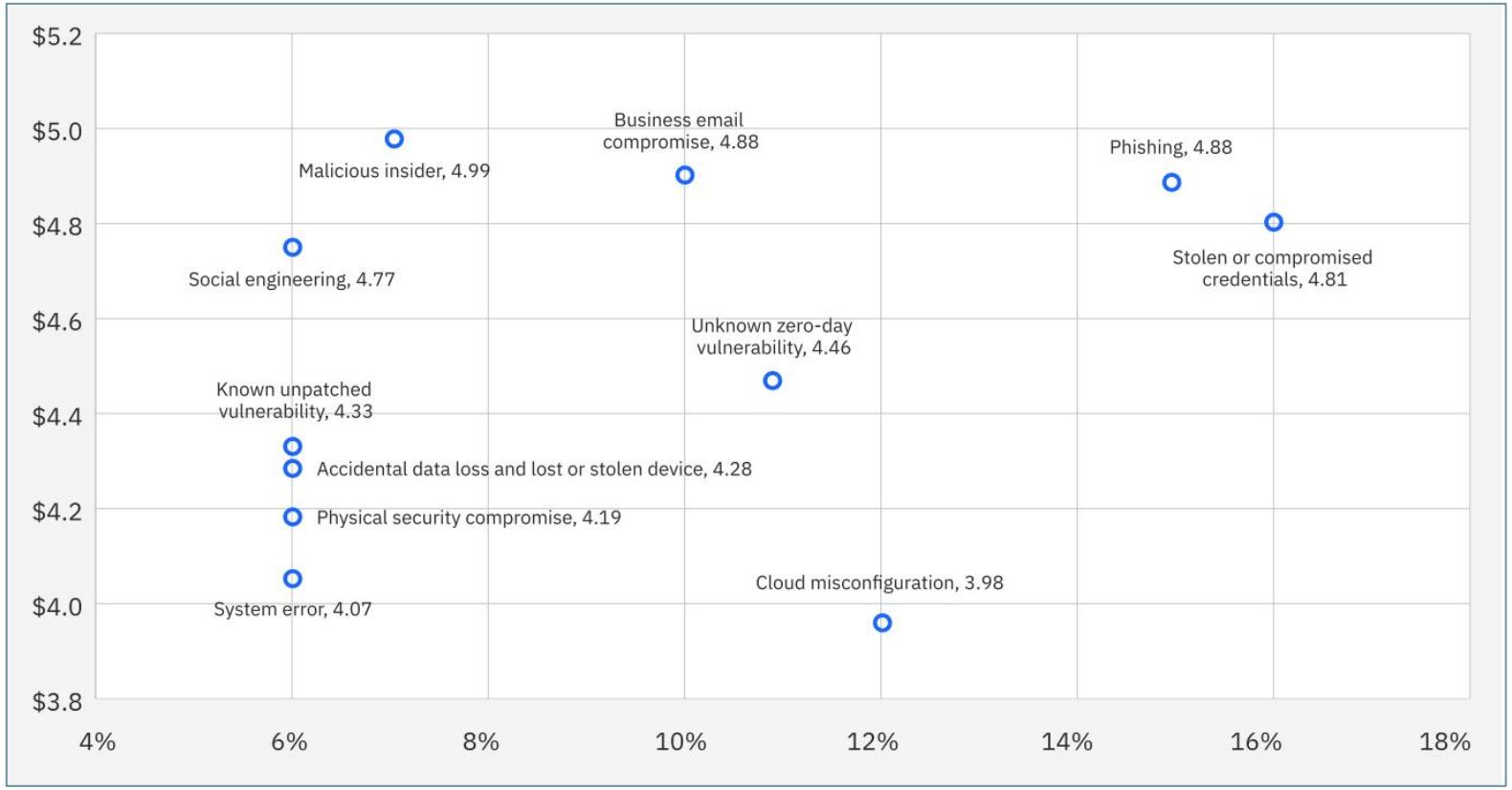
Costs from lost business and post-breach response rose nearly 11% over the previous year, which contributed to the significant rise in overall breach costs. Lost business costs include revenue loss due to system downtime, and the cost of lost customers and reputation damage. Post-breach costs can include the expense of setting up call centers and credit monitoring services for impacted customers, and paying regulatory fines.

Fig.1.: measured in USD millions.

* Source: IBM Cost of a Data Breach 2024 Report, available at https://www.ibm.com/think/topics/cybersecurity

Cost and Frequency of a Data Breach *

Fig. 2. Cost and Frequency of a Data Breach by Initial Attack Vector *



Phishing and stolen or compromised credentials were the 2 most prevalent attack vectors. Both also ranked among the top 4 costliest incident types.

Fig.2: Measured in USD millions; Percentage of all breaches.

* Source: IBM Cost of a Data Breach 2024 Report, available at https://www.ibm.com/think/topics/cybersecurity

Cybersecurity Challenges *

- **The pervasive adoption of cloud computing** can increase network management complexity and raise the risk of cloud misconfigurations, improperly secured APIs and other avenues hackers can exploit.
- **More remote work, hybrid work and bring-your-own-device (BYOD)** policies mean more connections, devices, applications and data for security teams to protect.
- **Proliferating Internet of Things (IoT) and connected devices**, many of which are unsecured or improperly secured by default, can be easily hijacked by bad actors.
- **The rise of artificial intelligence (AI), and of generative AI in particular**, presents an entirely new threat landscape that hackers are already exploiting through prompt injection and other techniques. According to recent research from the IBM® Institute for Business Value, only 24% of generative AI initiatives are secured.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity

Significant Cyber Incidents in 2025 *

- **January 2025**: Suspected **Russian hackers** executed spearphishing attacks against Kazakh diplomatic entities. Attackers imbedded malicious code within diplomatic documents, including one allegedly outlining an agreement between Germany and several Central Asian countries, for cyber espionage purposes *.
- **January 2025**: A **pro-Russian hacking group** claimed responsibility for a cyberattack targeting Italian government websites, including ministries, public services, and transportation platforms in cities like Rome and Palermo. The attack was reportedly a response to Italian Prime Minister Giorgia Meloni's meeting with Ukrainian President Volodymyr Zelenskyy, where she reiterated support for Ukraine *.

* Source: Center for Strategic and International Studies, 2025, available at https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Significant Cyber Incidents in 2025 (2) *

- **January 2025 ***: **Russian cyberattacks on Ukraine** surged by nearly 70% in 2024, with 4,315 incidents targeting critical infrastructure, including government services, the energy sector, and defense-related entities. Ukraine's cybersecurity agency reported that attackers aimed to steal sensitive data and disrupt operations, with tactics such as malware distribution, phishing, and account compromises.
- **January 2025 ***: **Cyberattacks on Taiwan by Chinese groups** doubled to 2.4 million daily attempts in 2024, primarily targeting government systems and telecommunications firms, according to Taiwan's National Security Bureau. Attackers aimed to steal sensitive data and disrupt critical infrastructure, with successful attacks rising by 20% compared to 2023.

* Source: Center for Strategic and International Studies, 2025, available at https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Cyberthreats vs IT Outage: Regional and Global Incidents

1) **UK: In January 2025, Barclays**' IT Glitch locked customers out of their accounts for two consequetive days *;
2) **UK: In September 2023**, **Transport for London (TfL)** has restricted its online services as its computer systems were affected by a cyber attack **;
3) **UK: In August 2022,** a cyber-attack on a major IT provider of the **NHS** has been confirmed as a ransomware attack ***.

* Source: Guardian, available at https://www.theguardian.com/business/2025/feb/02/barclays-says-it-glitch-that-locked-customers-out-of-accounts-is-fixed

** Source: BBC, available at https://www.bbc.co.uk/news/technology-62506039

*** Source: BBC, available at https://www.bbc.co.uk/news/articles/cwyjezrne3go

Cyberthreats vs IT Outage: Regional and Global Incidents (2)

2) **Global: In March 2025,** crypto exchange ByBit's Hack - $ 1.5 bln (£1.1 bln) of stolen funds **;

3) **Global: In 2014,** crypto exchange Mt Gox filed for bankruptcy after $350m (£210m) worth of digital currency had been stolen due to a loophole in its security **.

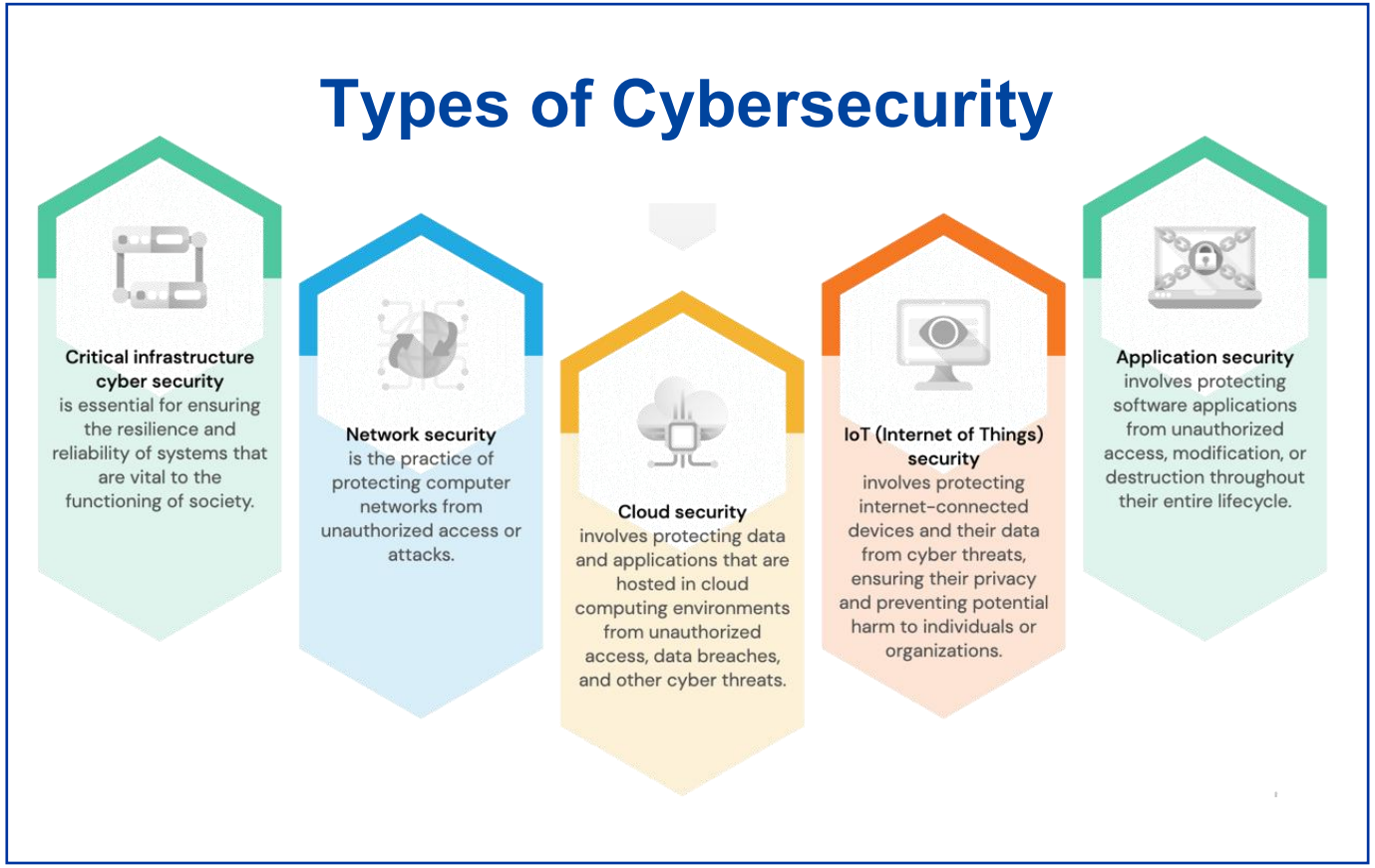
4) **Global: In 2019,** hackers stole $41m worth of bitcoin (BTC) from the Binance exchange in another major crypto-currency heist **.

* Source: Guardian, available at https://www.theguardian.com/business/2025/feb/02/barclays-says-it-glitch-that-locked-customers-out-of-accounts-is-fixed

** Source: BBC, available at https://www.bbc.co.uk/news/articles/cx2844nvwx8o

Types of Cybersecurity *

- AI security
- **Critical infrastructure security**
- **Network security**
- Endpoint security
- **Application security**
- **Cloud security**
- Information security
- Mobile security



* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity

I. AI Security *

- **AI security** refers to measures and technology aimed at preventing or mitigating cyberthreats and cyberattacks that target AI applications or systems or that use AI in malicious ways.
- **Generative AI** offers threat actors **new attack vectors to exploit**. Hackers can use malicious prompts to manipulate AI apps, poison data sources to distort AI outputs and even trick AI tools into sharing sensitive information. They can also use (and have already used) generative AI to create malicious code and phishing emails.
- AI security uses specialized risk management frameworks - and increasingly, AI-enabled cybersecurity tools - to protect the AI attack surface. Organizations that deployed AI-enabled security tools and automation extensively for cyberthreat prevention saw a USD 2.2 million lower average cost per breach compared to organizations with no AI deployed**.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity

** Source: IBM Cost of a Data Breach 2024 Report, available at https://www.ibm.com/think/topics/cybersecurity

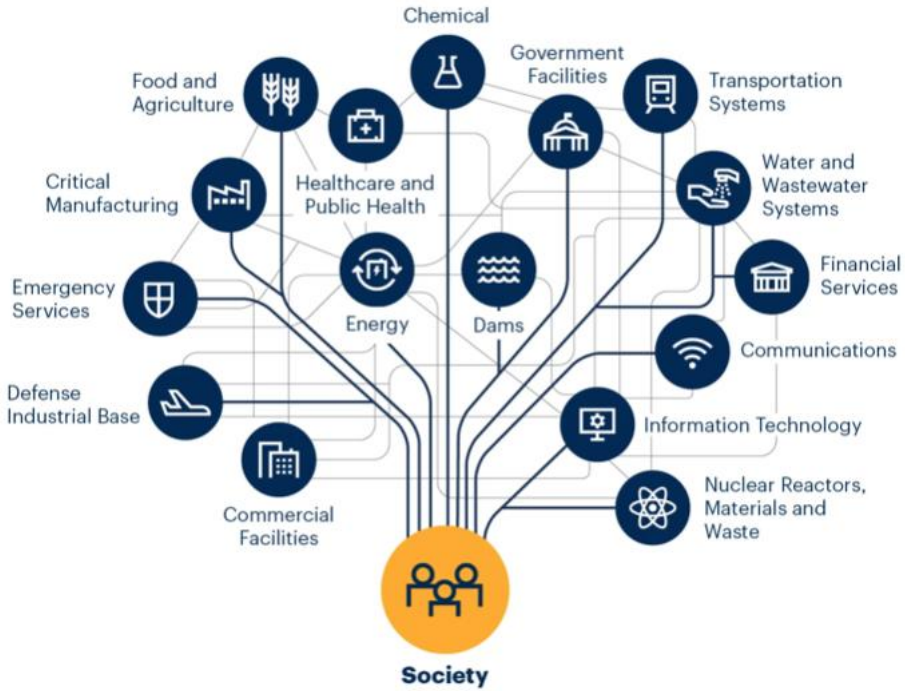
II. Critical Infrastructure Security *

- **Critical infrastructure security** protects the computer systems, applications, networks, data and digital assets that a society depends on for national security, economic health and public safety.
- **Example 1.** In the United States, the National Institute of Standards and Technology (NIST) offers a cybersecurity framework to help IT providers and stakeholders secure critical infrastructure. The US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) also provides guidance.
- **Example 2**. In the UK, responsibility for the protection of the CNI IT networks, data and systems from cyber attack sits with the National Cyber Security Centre (NCSC). NPSA works in partnership with the NCSC so that collectively we deliver holistic advice that takes into account all aspects of protective security.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity

II. Critical Infrastructure Security (2)

16 Critical Infrastructure Sectors in the US *



13 Critical Infrastructure Sectors in the UK **

1. Chemicals
2. Civil Nuclear
3. Communications
4. Defence
5. Emergency Services
6. Energy
7. Finance
8. Food
9. Government
10. Health
11. Space
12. Transport
13. Water

* Source: Gartner, 2022, available at https://www.gartner.com;

** Source: NPSA, 2025, available at https://www.npsa.gov.uk/critical-national-infrastructure-0

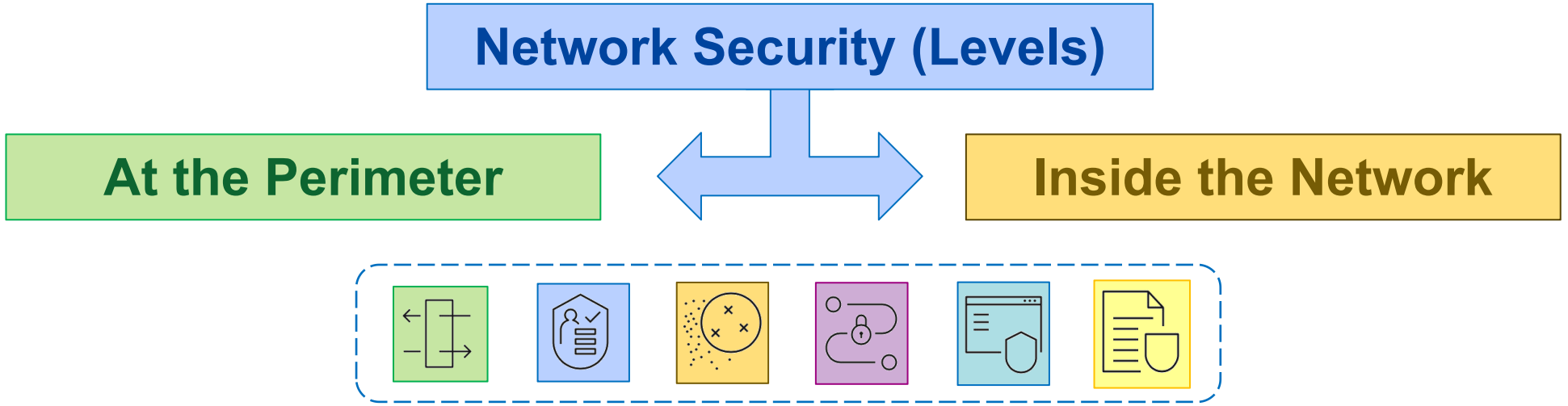
III. Network Security *

- **Network security** focuses on preventing unauthorized access to networks and network resources. It also helps ensure that authorized users have secure and reliable access to the resources and assets they need to do their jobs *.
- **Network security** is the field of cybersecurity focused on protecting computer networks and systems from internal and external cyberthreats and cyberattacks. Network security has three chief **aims** **:
  1. to prevent unauthorized access to network resources;
  2. to detect and stop cyberattacks and security breaches in progress;
  3. to ensure that authorized users have secure access to the network resources they need, when they need them.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity

** Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security

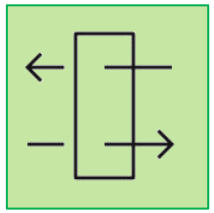
III. Network Security (2) *



At the **perimeter**, security controls try to stop cyberthreats from entering the network. But **network attackers** sometimes break through, so IT security teams also put controls around the resources inside the network, such as laptops and data. Even if attackers get in, they won't have free reign. This strategy - layering multiple controls between hackers and potential vulnerabilities - is called "**defense in depth**" *.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security

III. Network Security (3) *



Firewalls

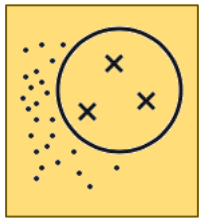
A **firewall** is software or hardware that stops suspicious traffic from entering or leaving a network while letting legitimate traffic through. Firewalls can be deployed at the edges of a network or used internally to divide a larger network into smaller subnetworks. If one part of the network is compromised, hackers are still shut off from the rest.

Network access control (NAC)

Network access control solutions act like gatekeepers, authenticating and authorizing users to determine who is allowed into the network and what they can do inside. "Authentication" means verifying that a user is who they claim to be. It also means granting authenticated users permission to access network resources.

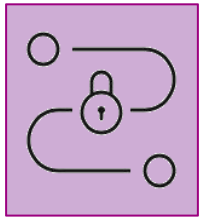
* Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security

III. Network Security (4) *



Intrusion detection and prevention systems (IDPSs)

An **intrusion detection and prevention system** - sometimes called an intrusion prevention system - can be deployed directly behind a firewall to scan incoming traffic for security threats. These security tools evolved from intrusion detection systems, which only flagged suspicious activity for review. IDPSs have the added ability to automatically respond to possible breaches, such as by blocking traffic or resetting the connection. IDPSs are particularly effective at detecting and blocking brute force attacks and denial of service (DoS) or distributed denial of service (DDoS) attacks.



Virtual private networks (VPNs)

A **virtual private network (VPN)** protects a user's identity by encrypting their data and masking their IP address and location. When someone uses a VPN, they no longer connect directly to the internet but to a secure server that connects to the internet on their behalf.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security

III. Network Security (5) *

Application security

Application security refers to the steps security teams take to protect apps and **application programming interfaces (APIs)** from network attackers. Because many companies today use apps to carry out key business functions or process sensitive data, apps are a common target for cybercriminals. And because so many business apps are hosted in public clouds, hackers can exploit their vulnerabilities to break into private company networks.

Email security

Phishing is the most common initial cyberattack vector **. Email security tools can help thwart phishing attacks and other attempts to compromise users' email accounts. Most email services have built-in security tools like spam filters and message encryption. Some email security tools feature sandboxes, isolated environments where security teams can inspect email attachments for malware without exposing the network.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security

** Source: IBM X-Force Threat Intelligence Index 2024, available at https://www.ibm.com/reports/threat- intelligence

III. Network Security: Related Technologies *

- **Data loss prevention (DLP)** refers to information security strategies and tools that ensure sensitive data is neither stolen nor accidentally leaked. DLP includes data security policies and purpose-built technologies that track data flows, encrypt sensitive information and raise alerts when suspicious activity is detected.
- **Web security** solutions, such as secure web gateways, block malicious internet traffic and keep users from connecting to suspicious websites and apps.
- **Network segmentation** is a way of breaking large networks down into smaller subnetworks, either physically or through software. Network segmentation can limit the spread of ransomware and other malware by walling off a compromised subnetwork from the rest of the network. Segmentation can also help keep legitimate users away from assets they shouldn't access.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security

III. Network Security: Related Technologies (2) *

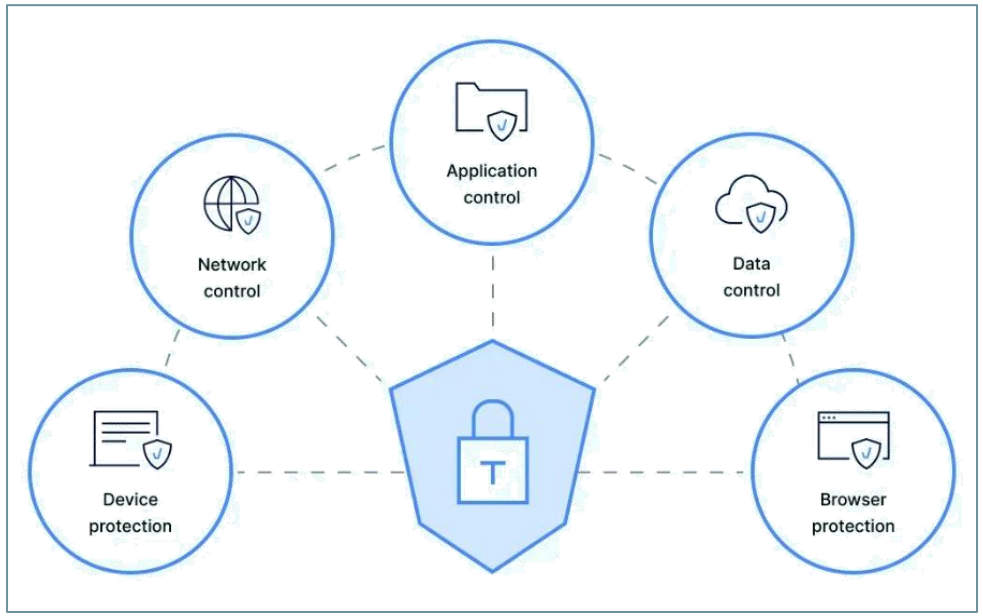
- **Cloud Security** solutions protect data centers, apps and other cloud assets from cyberattacks. Most cloud security solutions are simply standard network security measures—such as firewalls, NACs, and VPNs—applied to cloud environments. Many cloud service providers build security controls into their services or offer them as add-ons.
- **User and Entity Behavior Analytics (UEBA)** uses behavioral analytics and machine learning to flag abnormal user and device activity. UEBA can help catch insider threats and hackers who have hijacked user accounts.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security

** Image source: HyTrust (A Model for Securing Cloud Workloads)

IV. Endpoint Security *

- **Endpoint security** solutions protect any devices that connect to a network - such as laptops, desktops, servers, mobile devices or IoT devices - against hackers who try to use them to sneak into the network.



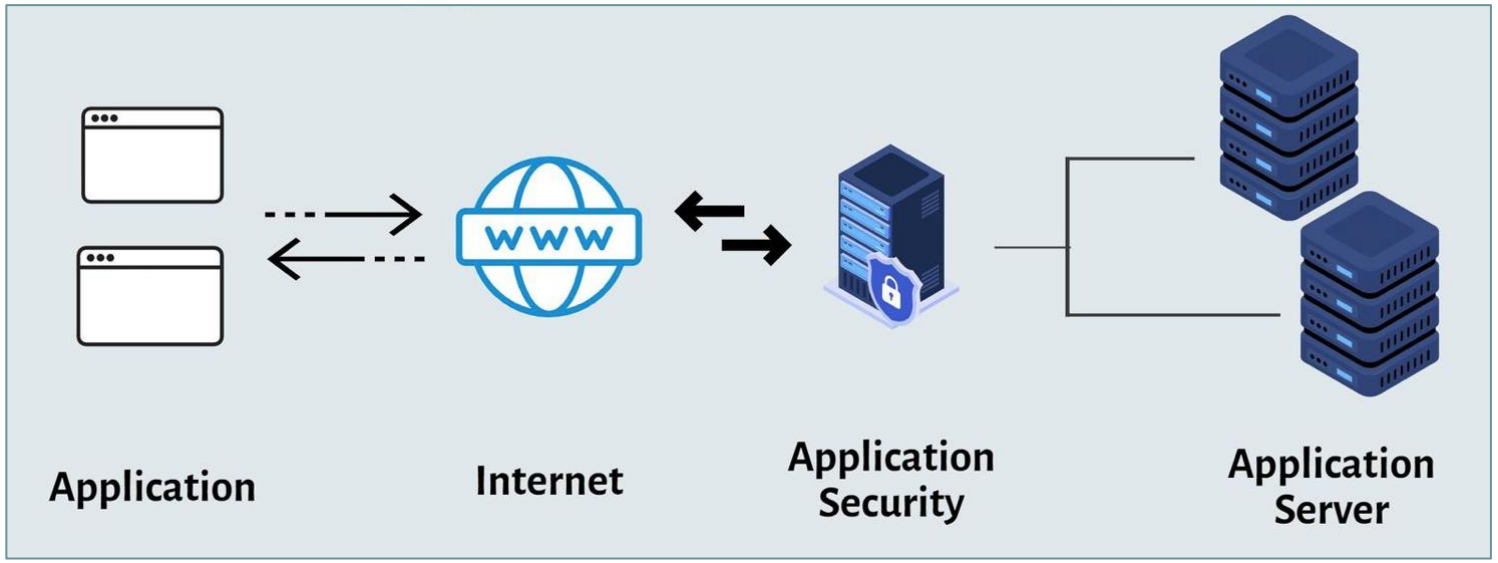
Antivirus software can detect and destroy trojans, spyware, and other malicious software on a device before it spreads to the rest of the network.

Endpoint detection and response solutions are more advanced tools that monitor endpoint behavior and automatically respond to security events. Unified endpoint management software allows companies to monitor, manage and secure all end-user devices from a single console.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security
** Image source: Nordlayer, available at https://nordlayer.com/blog/what-is-endpoint-security/

IV. Application Security *

Application security helps prevent unauthorized access to and use of apps and related data. It also helps identify and mitigate flaws or vulnerabilities in application design.



Modern application development methods such as DevOps and DevSecOps build security and security testing into the development process.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security

** Image source: Atatus, 2025, available at https://www.atatus.com/glossary/application-security/

V. InfoSec, Data Security and Mobile Security *

Information security (InfoSec) protects an organization's important information—digital files and data, paper documents, physical media—against unauthorized access, use or alteration.

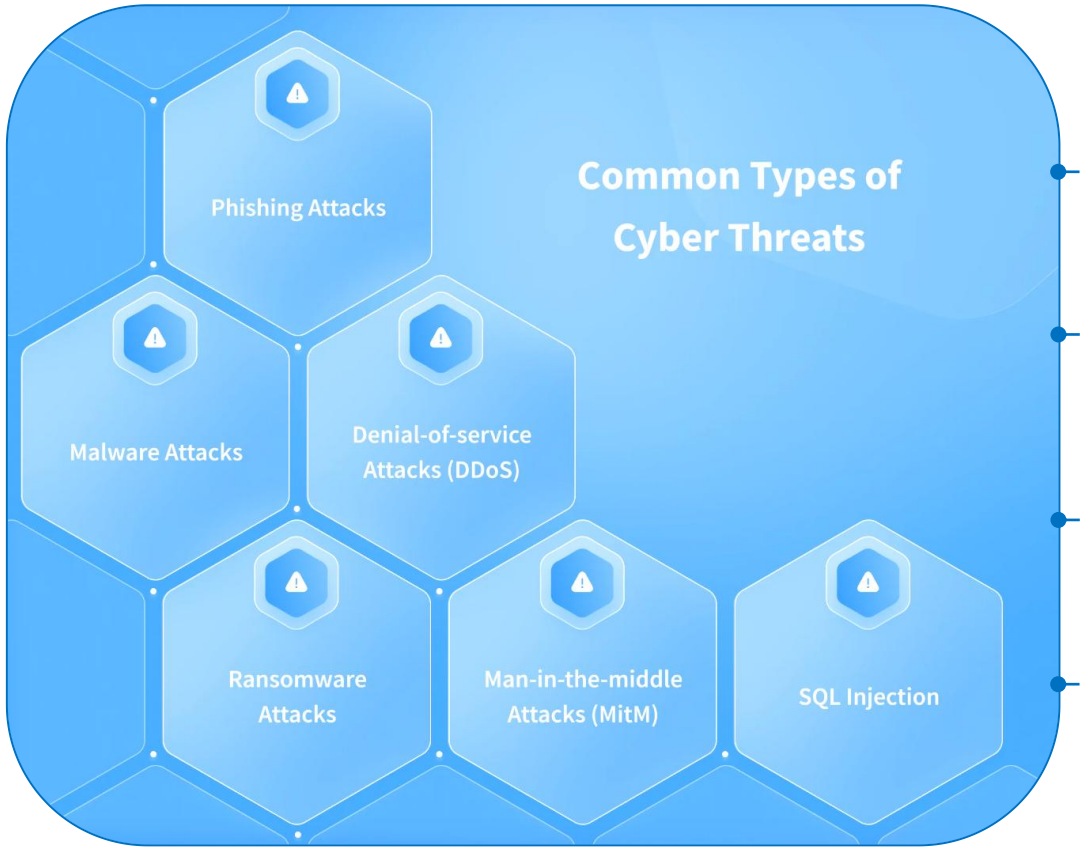
Data security, the protection of digital information, is a subset of information security and the focus of most cybersecurity-related InfoSec measures.

Mobile security encompasses cybersecurity tools and practices specific to smartphones and other mobile devices, including mobile application management (MAM) and enterprise mobility management (EMM).

More recently, organizations are adopting unified endpoint management (UEM) solutions that allow them to protect, configure and manage all endpoint devices, including mobile devices, from a single console.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security

Common Cybersecurity Threats *

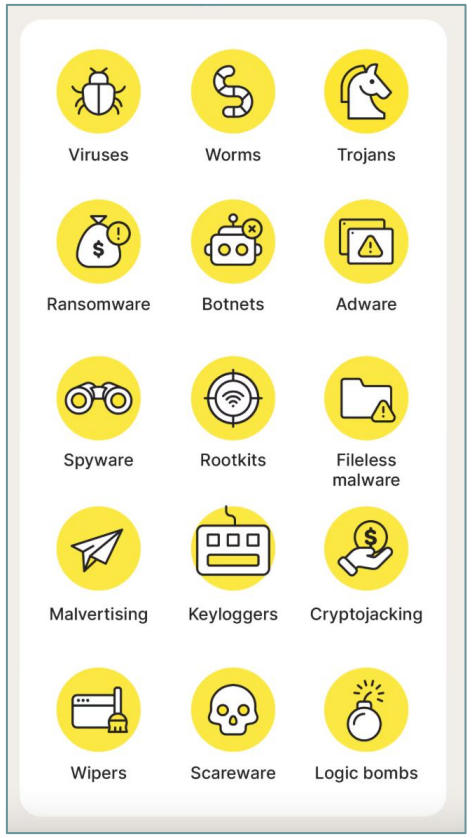


- Malware
- Ransomware
- Phishing
- Credential Theft and abuse
- Insider Threats
- AI Attacks
- Cryptojacking
- Distributed denial of service
- (DDoS)

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity
** Image source: NIX, available at https://nix-united.com/blog/personal-cyber-security-tips-and-best-practices/

I. Cybersecurity Threats: Malware *

Types of Malware



- **Malware**, short for "**malicious software**", is any software code or computer program that is intentionally written to harm a computer system or its users. Almost every modern cyberattack involves some type of malware.
- Hackers and cybercriminals create and use malware to gain unauthorized access to computer systems and sensitive data, hijack computer systems and operate them remotely, disrupt or damage computer systems, or hold data or systems hostage for large sums of money (see **"ransomware"**).

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity
** Image source: Norton, 2025, available at https://uk.norton.com/blog/malware/types-of-malware

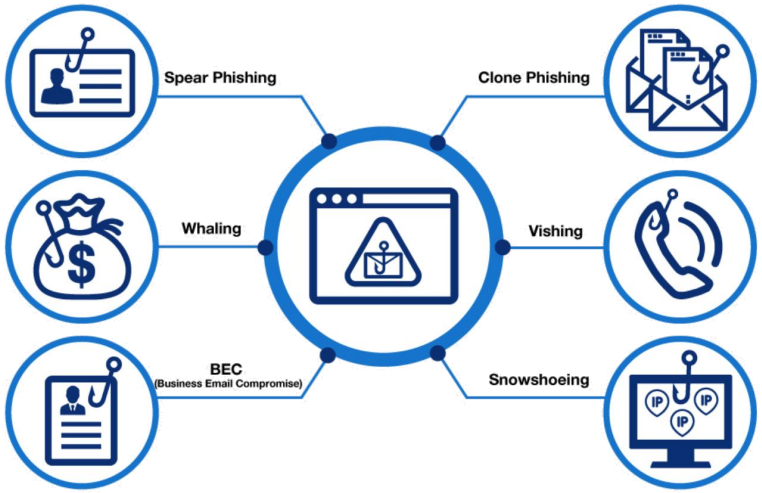
II. Cybersecurity Threats: Ransomware *

- **Ransomware** is a type of malware that encrypts a victim's data or device and threatens to keep it encrypted - or worse - unless the victim pays a ransom to the attacker.
- The **earliest ransomware attacks** demanded a ransom in exchange for the encryption key required to unlock the victim's data. Starting around 2019, almost all ransomware attacks were double extortion attacks that also threatened to publicly share victims' data; some triple extortion attacks added the threat of a distributed denial-of-service (DDoS) attack.
- More recently, ransomware attacks are **on the decline**. Ransomware attacks accounted for 20% of all attacks in 2023, down 11.5% from 2022 **. The decline is likely the result of improved ransomware prevention, more effective law enforcement intervention and data backup and protection practices that enable businesses to recover without paying the ransom.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity

** Source: IBM X-Force Threat Intelligence Index 2024, available at https://www.ibm.com/reports/threat- intelligence

III. Cybersecurity Threats: Phishing *



- **Phishing attacks** are email, text or voice messages that trick users into downloading malware, sharing sensitive information or sending funds to the wrong people.
- **Bulk phishing scams** - mass - mailed fraudulent messages that appear to be from a large and trusted brand, asking recipients to reset their passwords or reenter credit card information.
- More sophisticated phishing scams, such as **spear phishing** and **business email compromise (BEC)**, target specific individuals or groups to steal especially valuable data or large sums of money.

Phishing is just one type of social engineering, a class of "human hacking" tactics and interactive attacks that use psychological manipulation to pressure people into taking unwise actions.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security
** Image source: Fortinet, available at https://www.fortinet.com/resources/cyberglossary/phishing

IV. Cybersecurity Threats: Credential Theft and Account Abuse *

- **Identity-based attacks**, which hijack legitimate user accounts and abuse their privileges, account for 30% of attacks **. This makes identity-based attacks the most common entry point into corporate networks.
- Hackers have many techniques for stealing credentials and taking over accounts.
- **Example 1.** Kerberoasting attacks manipulate the Kerberos authentication protocol commonly used in Microsoft Active Directory to seize privileged service accounts. In 2023, the IBM X-Force team experienced a 100% increase in Kerberoasting incidents **.
- **Example 2.** the X-Force team saw a 266% increase in the use of infostealer malware that secretly records user credentials and other sensitive data **.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security
** Source: IBM X-Force Threat Intelligence Index 2024, available at https://www.ibm.com/reports/threat- intelligence

V. Cybersecurity Threats: Insider Threats *

- **Insider threats** are threats that originate with authorized users—employees, contractors, business partners—who intentionally or accidentally misuse their legitimate access or have their accounts hijacked by cybercriminals.
- **Insider threats** can be harder to detect than external threats because they have the earmarks of authorized activity and are invisible to antivirus software, firewalls and other security solutions that block external attacks.

Insider Threat Expressions **

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security

** Imange source: CISA.

VI. Cybersecurity Threats: AI Attacks *

- Much like cybersecurity professionals are using AI to strengthen their defenses, cybercriminals are using AI to conduct advanced attacks.
- **In generative AI fraud**, scammers use generative AI to produce fake emails, applications and other business documents to fool people into sharing sensitive data or sending money.
- Scammers can use open **source generative AI tools to craft convincing phishing emails** in as little as **five minutes** **. For comparison, it takes scammers 16 hours to come up with the same message manually.
- Hackers are also using organizations' AI tools as attack vectors. For example, in **prompt injection attacks**, threat actors use malicious inputs to manipulate generative AI systems into leaking sensitive data, spreading misinformation or worse.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security

** Source: IBM X-Force Threat Intelligence Index 2024, available at https://www.ibm.com/reports/threat- intelligence

VII. Cybersecurity Threats: Cryptojacking *

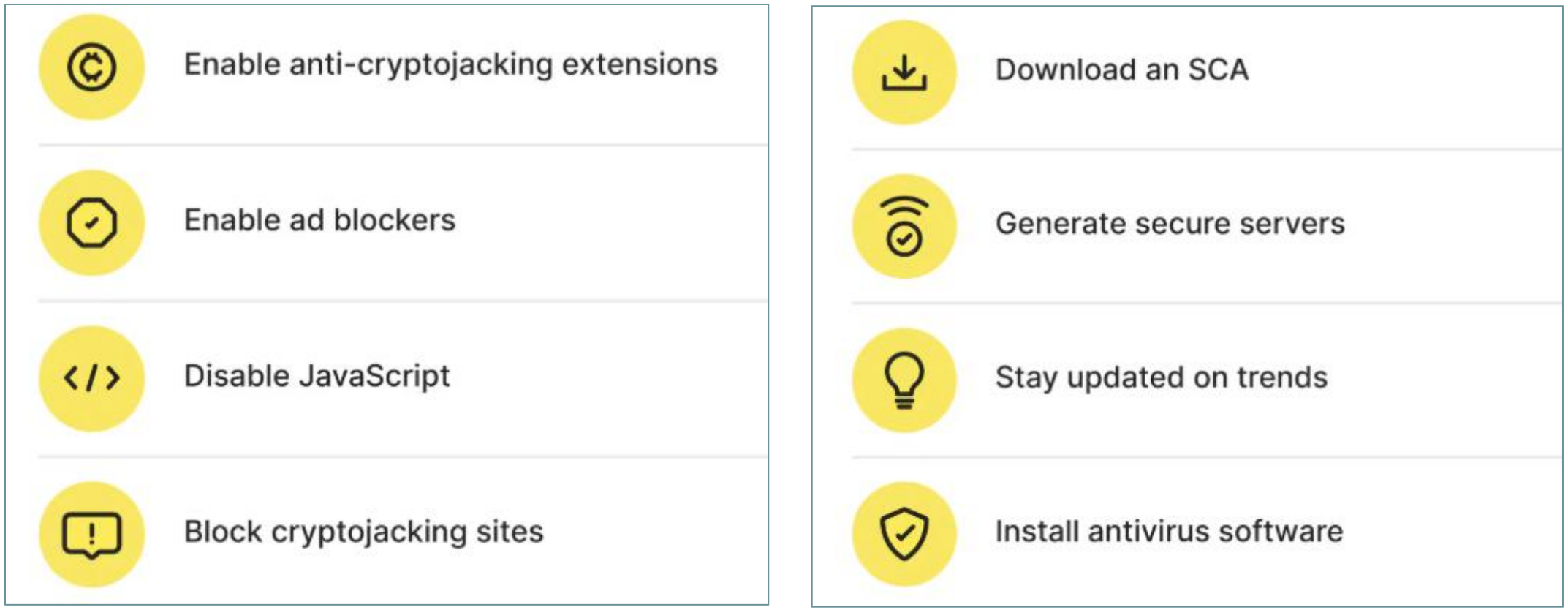
How Cryptojacking Works **

- **Cryptojacking** happens when hackers gain access to an endpoint device and secretly use its computing resources to mine cryptocurrencies such as bitcoin (BTC), ether (ETH) or monero (XMR).
- Security analysts identified cryptojacking as a cyberthreat around 2011, shortly after the introduction of cryptocurrency. **Cryptojacking is now among the top three areas of operations for cybercriminals** **.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security
** Source: Norton, available at https://us.norton.com/blog/emerging-threats/cryptojacking

VII. Cybersecurity Threats: Cryptojacking (2) *

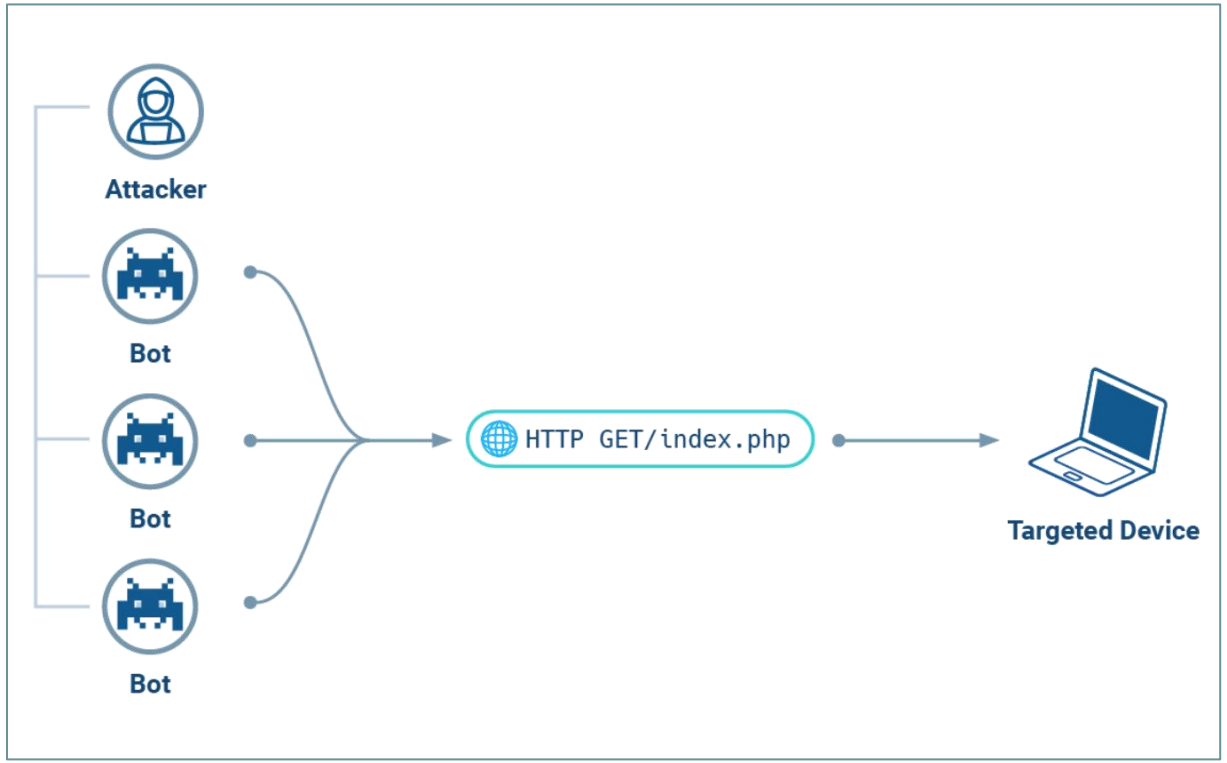
How To Prevent Cryptojacking **



* Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security

** Source: Norton, available at https://us.norton.com/blog/emerging-threats/cryptojacking

VIII. Cybersecurity Threats: Distributed denial of service (DDoS) *



A **Distributed denial of service (DDoS) attack** attempts to crash a server, website or network by overloading it with traffic, usually from a botnet - a network of distributed systems that a cybercriminal hijacks by using malware and remote-controlled operations.

The global volume of DDoS attacks spiked during the COVID-19 pandemic. Increasingly, attackers are combining DDoS attacks with ransomware attacks, or simply threatening to launch DDoS attacks unless the target pays a ransom.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/network-security;
** Image source: Haproxy, available at https://www.haproxy.com/glossary/what-is-a-distributed-denial-of-service-ddos-attack

Cybersecurity Myths *

1). "Strong passwords are adequate protection":

For example, a 12-character password takes 62 trillion times longer to crack than a 6-character password. But passwords are relatively easy to acquire in other ways, such as through ***social engineering, keylogging malware, buying them on the dark web or paying disgruntled insiders*** to steal them;

2). "Most cybersecurity risks are well-known":

In fact, the cyberthreat ***landscape is constantly changing***. Thousands of new vulnerabilities are reported in old and new applications and devices every year. ***Opportunities for human error*** - specifically by negligent employees or contractors who unintentionally cause a data breach - keep increasing.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity

Cybersecurity Myths (2) *

3). "All cyberattack vectors are contained":

Cybercriminals find new attack vectors all the time*. The rise of AI technologies, operational technology (OT), Internet of Things (IoT) devices and cloud environments* all give hackers new opportunities to cause trouble;

4). "My industry is safe":

Every industry has its share of cybersecurity risks. For example, ransomware attacks are targeting more sectors than ever, including local governments, nonprofits and healthcare providers. Attacks on supply chains, ".gov" websites and critical infrastructure have also increased.

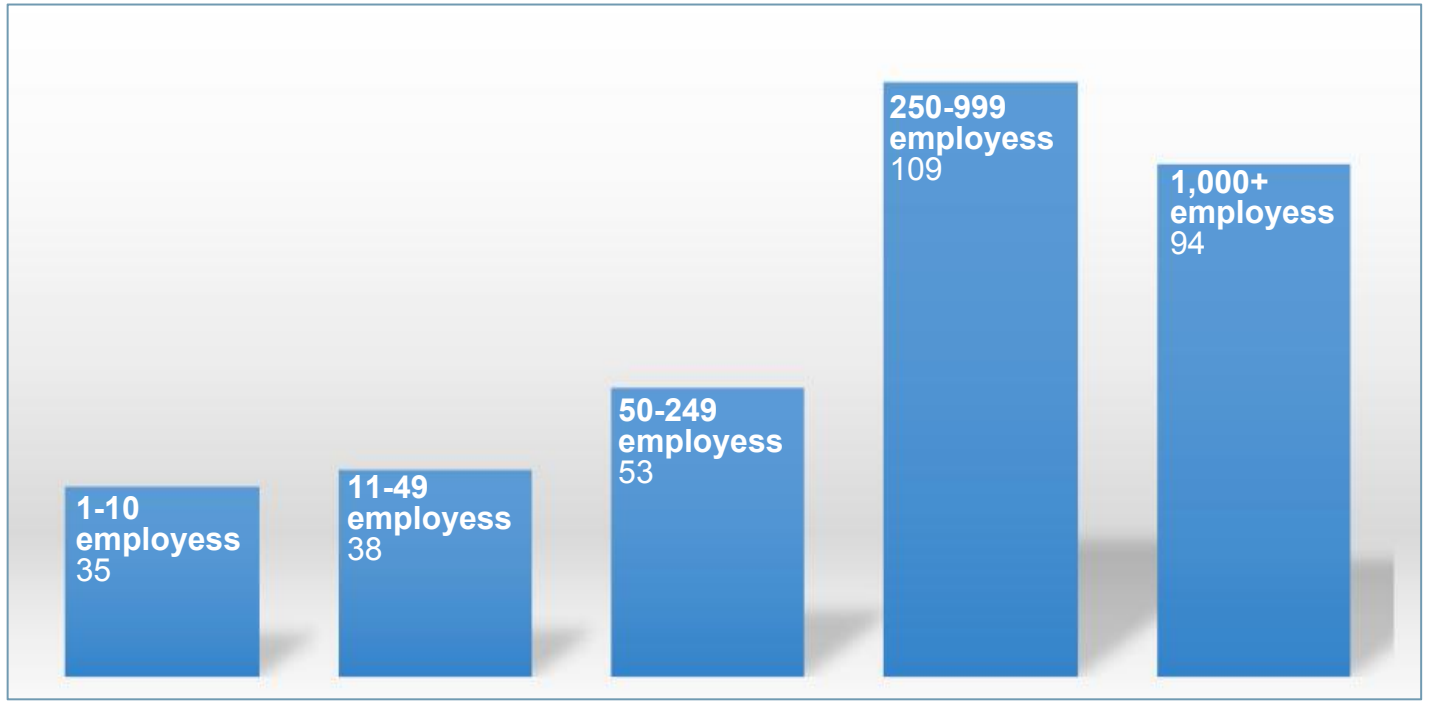
* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity

Cybersecurity Myths (3) *

5). "Cybercriminals don't attack small businesses":

In fact, they do. The Hiscox Cyber Readiness Report found that almost half (41%) of small businesses in the US experienced a cyberattack in the last year**.

Fig. 3. Average number of Cyber attacks in 2023 **

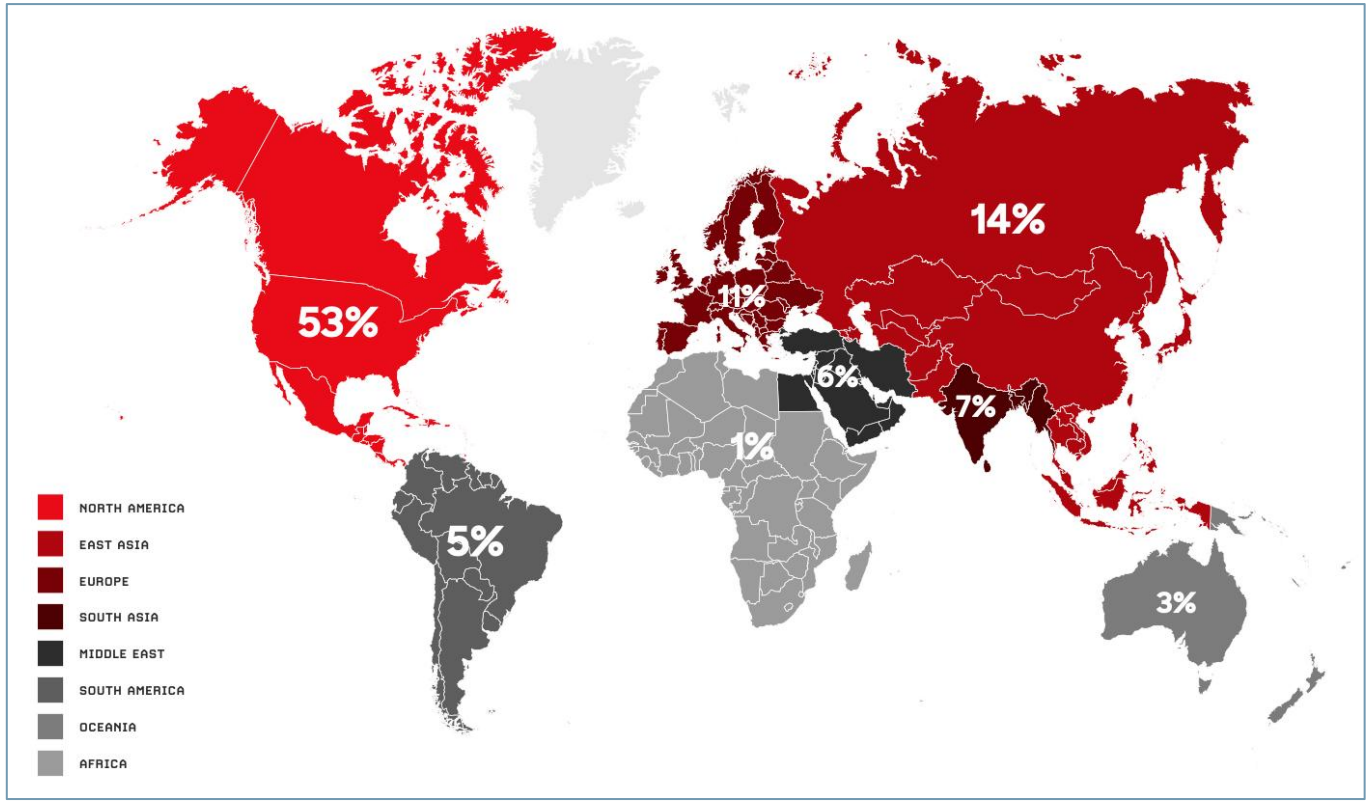


* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity

** Source: The Hiscox Cyber Readiness Report 2024, available at https://www.hiscoxgroup.com/cyber-readiness

Interactive Intrusions: Global Upward Trend

Fig. 4. Interactive Intrusions by Region, Jan. - Dec. 2024 *



Modern cyber threats are increasingly dominated by "**interactive intrusion**" techniques, where adversaries execute hands-on-keyboard actions to achieve objectives.

Unlike traditional malware attacks, these intrusions rely on human adversaries ***mimicking legitimate user or administrator behavior***, making them exceptionally difficult to detect.

* Source: 2025 Global Threat Report, available at https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf

Interactive Intrusions: Global Upward Trend (2)

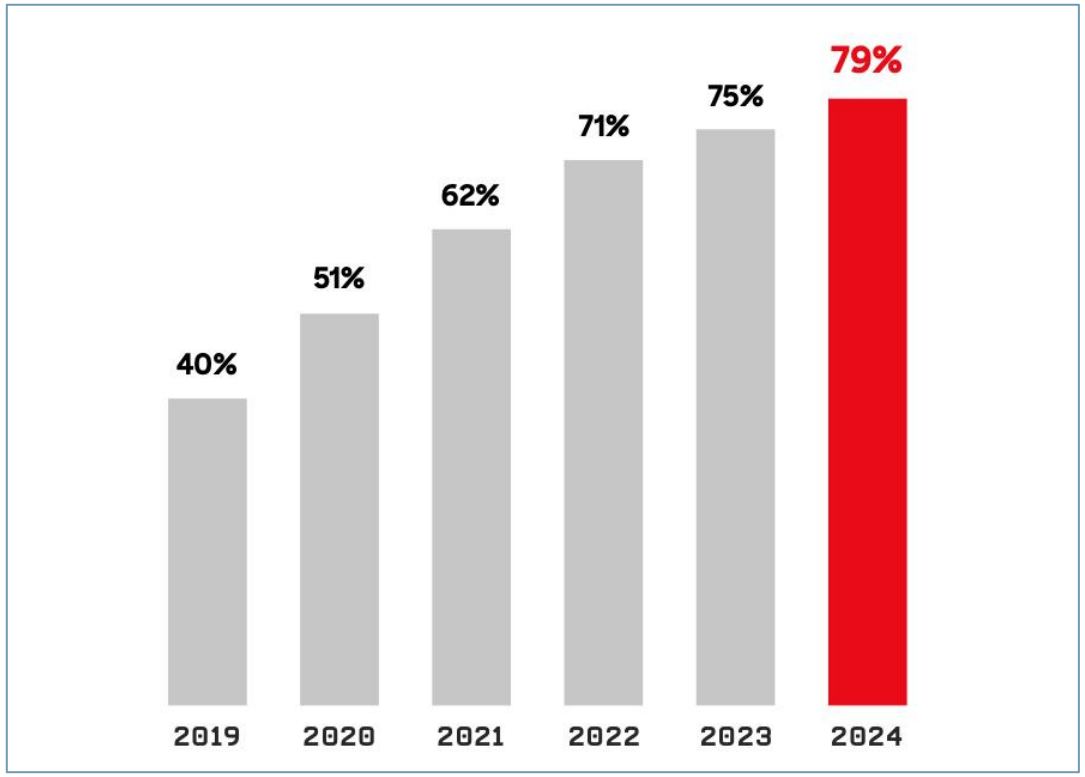
Fig. 5. Top 10 Industries Targeted by Interactive Intrusions, Jan. - Dec. 2024 *

In 2024, the report observed a 35% year-over-year increase in interactive intrusion campaigns. For the seventh consecutive year (2017-2024), the **technology sector** remained the most targeted industry, with high attack volumes also observed in consulting, manufacturing, and retail. The charts on the following page reflect the relative frequency of intrusions in the industry verticals *.

* Source: 2025 Global Threat Report, available at https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf

Interactive Intrusions: Global Upward Trend (3)

Fig. 6. Percentage of Malware-Free Detections, 2019- 2024 *



These statistics highlight the global reach of adversary operations and the necessity for cross-domain security strategies that account 40% for identity compromise, lateral movement, and cloud-based attack vectors.

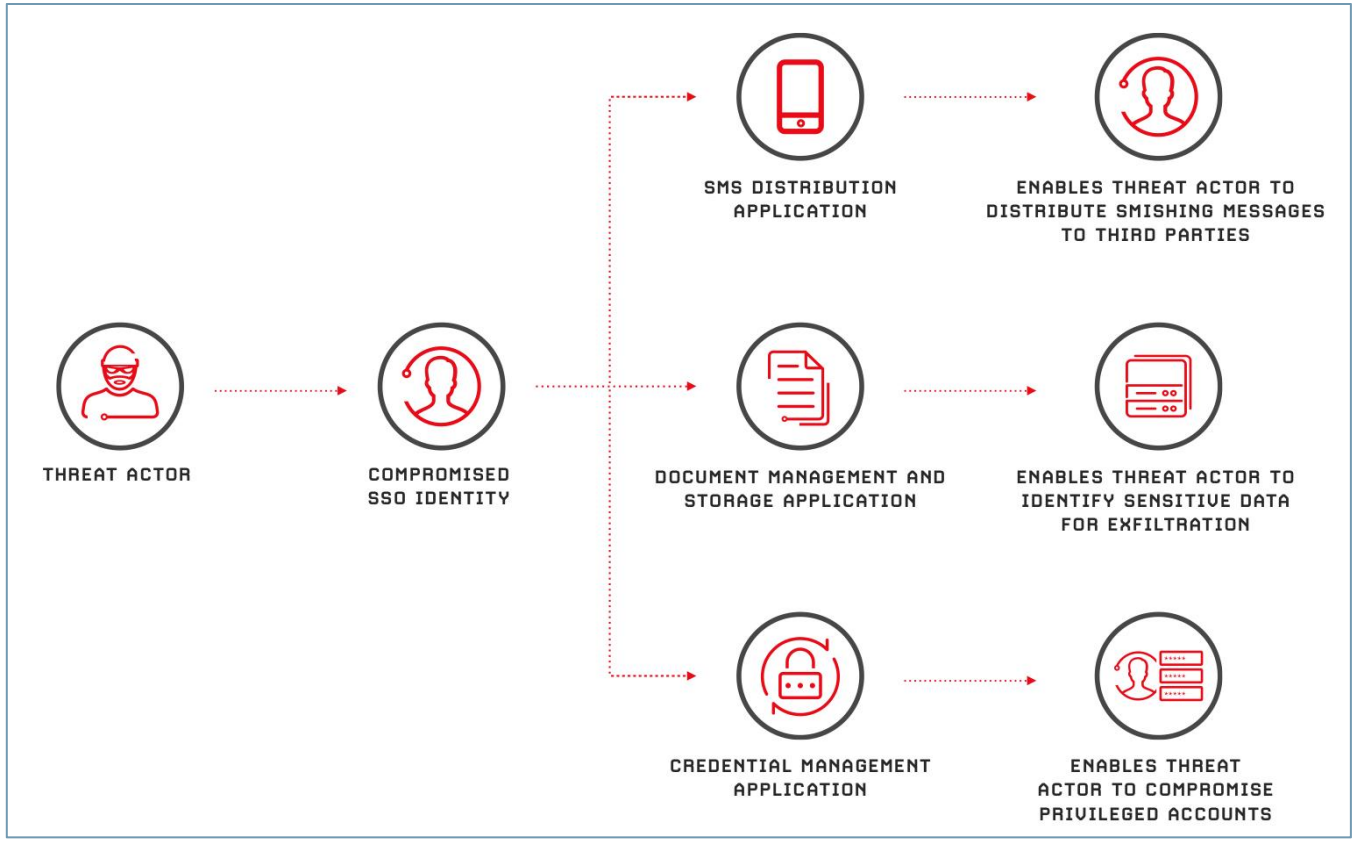
This shift toward malware-free attack techniques has been a defining trend over the past five years.

In 2024, malware-free activity accounted for 79% of detections, a significant rise from 40% in 2019.

* Source: 2025 Global Threat Report, available at https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf

SaaS Exploitation Techniques *

Fig. 7. SaaS Exploitation Techniques *

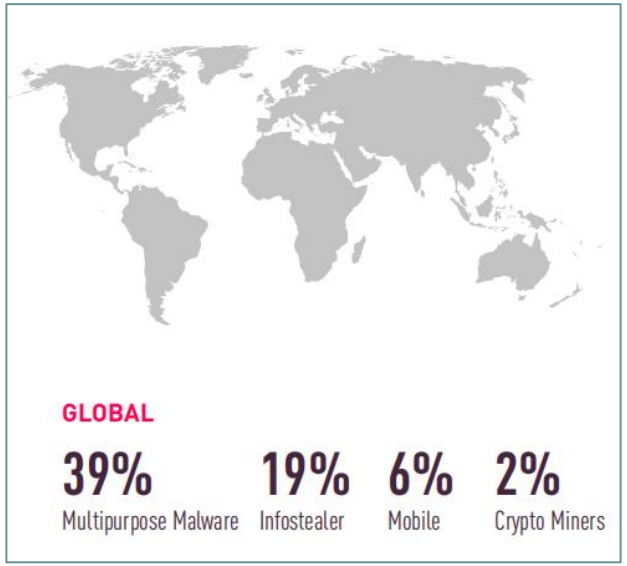


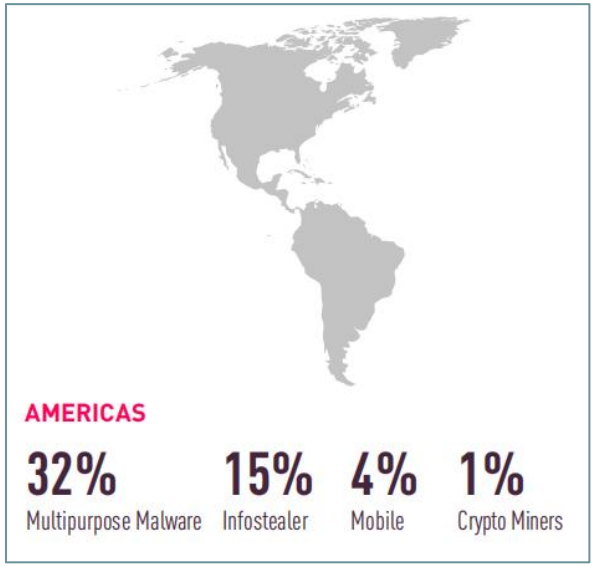
In 2025, enterprising adversaries will undoubtedly continue to seek advanced exploitation opportunities across multiple domains, specifically cloud-based SaaS applications, to access sensitive data and conduct lateral movement. With many organizations migrating data from on-premises systems to cloud-based services, adversaries are expected to continue to adapt their tradecraft accordingly *.

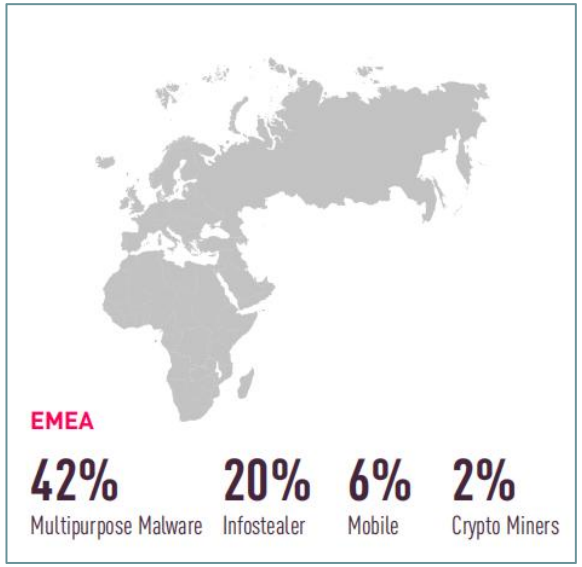
* Source: 2025 Global Threat Report, available at https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrikeGlobalThreatReport2025.pdf

Cyberattacks by Region in 2024 *

Fig. 8. Percentage of Organizations affected by Malware Type in 2024 *







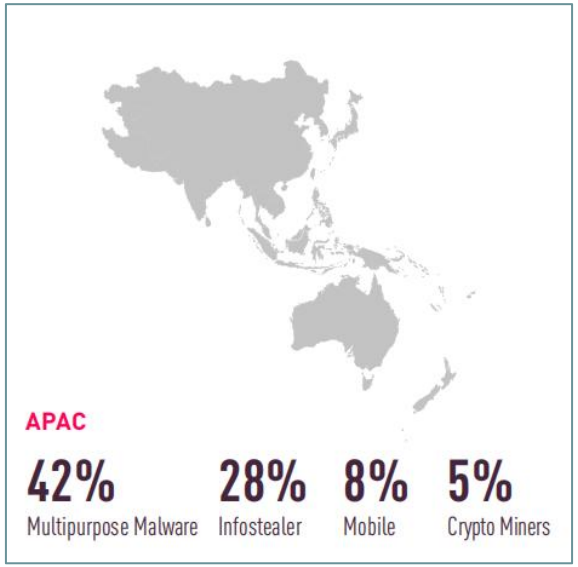


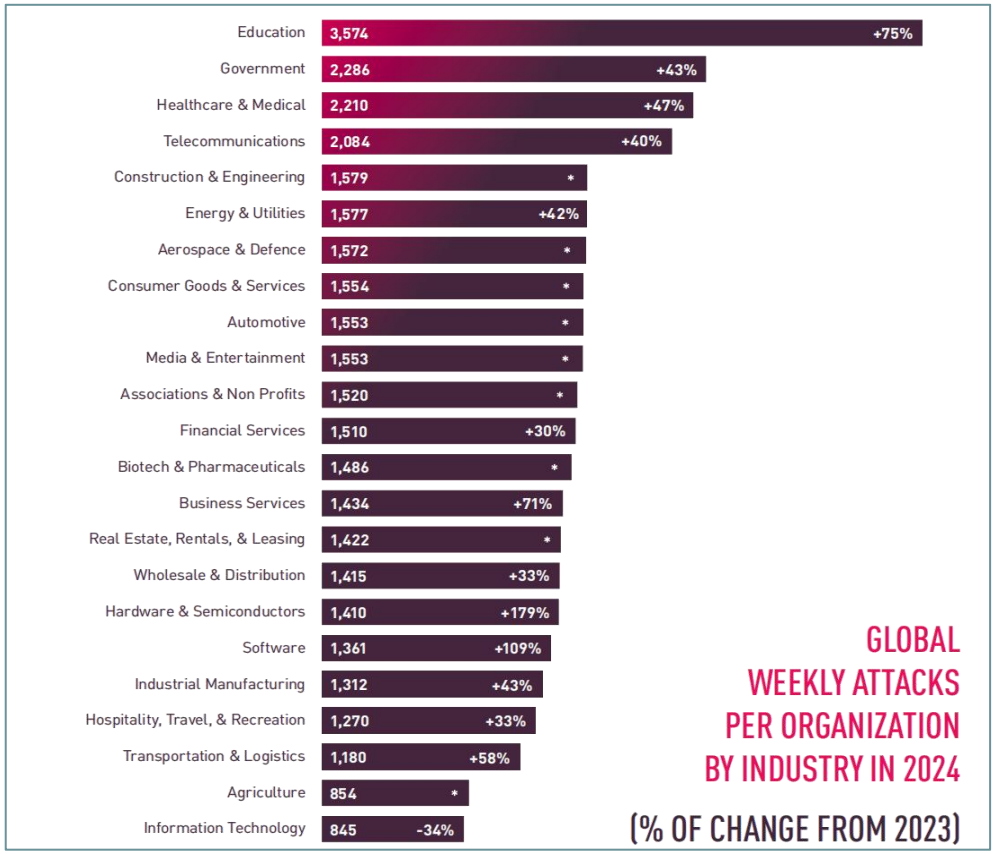
Figure 8 shows attacks according to malware type. These numbers exclude general scans and only deal with direct attacks, which enabled us to classify the type of malware and its intention.

In 2024, there was a notable increase in attempted attacks by both Infostealers and Multipurpose malware. Multipurpose malware (RATs, botnets, and bankers) is frequently used in the initial stages of an attack to drop additional tools and expand the attackers' control over the breached system. It's therefore unsurprising that this is the most common malware type, with 39% of organizations affected in 2024. This figure marks a significant 25% increase compared to 2023 when only 31% of organizations faced similar attempts.

* Source: The State of Cybersecurity 2025 Report, available at https://engage.checkpoint.com/security-report-2025/

Global Weekly Attacks Per Organization by Industry in 2024 *

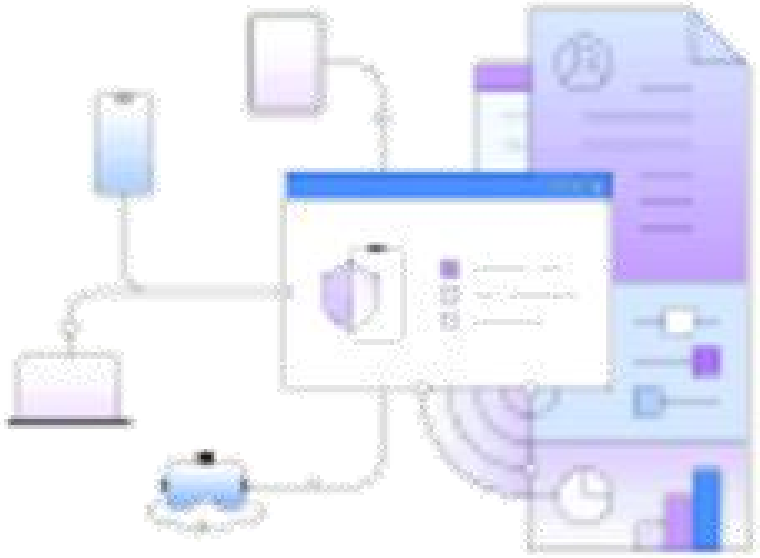
Fig. 9. The Average Number of Weekly Attacks per Organization by Industry in 2024 *



In 2024, there was a significant increase in the number of attacks per week across most sectors. Education institutions were specifically targeted for personal information collection. This persistent rise in attack rates impacts universities, schools, and educational departments and services. The technological supply chain sector, including software, hardware, and semiconductor companies, also experienced a significant surge in cyberattacks. Notably, the hardware and semiconductor industries saw the sharpest rise, with a staggering 179% increase in average weekly attacks, with the total number now exceeding 1,400. This spike can be attributed to the growing global demand for hardware and the heightened focus on AI technologies. As critical components of modern infrastructure and innovation, these industries have become prime targets for cyber criminals seeking to exploit supply chain vulnerabilities for financial gain, espionage, or disruption.

* Source: The State of Cybersecurity 2025 Report, available at https://engage.checkpoint.com/security-report-2025/

Cybersecurity: Best Practices and Technologies *



- Security awareness training
- Data security tools
- Identity and access management
- Threat detection and response
- Disaster recovery

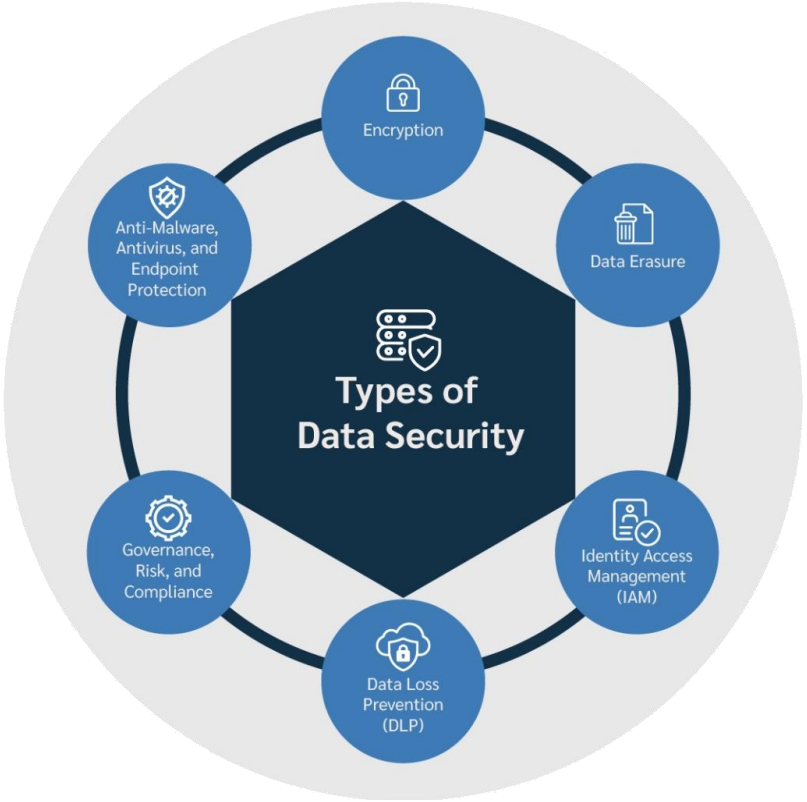
* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity

I. Cybersecurity: Security Awareness Training *

- **Security awareness training** helps users understand how seemingly harmless actions - from using the same simple password for multiple log-ins to oversharing on social media - increase their own or their organization's risk of attack.
- Combined with thought-out data security policies, security awareness training can help employees protect sensitive personal and organizational data. It can also help them recognize and avoid phishing and malware attacks.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity

II. Cybersecurity: Data Security Tools *



- **Data security tools**, such as **encryption** and **data loss prevention (DLP)** solutions, can help stop security threats in progress or mitigate their effects.
- **For example**, DLP tools can detect and block attempted data theft, while encryption can make it so that any data that hackers steal is useless to them.

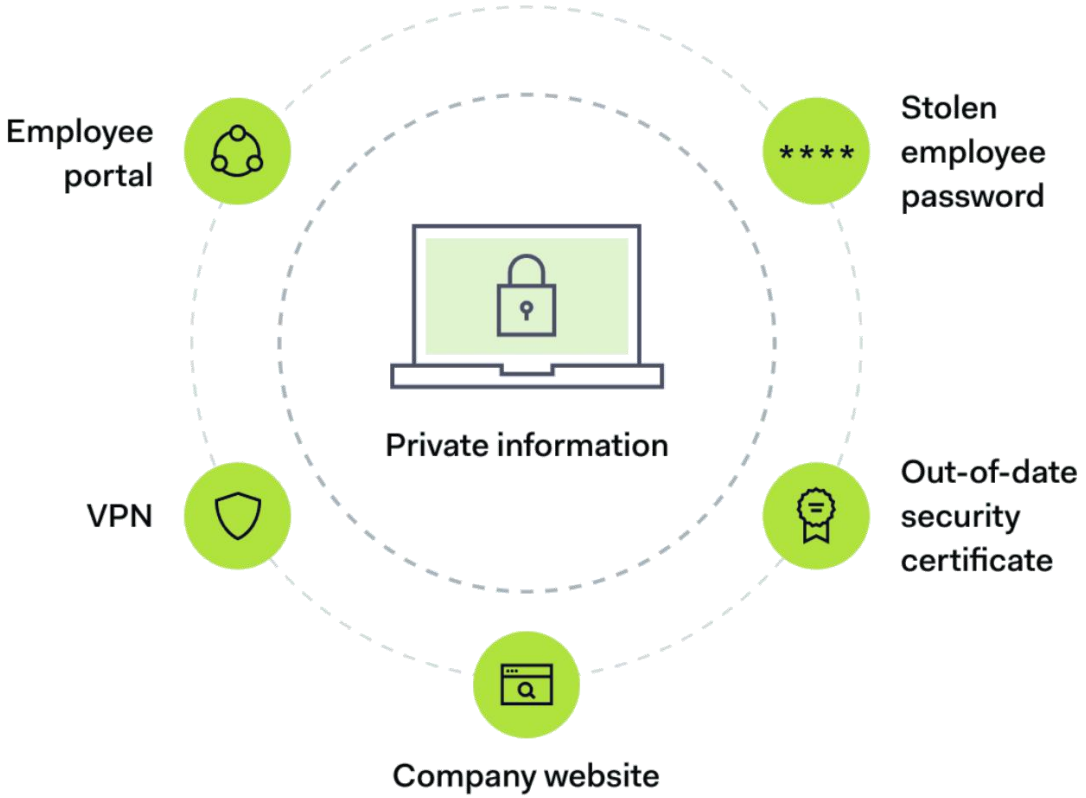
* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity;
** Image source: Memcyco, available at https://www.memcyco.com/data-security-management/

III. Cybersecurity: Identity and Access Management *

- **Identity and access management (IAM)** refers to the tools and strategies that control how users access resources and what they can do with those resources.
- **IAM technologies** can help protect against **account theft**. For example, multifactor authentication requires users to supply multiple credentials to log in, meaning threat actors need more than just a password to break into an account.
- Likewise, **adaptive authentication systems** detect when users are engaging in risky behavior and raise additional authentication challenges before allowing them to proceed. Adaptive authentication can help limit the lateral movement of hackers who make it into the system.
- A **zero trust architecture** is one way to enforce strict access controls by verifying all connection requests between users and devices, applications and data.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity

IV. Cybersecurity: Attack Surface Management *



- **Attack surface management (ASM)** is the continuous discovery, analysis, remediation and monitoring of the cybersecurity vulnerabilities and potential attack vectors that make up an organization's attack surface.
- Unlike other cyberdefense disciplines, **ASM** is conducted **entirely from a hacker's perspective** rather than the perspective of the defender. It identifies targets and assesses risks based on the opportunities they present to a malicious attacker.

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity;
** Image source: Nordlayer, available at https://nordlayer.com/blog/attack-surface-management-a-brief-guide/

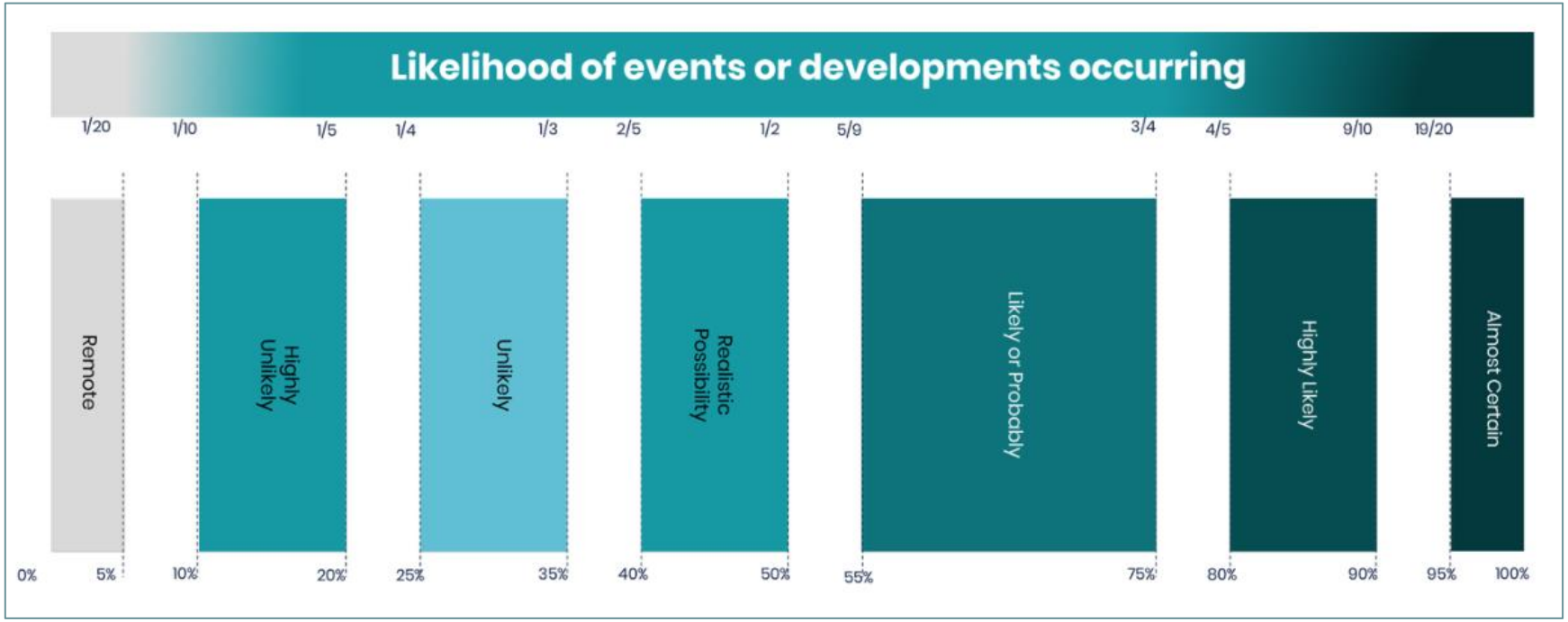
V. Cybersecurity: Threat Detection and Response and Disaster Recovery *

- **Analytics- and AI-driven technologies** can help identify and respond to attacks in progress. These technologies can include security information and event management (SIEM), security orchestration, automation and response (SOAR) and endpoint detection and response (EDR). Typically, organizations use these technologies as part of a formal incident response plan.
- **Disaster recovery** capabilities can play a key role in maintaining business continuity and remediating threats in the event of a cyberattack. For example, the ability to fail over to a backup that is hosted in a remote location can help a business resume operations after a ransomware attack (sometimes without paying a ransom)

* Source: IBM, 2025, available at https://www.ibm.com/think/topics/cybersecurity

Case 1. The Near-Term impact of AI on the Cyberthreat in the UK, 2024 - 2026 *

Fig. 10. How Likely is a Realistic Probability? *



Professional Head of Intelligence Assessment (PHIA) probability yardstick

NCSC Assessment uses the PHIA probability yardstick every time we make an assessment, judgement, or prediction. The terms used correspond to the likelihood ranges (see Fig. 10)

* Source: NCSC Assessment 2024, available at https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

Case 1. The Near-Term impact of AI on the Cyberthreat in the UK, 2024 - 2026 (2) *

- **Artificial intelligence (AI)** will almost certainly increase the volume and heighten the impact of cyber attacks over the next two years. However, the impact on the cyber threat will be uneven.
- The threat to 2025 comes from evolution and enhancement of existing tactics, techniques and procedures (TTPs).
- **All types of cyber threat actor** – state and non-state, skilled and less skilled – are already **using AI**, to varying degrees.
- AI provides capability uplift in reconnaissance and social engineering, almost certainly making both more effective, efficient, and harder to detect.
- More sophisticated uses of AI in cyber operations are highly likely to be restricted to threat actors with access to quality training data, significant expertise (in both AI and cyber), and resources. More advanced uses are unlikely to be realised before 2025.

* Source: NCSC Assessment 2024, available at https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

Case 1. The Near-Term impact of AI on the Cyberthreat in the UK, 2024 - 2026 (3) *

- **AI will almost certainly make cyber attacks against the UK more impactful** because threat actors will be able to analyse exfiltrated data faster and more effectively, and use it to train AI models.
- **AI lowers the barrier for novice cyber criminals**, hackers-for-hire and hacktivists to carry out effective access and information gathering operations. This enhanced access will likely contribute to the global ransomware threat over the next two years.
- Moving towards 2025 and beyond, **commoditisation of AI-enabled capability in criminal and commercial markets** will almost certainly make improved capability **available to cyber crime and state actors**.

* Source: NCSC Assessment 2024, available at https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

Research Activity 3. Cyberthreats in the Modern World on the Regional and International Levels

Research Activity 3. Brainstorming: Cyberthreats in the Modern World on the Regional and International Levels

Steps to follow:

1. Choose the cyberthreat incident within a region or country to be investigated;
2. Conduct research anaylsis on the selected cyberthreat incident;
3. Present the summary of the selected cyberthreat incident:
    - Identify features and security challenges of the incident;
    - Analyse preferred solutions for a disaster recovery;
    - Apply secondary data to present the evidence for your conclusions.

Q&A

Thank you!