Bytes Holiday Hangover

Welcome back! Here are your holiday hangover headaches for 2025!

The complex geopolitical environment is shaping the cyber threat landscape. Politically-motivated cyber threat actors are leveraging malicious activities such as social engineering, DDoS attacks, data breaches, and spyware deployment. Security investments in new and innovative technologies are likely to spark retaliatory cyber action from state-backed groups.

20 +

Years' Experience in Security

£115M +

Security Projects Delivered Annually

2024 in 12 Threat statistics

Over 1000 new vulnerabilities are identified weekly **(Statista)**	30% year-over-year increase in number of weekly cyber attacks **(CheckPoint)**	75% increase in cloud intrusions, highlighting the need for robust cloud security measures. **(CrowdStrike)**	$2.73million average ransom demanded, almost $1million more than 2023. **(Varonis)**
99% of Organisations noticed phishing becoming more advanced, sophisticated and quicker **(ISF)**	67% of successful cyberattacks resulted from human negligence, or human-based attacks **(ISACA Journal)**	94% of Malware was delivered by email **(Varonis)**	$22million Ransom following the change Healthcare attack by Ransom Hub **(Integrity 360)**
560 million customer details stolen in Ticketmaster breach **(BBC)**	99% of identity attacks are password based **(Microsoft)**	Nation-State actors increasingly collaborate with Cybercriminals. North Korea have stolen over $3billion in crypto **(Microsoft)**	Education and Research sector targeted by nation-state actors for valuable information. **(Microsoft)**

BYTES

Headline Statistics for 2025

Global Cybercrime Costs:
Cybercrime is expected to cost the world $10.5 trillion annually by 2025 *[Cybersecurity Ventures].*

Ransomware Attacks:

59% of all organisations are projected to be hit by ransomware attacks in 2025. *[Sophos]*

Regulatory Compliance:
Regulatory compliance requirements will tighten, with more stringent cybersecurity regulations being imposed on organisations *[Strobes]*

AI attacks:

69% of organisations believe AI will be necessary to respond to cyberattacks by 2026. *[Capgemini]*

Human Error:

Despite advanced tools, human error remains the leading cause of breaches. A study by IBM found that 95% of breaches involve some form of human error. Common issues include weak passwords, falling for phishing scams, and mishandling sensitive data. *[IBM]*

Cyber Insurance:

Global cyber insurance premiums are projected to grow from $14 billion in 2023 to $29 billion by 2027. *[Munich RE]*

Top Threats for 2025

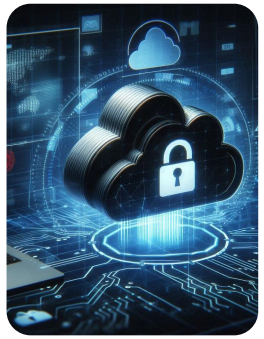
01

Geopolitical and State-Sponsored Threats

02

AI-driven Cyberattacks

03



Cloud Environment Vulnerabilities

04

Supply Chain attacks

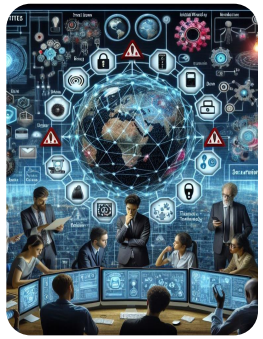
05

Social Engineering attacks

06

Quantum computing risks

07



IOT and Edge Devices

Geopolitical and State Sponsored Threats

2024

Cyberespionage

We saw Increased Cyber espionage from Russia/China, including breaches of government networks, exfiltration of sensitive data and political targeting by APTs.

AI Technology

Deepfake Technology became more prevalent, used to create convincing clones of high-profile individuals for fraud and to manipulate public opinion.

Election Interference

Numerous worldwide elections encouraged cyber operations aimed at influencing electoral outcomes, although improved defensive measures helped mitigate these threats.

Supply Chain Attack

These continued to be a significant threat, with nation-state actors targeting less secure elements of supply chains to compromise larger organisations.

1/3

More than one-third of CEOs expect geopolitical disruption to be among the top disruptive forces in the next 12 months. [EY]

50%

of Nation-states actors' targets will be government entities, think tanks, NGOs, IT, and education sectors. [ZeroFox]

2025

Increased Cyber warfare

Nation-states are likely to engage in more aggressive cyber warfare tactics, targeting critical infrastructure and government systems to disrupt services and gather intelligence.

AI-enhanced attacks

AI is likely to become more sophisticated, enabling more precise and damaging operations, including AI-driven malware and automated phishing campaigns.

Geopolitical Tensions

Ongoing geopolitical tensions, particularly between major powers like the US, Russia and China are highly likely to drive an increase in state-sponsored cyber activities aimed at espionage and disruption.

Supply-Chain vulnerabilities

Supply chain attacks are highly likely to continue to be a significant threat, with nation-state actors and cybercriminals targeting third-party vendors to gain access to large networks.

AI-driven Cyber attacks

2024

Targeted Cybercrime

The overall level of cybercrime reached record levels, with AI making attacks more targeted and efficient, with highly personalised and realistic phishing emails.

Automated Reconnaissance

AI tools were employed to automate the reconnaissance phase of cyberattacks, enabling attackers to quickly identify vulnerabilities and potential targets.

Deepfake Tech

The use of deepfake technology in cyberattacks increased, with attackers creating convincing video and audio impersonations of high-profile individuals to deceive and manipulate targets.

AI driven Malware

AI was used to develop more adaptive and resilient malware, capable of evading traditional detection methods and causing significant damage.

62-65%

In 2025, it is expected that 45-50% of phishing emails targeting businesses will be AI-generated, with the victim response rate potentially rising to 62-65% [VPN ranks]

Targeting

Cyber adversaries will increasingly target AI systems themselves, exploiting vulnerabilities in AI models, datasets, and operations. [Zdnet]

2025

AI-enhanced phishing

Attackers are almost certain to continue crafting ever more sophisticated AI-enhanced phishing emails, making it increasingly difficult to identify malicious communications.

Multi-channel attacks

Social engineering will almost certainly use multiple channels (email, text, phone) to build trust and create believable scenarios, making their attacks more effective.

Deepfake Technology

The use of deepfake technology will almost certainly continue to rise, with attacks creating realistic video and audio impersonations to deceive and manipulate targets.

Synthetic identities

Attackers are highly likely to use AI to create synthetic identities, combing real and fake information to impersonate individuals and gain unauthorised access.

Cloud Environment Vulnerabilities

2024

Cyberespionage

Increased Cyber espionage from Russia/China, including breaches of government networks, exfiltration of sensitive data and targeting of political campaigns by APTs.

AI Technology

Deepfake Technology became more prevalent, used to create convincing clones of high-profile individuals for fraud and to manipulate public opinion.

Election Interference

Numerous worldwide elections encouraged cyber operations aimed at influencing electoral outcomes, although improved defensive measures helped mitigate these threats.

Supply Chain Attack

These continued to be a significant threat, with nation-state actors targeting less secure elements of supply chains to compromise larger organisations.

70%

It's assessed that up to 70% of cloud security incidents will stem from misconfigurations. [Google Cloud]

60%

Is assessed to be the number of cloud security incidents which will results from compromised identities in cloud environments. [Google Cloud]

2025

Increased Cyber warfare

Nation-states are likely to engage in more aggressive cyber warfare tactics, targeting critical infrastructure and government systems to disrupt services and gather intelligence.

AI-enhanced attacks

AI is likely to become more sophisticated, enabling more precise and damaging operations, including AI-driven malware and automated phishing campaigns.

Geopolitical Tensions

Ongoing geopolitical tensions, particularly between major powers like the US, Russia and China are highly likely to drive an increase in state-sponsored cyber activities aimed at espionage and disruption.

Supply-Chain vulns

Supply chain attacks are highly likely to continue to be a significant threat, with nation-state actors and cybercriminals targeting third-party vendors to gain access to large networks.

Supply Chain Attacks

2024

Increased Frequency

The number of supply chain attacks doubled compared to previous years, highlighting the growing complexity and interconnectedness of global supply chains.

High-profile Attacks

Several high-profile incidents occurred, such as the Synnovis attack, from the Russian group Quiilin, targeting the NHS.

Critical Infrastructure

Attackers increasingly targeted critical infrastructure, including healthcare, financial institutions and the government, to cause widespread disruption and gain geopolitical leverage.

Third-party Risks

The use of third=party services and applications introduced additional vulnerabilities, requiring o data transparency and security from vendors.

30%

Supply chain attacks are expected to rise by 30% year-over-year, driven by the increasing complexity and interconnectedness of global supply chains. [Gartner]

RaaS

The prevalence of RaaS is predicted to grow, leading to more frequent and sophisticated ransomware attacks targeting supply chain. [ZScaler]

2025

AI-powered attacks

It is likely cybercriminals will leverage AI to conduct more sophisticated supply chain attacks, to identify vulnerabilities and automate the attack process, making detection more difficult.

Cloud compromise

As mor organisations move to cloud attackers will increasingly target cloud infrastructure. Misconfigurations and vulnerabilities are likely to provide a focus, whilst IOT devices will provide new attack methods and weak security.

RaaS

Ransomware-as-a-Service is likely to continue growing, with more cybercriminals offering their ransomware to other attackers, increasing the number of ransomware attacks targeting supply chains.

Regulatory Scrutiny

Governments and regulatory bodies are almost certain to impose stricter cybersecurity regulations on supply chains, requiring organisations to implement more robust security measures.

Social Engineering

2024

AI-driven Phishing

AI driven phishing attacks were prominent, with criminals creating longer, more convincing phishing emails, which were difficult to distinguish from legitimate communications.

Deepfake Tech

Deepfake technology in social engineering attacks increased, with attackers creating realistic video and audio impersonations of high-profile individuals to deceive and manipulate targets.

Image-based phishing

There was a significant rise in image-based phishing attacks, with attackers using images o bypass traditional text-based detection methods, including using QR codes.

Exploiting legitimate services

Cybercriminals increasingly exploited legitimate services, such as file-sharing platforms and e-signature solutions, to enhance phishing attacks and make distinguishing harder.

8.4/1000

The success rate of phishing attacks is predicted to increase, with 8.4 out of every 1,000 users clicking on phishing links per month, nearly triple the average from previous years. [Netskope]

25%

Increase in BEC attacks likely, with attackers using social engineering tactics to trick employees into transferring funds or revealing sensitive information. [Netskope]

2025

AI-enhanced phishing

Attackers are almost certain to continue using AI to create highly personalised and convincing emails, increasing the challenge of identifying malicious communications.

Deepfake tech

The use of deepfake tech will continue to rise, with attackers creating realistic video and audio impersonations to deceive and manipulate targets.

Multi-channel attacks

Social engineering will use multiple channels (email, text, phone) to build trust and create believable scenarios making their attacks more effective.

Synthetic identities

Attackers will use AI to create synthetic identities, combining real and fake information to impersonate individuals and gain unauthorised access.

IOT and Edge devices

2024

AI/ML Integration

The synergy between IoT devices and AI/ML technologies deepened, enabling more efficient and autonomous systems. Machine learning algorithms embedded in IoT devices allowed for local data analysis and decision-making

Edge computing

Edge computing became more prominent, addressing the limitations of traditional cloud computing by processing data closer to the source, reducing latency, optimising bandwidth usage, and enhancing security.

Security Challenges

As the number of connected devices grew, so did the security challenges. Ensuring the security of IoT and edge devices remained a critical concern, with a focus on protecting data and preventing unauthorised access.

Industry apps

IoT and edge devices continued to transform various industries, including healthcare & manufacturing, These tech enabled more efficient processes, such as predictive maintenance, energy management, and automation

75 bn

By 2025, its predicted there will be over 75 billion connected IOT devices worldwide driven by advances in technology and increased adoption across various industries. [Toxigon]

$1.6trn

The global IoT market is projected to reach $1.6 trillion by 2025, with significant investments in smart cities, industrial IoT, and healthcare. [Review42]

2025

AI-enhanced IOT

The integration of AI with IoT devices will enable more intelligent and autonomous systems. This includes predictive maintenance, personalised customer experiences, and automated quality assurance

Sustainable IOT

Emphasis on sustainable IoT solutions and developing energy-efficient IOT devices will help reduce the carbon footprint of various industries through better energy management and waste reduction.

IOT- Focussed MVNOs

Mobile Virtual Network Operators (MVNOs) will offer tailored IoT solutions, such as e-SIMs for niche markets, providing more flexible and cost-effective connectivity options.

Cybersecurity in IOT

As the number of connected devices grows, so will the focus on securing IoT ecosystems. Organizations will invest in robust security protocols and compliance measures to protect against evolving threats.

BYTES