Cybersecurity Trends & Predictions 2025

CERT-MU

April 2025

Contents

Introduction

The cybersecurity landscape continues to evolve at an unprecedented pace, marked by both the sophistication of threats and the expanding attack surface driven by digital transformation. In 2024, the world witnessed a surge in cyber-attacks that not only disrupted organisations but also impacted individuals, governments, and critical infrastructures on an unprecedented scale. These incidents revealed significant vulnerabilities across sectors, from healthcare and finance to energy and technology, with malicious actors exploiting weaknesses in both legacy systems and cutting-edge innovations. The increasing reliance on interconnected systems, coupled with the rapid evolution of attack methods, has made cybersecurity a top priority for stakeholders worldwide.

Among the defining trends of 2024 were the rise in sophisticated ransomware operations, the expansion of supply chain attacks, and an alarming increase in critical infrastructure breaches. Cybercriminal groups and state-sponsored actors demonstrated heightened capabilities, leveraging automation, artificial intelligence, and zero-day vulnerabilities to target victims with greater precision and impact. High-profile incidents, such as breaches of cloud-based platforms and data exfiltration from global enterprises, served as stark reminders of the persistent threats that accompany digital transformation.

From the region's perspective, African countries are no exception. Cyberthreats have become one of the most serious challenges facing governments and organisations. A report by Positive Technologies reveal that during the Q1 2023–Q3 2024 period, the region faced numerous cyberthreats, including attacks on critical infrastructure, data breaches, and online fraud. According to data from open sources, a significant portion of cyberattacks in the region occurred in South Africa (22%) and Egypt (13%), while dark web listings frequently concerned the targets in South Africa (25%), Nigeria (18%),

and Algeria (13%). Additionally, Africa's rich natural resources are driving industrial growth in the region, which is another motivation for cybercriminal interest.

On the local front, Mauritius has made significant strides in strengthening its cyber resilience through several initiatives. However, 2024 highlighted recurrent threats, including online harassment, scams and frauds, phishing and social media-based incidents. As Mauritius continues to position itself as a technology and innovation hub, its increasing reliance on digital platforms has expanded the attack surface, making cybersecurity a critical national priority.

As we enter 2025, the landscape is set to evolve further, with emerging technologies like artificial intelligence, blockchain, and quantum computing influencing both attack vectors and defense mechanisms. Geopolitical dynamics, regulatory shifts, and the increasing adoption of hybrid work environments are expected to further shape the threat environment.

This report provides a comprehensive overview of the biggest cyberattacks of 2024, analysing their techniques, consequences, and lessons learned. It also offers insights into key cybersecurity trends for 2025, highlighting areas that demand attention from organizations aiming to fortify their defenses. By examining the past and forecasting the future, this report seeks to empower readers with the knowledge needed to navigate the complexities of an ever-changing cyber threat landscape.

2024: The Notable Cyber Attacks

The year 2024 was marked by a surge in cyber threats that underscored the growing sophistication and scale of malicious activities worldwide. High-profile ransomware attacks targeted critical infrastructure, healthcare systems, and large enterprises, disrupting operations and causing significant financial and reputational damage. Let us reflect on the most significant cyberattacks, threats, and data breaches that occurred in 2024:

Namibia Telecom Ransomware Attack

In December 2024, Namibia's state-owned telecom provider was victim to a ransomware attack and some of its customers' data was leaked on the dark web. Telecom Namibia attributed the attack to a threat actor known as Hunters International. According to the company's chief executive, Stanley Shanapinda, the hackers made the stolen data public after Telecom Namibia had refused to negotiate with them about the potential ransom.

As per news sources, the hackers accessed over 400,000 files, including personal and financial data belonging to some high-ranking government officials and Telecom Namibia's clients.

City of Columbus Ransomware Attack

In July 2024, the City of Columbus, Ohio became victim to a ransomware attack, resulting in outages to some resident-facing IT services. After failed negotiations with the city, the perpetrators, the Rhysida ransomware group, allegedly posted 3.1 TB of personal and other sensitive data exfiltrated by the attackers. In November, City officials notified 500,000 residents that their personal data may have been compromised by the attackers. With Columbus' population 915,000, the breach could affect approximately 55% of residents. The attackers reportedly accessed highly sensitive data, such as Social Security numbers, bank account details and driver's license information. This exposure is believed one of the most significant public sector data breaches in recent history.

Transport for London cyber-attack exposes customer data in major breach

In September 2024, a cyber-attack on Transport for London (TfL), saw attackers breach systems and access sensitive customer data. The compromised information included Oyster refund data, bank account numbers, sort codes, and personal contact details for around 5,000 customers. TfL responded by suspending certain services, such as applications for Oyster photocards and Zip cards, to prevent further unauthorized access. The National Crime Agency arrested a 17-year-old suspect in connection with

the attack. This incident underscores the escalating threats facing public infrastructure and the importance of robust cyber security measures.

Seattle Airport cyber attack

In August 2024, the Port of Seattle, a local government agency overseeing the seaport of Seattle and Seattle–Tacoma International Airport became victim to a cyber-attack. This attack disrupted travel and also led to significant delays to the check-in process at the SEA, with Wi-Fi unavailable and display screens not working. In an update, the Port of Seattle confirmed the incident was caused by a ransomware attack by the Rhysida gang. The attackers were able to access parts of the ports computer systems and encrypt access to some data.

The majority of systems were brought back online within a week, enabling passenger travel to resume as normal. The Port of Seattle and SEA website was fully restored in November 2024.

CrowdStrike outage

The CrowdStrike outage which occurred in July 2024 is described as one of the worst cyber incidents in history, whereby over 8.5 million computers around the world were hit. CrowdStrike, a leading cybersecurity company, experienced a significant outage that disrupted its Falcon platform, widely relied upon for endpoint protection and threat detection. The incident, attributed to a database configuration issue during routine maintenance, caused service interruptions that impacted numerous customers globally. The outage raised concerns about the resilience of cloud-based cybersecurity solutions and the potential cascading effects on organizations that depend on these services for real-time threat monitoring. While CrowdStrike swiftly addressed the issue and restored operations, the event highlighted the critical need for robust failover mechanisms, transparency during incidents, and continuous monitoring of cloud-based infrastructures to ensure service reliability and maintain customer trust.

CDK Global Ransomware Attack

In June 2024, CDK Global, a leading US-based software provider for the automotive industry, suffered a significant ransomware attack. First reported on 18 June, the incident began when an employee inadvertently downloaded malware, leading to the encryption of critical files and systems. The BlackSuit ransomware gang, linked to Eastern Europe and Russia, claimed responsibility, demanding a ransom that escalated from $10 million to over $50 million.

The attack forced CDK Global to shut down its IT systems, affecting nearly 15,000 car dealer locations across North America. This disruption cost dealerships more than $1 billion collectively and impacted automakers like BMW, Nissan, and Honda. Customers faced delays in purchasing vehicles and scheduling services as dealerships resorted to manual processes.

NHS Ransomware Attack

In June 2024, a ransomware attack on a critical supplier of pathology services to UK NHS hospitals, Synnovis, resulted in thousands of operations and appointments being cancelled. The incident significantly impacted the delivery of vital healthcare services at King's College Hospital NHS Foundation Trust and Guy's and St Thomas' NHS Foundation Trust, such as blood transfusions and test results, over several months.

The attack was claimed by ransomware gang Qilin, which reportedly published 400GB of data stolen from Synnovis on June 20. The data stolen by the attackers included patient names, NHS numbers and descriptions of blood tests. that has been impacted.

Snowflake Data Breach

In June 2024, the cloud storage provider Snowflake faced a spate of cyberattacks that targeted customer accounts, exploiting stolen login credentials to access sensitive data. Notably, high-profile clients such as Ticketmaster and Santander were impacted, with attackers accessing data and demanding a hefty ransom.

The breach did not involve a direct compromise of Snowflake's infrastructure. Instead, attackers obtained customer credentials through infostealer malware, enabling them to bypass standard security measures such as multi-factor authentication in some cases. Snowflake has consistently denied any inherent flaws in its own systems, attributing the breach to widespread credential-stuffing attacks on customer accounts. The company has responded by enhancing security protocols and sharing guidance to help customers strengthen their defences

Ticketmaster Breach

In June 2024, Ticketmaster faced major scrutiny when its parent company, Live Nation, confirmed a massive data breach. Hackers known as ShinyHunters claimed they had stolen the personal information of 560 million customers and demanded a $500,000 ransom to prevent the sale of this data on the dark web. The stolen information included names, addresses, email addresses, usernames, and partial credit card details, leaving many customers vulnerable.

UK military Data Breach

In May 2024, hackers infiltrated the UK Ministry of Defence's payroll system, exposing sensitive personal information of 270,000 current and former military personnel. The breach included names, bank details, and other private data. As the Ministry of Defence, the data breach affected UK military personnel through a third-party payroll system, compromising names, bank details, and some addresses.

Dell Data Breach

In May 2024, Dell warned customers about a significant data breach after a threat actor claimed to have stolen information on approximately 49 million individuals. Dell began sending out notifications, confirming that a portal containing customer data related to purchases had been compromised. Dell's statement at the time revealed that the

exposed data included customer names, physical addresses, order service tags, item descriptions, order dates, and warranty information.

Ascension Health System Ransomware Attack

In May, Ascension - a non-profit health system with 140 hospitals operating across 19 states and Washington, D.C announced that its clinical operations were disrupted due to a ransomware attack. On 8 May, the organisation detected unusual activity on select technology network systems, signalling a security breach. The attack began when an employee inadvertently downloaded malware, which subsequently forced Ascension to divert emergency care from some of its hospitals, impacting patient services.

Sensitive data, including patients' health information, was likely stolen during the attack. This incident underscores the critical importance of robust cybersecurity measures in healthcare settings, where breaches can have severe consequences for patient care and data privacy. The attack on Ascension highlights the vulnerabilities that can arise from human error and the need for continuous staff training in cybersecurity protocols.

USA - Change Healthcare Cyber Attack

First disclosed on 22 February, the cyber-attack on Change Healthcare caused massive disruption in the US healthcare system for weeks. In response to the ransomware attack, an IT system shutdown was initiated, preventing many pharmacies, hospitals, and other healthcare facilities from processing claims and receiving payments. The Russian-speaking cybercriminal group known as BlackCat or ALPHV claimed responsibility. UnitedHealth Group CEO Andrew Witty confirmed in his Congressional testimony in May that the company paid a $22 million ransom following the attack. In June, Change Healthcare disclosed that sensitive patient medical data was exposed, potentially including diagnoses, medicines, test results, images, care, and the treatment.

Attack on Microsoft Corporate Systems

In January 2024, Microsoft detected a nation-state attack on its corporate systems, immediately initiating a response to investigate and mitigate the breach. The Microsoft Threat Intelligence investigation identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as NOBELIUM. The attackers used techniques like password-spray attacks and OAuth application exploitation to gain unauthorized access to sensitive corporate data, including internal email. This incident underscores the importance of balancing security with business risk. Using audit logs, Microsoft tracked the attackers' activity through Exchange Web Services (EWS), and began notifying other affected organisations. The incident remains under investigation, with ongoing analysis of Midnight Blizzard's tactics to better protect and respond to similar threats in the future.

Russian Space Research Center Data Breach

The Russia/Ukraine war continues to rage on with cyber-attacks being launched by both sides. Back in January 2024, the Main Intelligence Directorate of Ukraine's Ministry of Defence reported that pro-Ukrainian hacktivists breached the Russian Centre for Space Hydrometeorology, known as "Planeta", wiping out 2 petabytes of data. Planeta, a state research centre, uses satellite and ground data to predict weather, monitor natural disasters, and provide climate insights. Affiliated with Roscosmos, it supports sectors like the military, civil aviation, and agriculture. Ukrainian officials stated that cyber volunteers from the "BO Team" targeted Planeta's Far Eastern branch, the largest of its three locations. They allegedly destroyed 280 servers containing 2 petabytes (2,000 terabytes) of data.

The Ukrainian intelligence service estimated the damage at $10 million, impacting supercomputer clusters and years of research. Given sanctions on Russia, restoring sophisticated computer systems would have proven difficult, posing a significant challenge to Planeta’s operations.

Ivanti VPN Zero-Day Vulnerability

Ivanti's widely used Connect Secure VPNs experienced mass exploitation by threat actors following the January disclosure of two high-severity, zero-day vulnerabilities. Researchers reported that thousands of Ivanti VPN devices were compromised, with victims including the U.S. Cyber security and Infrastructure Security Agency (CISA) and Mitre, a significant provider of federally funded research and development. While additional vulnerabilities were later identified, Mandiant, a Google Cloud-owned cyber security firm, noted that the two original vulnerabilities saw extensive exploitation by a China-linked threat group known as UNC5221 and other unidentified groups. Mandiant's research indicated that attacks by UNC5221 dated back to December 3.

In response to the widespread attacks, CISA issued an urgent directive requiring civilian executive branch agencies to disconnect their Ivanti Connect Secure VPNs within 48 hours. On January 31, Ivanti released the first patch for some versions of its VPN software, three weeks after the initial vulnerability disclosure. The company stated that they prioritised mitigation releases as patches were being developed, consistent with industry best practices.

The Most Dominant Cyber Threats of 2024: Global Perspective

The year 2024 saw a significant escalation in cyber threats, with attackers employing increasingly sophisticated tactics to target critical infrastructure, businesses, and individuals. Ransomware attacks and supply chain breaches were particularly dominant causing widespread operational and financial disruptions. The integration of artificial intelligence by cybercriminals further amplified the scale and precision of attacks, challenging traditional defense mechanisms. Geopolitical tensions also fueled state-sponsored cyber activities, highlighting the interconnected nature of global cybersecurity risks. These events underscored the urgent need for stronger defenses, greater collaboration, and a proactive approach to safeguarding digital ecosystems.

Based on the findings of different cybersecurity research, the most dominating threats that we have seen in 2024 are described below:

1. Ransomware

Ransomware continued to dominate the cyber threat landscape in 2024, with attacks becoming more sophisticated, targeted, and costly. Cybercriminal groups leveraged advanced encryption techniques, double and triple extortion methods, and automation to maximize their impact and profits. Critical sectors such as healthcare, finance, and energy were frequent targets, with some attacks causing severe disruptions to essential services.

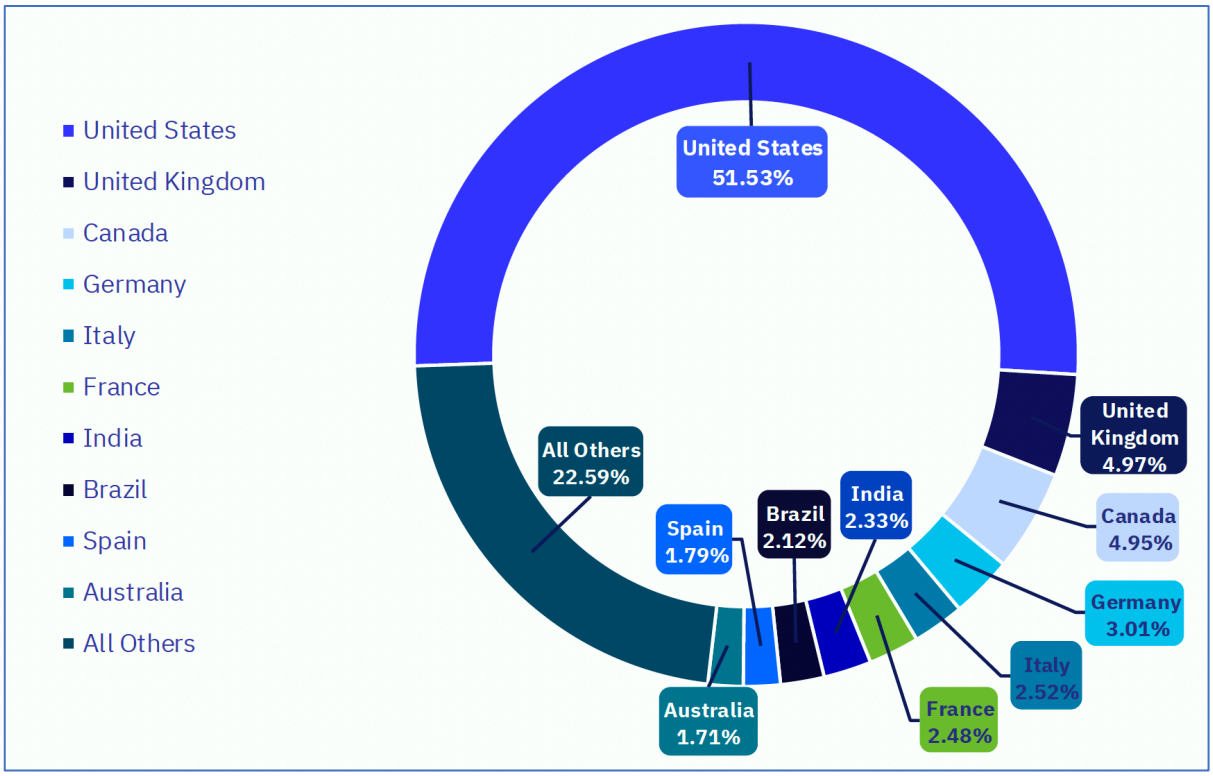
Moreover, the rise of ransomware-as-a-service (RaaS) further lowered the barrier to entry for aspiring attackers, leading to a proliferation of incidents worldwide. Geopolitical tensions also contributed to the use of ransomware as a tool for sabotage and espionage. Despite increased efforts from law enforcement and advancements in defensive technologies, many organizations struggled to keep pace with the evolving tactics, underscoring the urgent need for enhanced prevention, rapid response strategies, and greater international cooperation to combat the ransomware epidemic.

The below statistics have been gathered to demonstrate the state of ransomware in 2024:

- **Most Impacted Country** - As shown in figure 1 below, the United States remained the country most impacted by ransomware by several orders of magnitude, accounting for 51.53% of all observed ransomware attacks in 2024, a marginal increase of 1.5% from 2023. It continues to be the most impacted country regarding the number of raw ransomware victims claimed by threat groups.

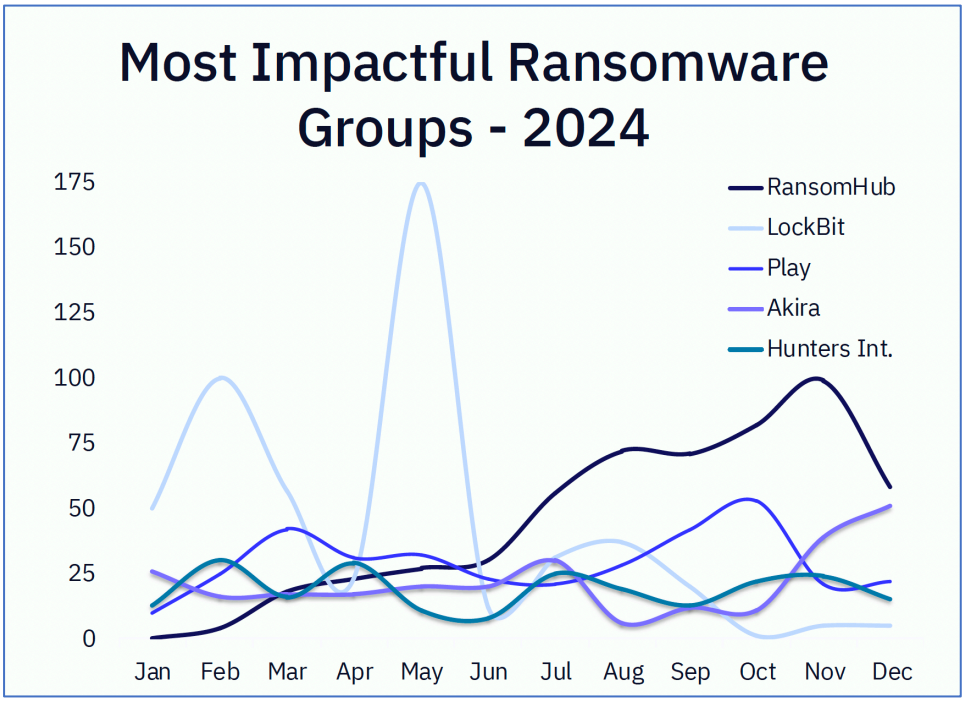
- Brazil and India experienced increased ransomware attacks from 2023 to 2024, rising 56.06% and 46.75% respectively. In both cases, groups such as LockBit and RansomHub were among the most impactful groups in terms of victim

volume.



Source: GRIT 2025 Ransomware & Cyber Threat Report

- **The most impacted ransomware group** - RansomHub has steadily increased their activities since their first posts in February 2024 to become the most active group during the year's second half. RansomHub was not alone in claiming an uptick of activity in H2 2024, with other Ransomware groups such as Akira and Play demonstrating similar growth.



Source: GRIT 2025 Ransomware & Cyber Threat Report

- **Most Impacted sector** - Manufacturing remained the industry most frequently impacted by ransomware groups in 2024, with 67% of the distinct ransomware groups having claiming at least one victim within the industry over the course of the year.

2. Malware

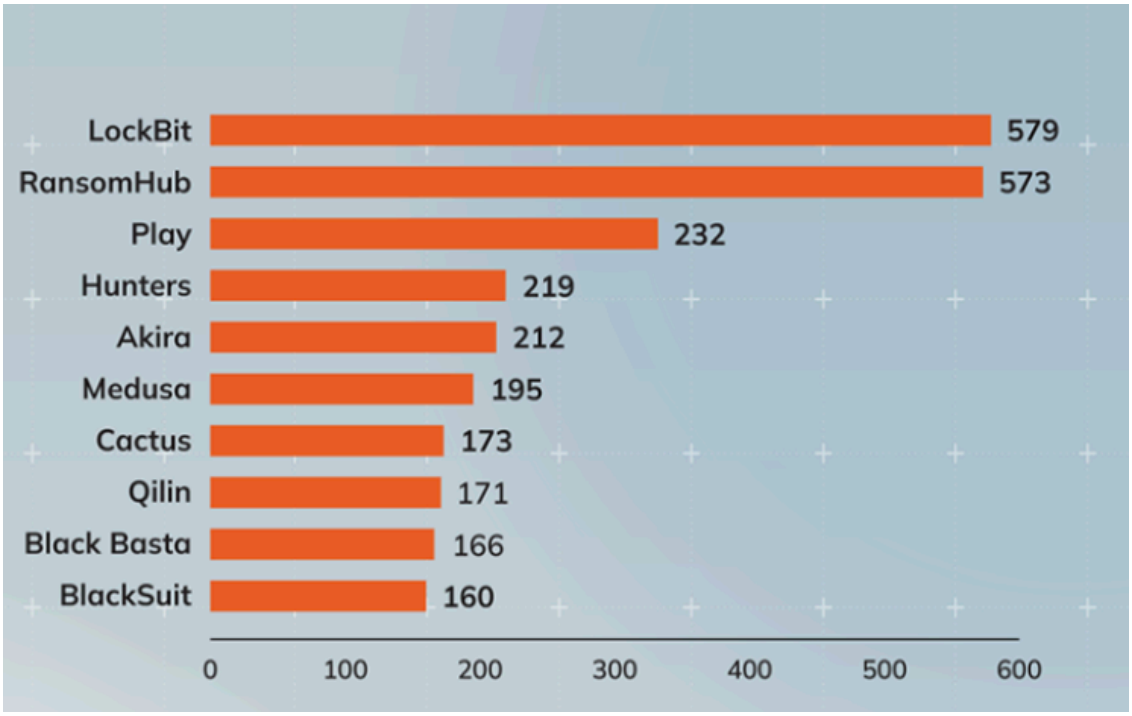
The year 2024 witnessed an increase in the number of malware incidents, characterized by the emergence of new threats and the evolution of attack methodologies. Data from Kaspersky's detection systems revealed an average of 467,000 malicious files that were detected in 2024, representing a 14% increase compared to the previous year. Notably, there was a 33% surge in Trojan detections, underscoring the heightened threat landscape.

Analysis from ANY.RUN highlighted that the malware type “stealers” were the most prevalent malware type in 2024, with 51,291 detections, a substantial rise from 18,290 in 2023. The malware type “loaders” followed with 28,754 detections, and 'Remote

Access Trojans (RATs)' accounted for 24,430 detections. This trend indicates a growing emphasis on data theft and unauthorized system access by cybercriminals. Moreover, the "Lumma Stealer" also emerged as a significant threat, with 12,655 detections in 2024. Other prominent malware families included "Agent Tesla" with 8,443 detections and "AsyncRAT" with 8,257 detections, reflecting their widespread adoption among threat actors.

3. Ransomware

In 2024, ransomware attacks continued to pose a significant threat to organisations worldwide, with notable shifts in attack patterns, financial impacts, and the emergence of new threat actors. There was also the emergence of new ransomware groups and the rebranding of existing ones. As per the statistics of Rapid7, between January and December 2024, 33 new or rebranded threat actors were identified, contributing to a total of 75 active groups. Collectively, these groups were responsible for 5,477 data leak site posts. Moreover, the RansomHub group became prominent in the latter half of the year, claiming 500 victim organizations and surpassing previous leaders like LockBit.



Source: Rapid7 Labs

4. Vulnerabilities in Systems and Applications

In 2024, the cybersecurity landscape experienced a notable increase in vulnerabilities found in systems and applications. According to the SecPod's 2024 Annual Vulnerability Report, around 40,704 vulnerabilities were identified in 2024, which represents a 30% increase compared to the previous year. The report also revealed the following statistics:

- Critical and high-severity vulnerabilities: 19,100, according to CVSS v3 and v4 algorithms
- Zero-day vulnerabilities: 31
- Malware-exploited vulnerabilities: 120, leading to high-fidelity attacks
- Widely exploited vulnerabilities: 129

The report also highlighted that Linux and Microsoft are the top affected vendors, with 2,315 and 1,205 vulnerabilities, respectively. Moreover, Linux was the most affected operating system, with 2,313 vulnerabilities detected, followed by macOS and Windows. The expansive ecosystem of applications and hardware also saw critical vulnerabilities, with Adobe Experience Manager leading the pack among applications and Tenda and Qualcomm dominating the hardware segment.

The Cybersecurity and Infrastructure Security Agency (CISA) and MITRE Security Report also highlighted some of the most critical software weaknesses for 2024 in a top 25 list. These vulnerabilities are ranked not only based on their prevalence but also their potential impact. The top 5 vulnerabilities from the list are as follows:

a) Cross-site scripting (XSS)

XSS Vulnerabilities arise when web applications do not adequately sanitize user inputs before including them in a web page. This deficiency enables attackers to inject

harmful scripts into a user's browser, which can result in stolen credentials, hijacked sessions, or the delivery of malicious payloads.

b) Out-of-bounds Write

Out-of-bounds write vulnerabilities emerge when a program writes data beyond the limits of allocated memory space. This critical flaw can trigger unexpected consequences like crashes, data corruption, or even the execution of malicious code.

c) Improper Neutralisation of Special Elements used in an SQL Command (SQL Injection)

SQL injection vulnerabilities occur when attackers manipulate input fields to execute unauthorized SQL queries. By taking advantage of applications that don't adequately sanitize user inputs, they can access databases, retrieve sensitive information, or perform administrative operations.

Some of the actively exploited SQL Injection vulnerabilities in 2024 are:

- CVE-2023-48788: Discovered in Fortinet FortiClient EMS, this vulnerability allowed attackers without authentication to run system-level commands through specially crafted requests. During the Connect: fun campaign, media companies were targeted, and attackers used this flaw to penetrate networks.

- CVE-2024-6670: In Progress WhatsUp Gold, attackers exploited this vulnerability to retrieve encrypted user passwords. They managed to achieve Remote Code Execution (RCE) by manipulating the Active Monitor PowerShell Script.

- CVE-2024-9379 and CVE-2024-29824: These vulnerabilities were present in Ivanti products. Exploited by a nation-state actor in chain attacks, they facilitated lateral movement within networks.

- CVE-2024-9465: In Palo Alto Networks Expedition, this flaw allowed attackers to access sensitive database contents, such as password hashes, usernames, and device configurations.

d) Cross-Site Request Forgery (CSRF)

This type of attack takes advantage of the trust between a user and a web application, allowing unauthorized actions like altering account settings or making monetary transfers. Notably, in 2024, **CWE-352** climbed five positions to take the fourth spot on the Top 25 list, highlighting the increasing concern surrounding this significant web threat.

An example of a notable CSRF vulnerability of 2024 was CVE-2014-100005. This outdated flaw in D-Link DIR-600 routers lets attackers take over administrator sessions and modify router settings. Despite its age, it still impacts devices that have reached their end-of-life phase and should be decommissioned or replaced following vendor recommendations.

e) Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Improper validation of user input in applications can open the door to path traversal vulnerabilities. This occurs when attackers alter file paths to access files and directories outside the permitted scope. When exploited, this flaw can lead to unauthorized access to sensitive data, data exposure, or even execution of malicious code. In 2024, this vulnerability climbed three positions, securing the fifth place in the Top 25 list, emphasizing the persistent threat of poorly managed file paths. Some of the most exploited path traversal vulnerabilities of 2024 are:

- CVE-2024-11667: A vulnerability in Zyxel firewalls allows the download or upload of files through manipulated URLs. Attackers leveraged this flaw in Helldown ransomware campaigns.

- CVE-2021-26086: Detected in Atlassian Jira Server and Data Center, this vulnerability lets attackers read restricted files, including those at the /WEB-INF/web.xml endpoint.

- CVE-2024-8963: Affecting Ivanti Cloud Services Appliance (CSA), this issue can be exploited to bypass admin authentication and execute arbitrary commands, especially when paired with other vulnerabilities like CVE-2024-8190.

- CVE-2024-32113: Found in Apache OFBiz, it exposes systems to remote code execution through poor file path validation.

- CVE-2024-28995: In SolarWinds Serv-U, this vulnerability enables attackers to access sensitive files on the host system through path traversal.

5. Mobile Devices Security Risks

The mobile threat landscape has evolved significantly in 2024, with cybercriminals employing advanced tactics to exploit vulnerabilities in mobile devices and applications. Many organisations, especially CIIs have integrated mobile devices and into their daily operations. Widespread bring-your-own-device (BYOD) policies have led to corporate, sensitive or regulated data being stored on or passing through mobile devices.

Since mobile devices are easy to carry, they are also easy to steal. Therefore, if a mobile device has high-value data stored on it, a breach can result in the immediate loss or theft of that data, especially if the device's lock screen is disabled or it does not have remote deletion capabilities. It is especially worrisome that attackers who compromise a mobile device frequently use the infected device to gain access to company networks. This can result in largescale data exfiltration, the spread of ransomware, customer and employee privacy violations and costly operational downtime.

A survey carried out by Verizon in 2024 revealed the following statistics on mobile devices security:

53%
of respondents experienced an organisational security incident involving a mobile or IoT device that resulted in data loss or downtime.

47%
of respondents report that such compromises had major impacts on their organisations.

25%
of organisations have at least one mobile device user on staff who has disabled their lock screen feature, even though only 3% of all devices have the lock screen disabled.

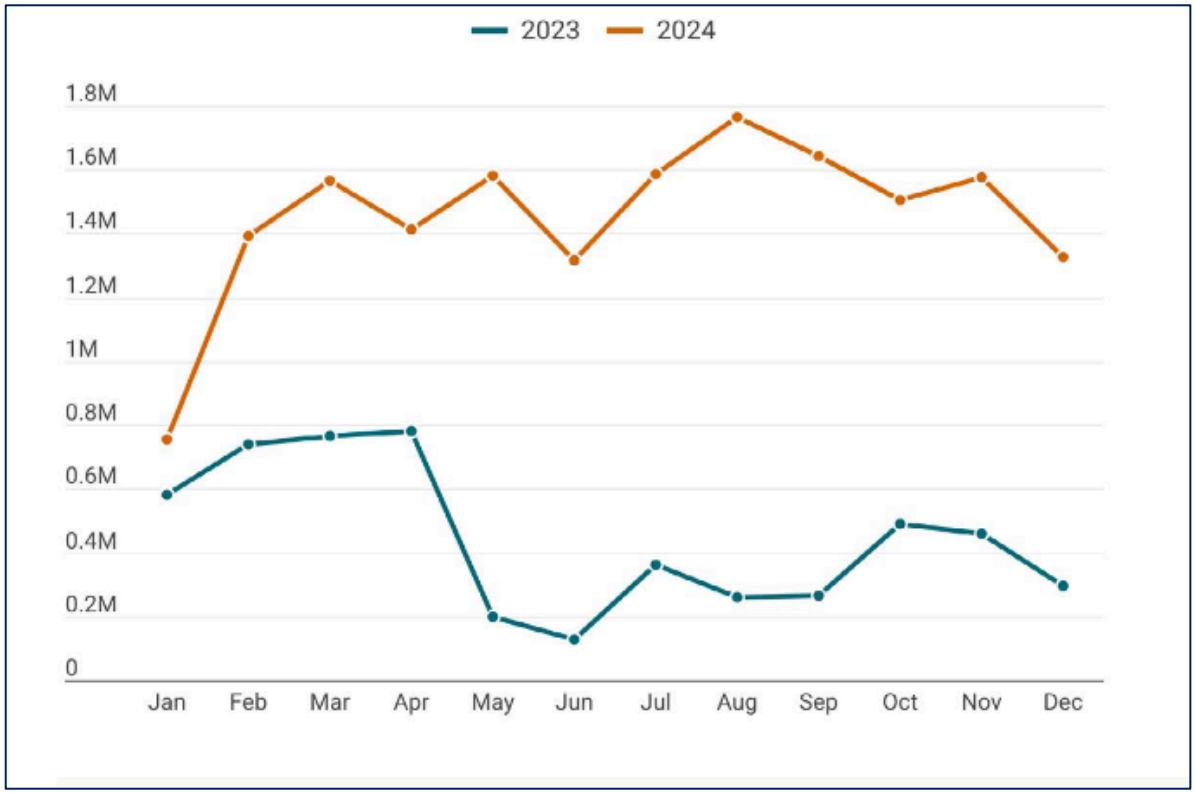
Sources: The Verizon's 2024 Mobile Index Report 2024

6. Internet of Things (IoT) Vulnerabilities

IoT devices are more and more connected to mobile networks. In 2024, IoT deployments in mobile has increased significantly. As per IoT statistics, there were 16.6 billion IoT devices at the end of 2023, and reached around 18.8 billion by the end of 2024.

As per the 2024 SonicWall Cyber Threat Report, the firm prevented more than 17 million attacks on IP cameras, ranging from 750,000 to 1.8 million attacks each month. Attackers are beginning to take note of the often-weak defenses of connected devices – specifically those used in government and critical infrastructure. These devices are left vulnerable to disruptive activities such as surveillance manipulation and Distributed Denial of Service (DDoS) attacks. IP cameras are often found in sensitive locations like government facilities and even polling locations, meaning the increase seen could have been at least partially attributed to the global 2024 elections. One of the most alarming IoT threat leveraged is the Hikvision IP Camera Command Injection (CVE-2021-36260) vulnerability, which allows threat actors to enter commands directly into

the camera's systems, allowing them to take full control of the device.



Source: 2024 SonicWall Cyber Threat Report

7. 5G Network Security Issues

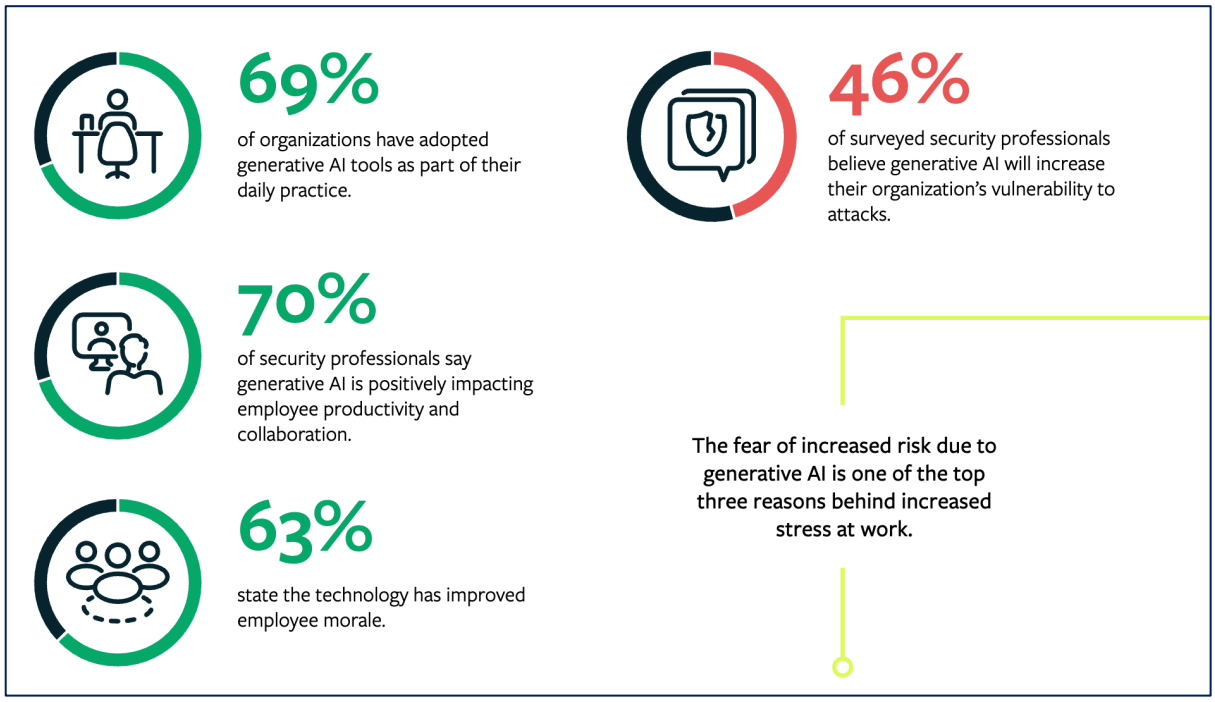
Private 5G networks are booming due to their use across critical industries including energy and utilities, military, logistics, healthcare, and smart manufacturing. According to a survey conducted by Trend Micro, 100% of respondents revealed they are either currently using them (86%) or evaluating their deployment (14%). The rapid deployment of 5G networks has however, introduced significant security challenges, primarily due to an expanded attack surface and increased device connectivity. As per Grand View Research, the global 5G security market was valued at approximately $3.63 billion in 2024, reflecting heightened concerns over vulnerabilities within these advanced networks. A notable incident which occurred involved Chinese hackers infiltrating U.S. telecommunications networks, compromising vast amounts of sensitive call data - a breach exacerbated by the extensive data capabilities inherent to 5G technology. Moreover, a research carried out jointly by Trend Micro and CTOne

revealed that a lack of communications technology (CT) expertise could expose private 5G networks to compromise, despite the widespread adoption of AI security tools.

8. The Rise of AI Powered Cyber Attacks

Artificial intelligence (AI) is transforming the cybersecurity world at a rapid pace. By using AI, organizations today can enhance their productivity and output. However, the world is also seeing a new and unsettling reality at the same time – the rise of AI powered attacks. With rising concerns over China's DeepSeek and its massive capabilities, the risk of AI-powered cyberattacks has never been greater. Cybercriminals are using AI and machine learning to enhance and automate their illegal activities. This majorly includes identifying vulnerabilities, designing attack paths and deploying campaigns, deceiving users with deepfakes, automated and repetitive attacks, and disrupting system operations. Furthermore, generative AI tools like FraudGPT and Worm GPT, provide a range of resources to conduct a cyberattack, making it more accessible and affordable for cybercriminals.

A survey carried out by Deep Instinct revealed the following:



Source: Deep Instinct Fourth Edition Report

Moreover, deep fake attacks have increased from 50% to 60% in 2024, with 140,000 to 150,000 global incidents, as per VPNRanks. These statistics highlight the growing sophistication of cyber threats as adversaries increasingly leverage AI technologies to enhance the scale and effectiveness of their attacks.

9. Cloud Security

The adoption of cloud infrastructure continues to increase. With businesses increasingly reliant on cloud technologies, the security of cloud platforms has escalated into a significant concern that highlights their potential and susceptibility. Traditional security measures often fall short in addressing the dynamic and sophisticated nature of threats faced in cloud settings, making it imperative to shift from a reactive to a preventative stance in security strategies.

10. Supply Chain Attacks

Over the past years, the software supply chain has become a primary attack vector for malicious actors. What was once a relatively niche method of attack has evolved into one of the most significant cybersecurity threats today, driven by the interconnectedness of modern software ecosystems and the increasing reliance on open source components. As software supply chains have grown in complexity, so too have the strategies employed by attackers, who have shifted their focus from directly targeting organizations to exploiting vulnerabilities within the broader supply chain and all of its downstream consumers.

In 2024, one of the most significant incidents around supply chain was the XZ-Utils Project. This incident could potentially become the most dangerous supply-chain attack of 2024 with devastating consequences. As part of a sophisticated operation lasting two-and-a-half years, a GitHub user known as Jia Tan managed to gain control over the XZ Utils project, which is a set of compression utilities included in many popular Linux distributions. With the project under his control, Jia Tan published two

versions of the package (5.6.0 and 5.6.1), both containing the backdoor. As a result, the compromised liblzma library was included in test versions of several Linux distributions. According to Igor Kuznetsov, head of Kaspersky's Global Research & Analysis Team (GReAT), the CVE-2024-3094 vulnerability could have become the biggest ever attack on the Linux ecosystem. Had the vulnerability been introduced into stable distributions, we might have seen massive server compromises. Fortunately, CVE-2024-3094 was detected in test and rolling-release distributions, so most Linux users remained safe.

11. Social Engineering Attacks

In the cybersecurity world, the biggest threat is not always a system bug or a rogue piece of code. It is something much harder to remediate, that is the human element. Unlike traditional cyber threats that seek to exploit system vulnerabilities, social engineering attacks bypass technical defenses by manipulating people into revealing confidential information or making security mistakes. Some of the most common types of social engineering attacks are phishing, vishing, smishing, CEO fraud, business email compromise, amongst others. In 2024, social engineering attacks remains a predominant threat in the cybersecurity landscape. Some of the statistics related to social engineering attacks are:

- 94% of businesses are reported to have experienced a phishing attack in 2024, with most of them experiencing negative impacts from these attacks. (Source: Egress)
- Business Email Compromise (BEC) accounts for 24-25% of financially motivated attacks. (Source: Verizon)
- 89% of social engineering attacks were motivated by financial gain, 11% by espionage (Source: Verizon).
- The average cost of a social engineering attack reached $130,000, reflecting the substantial financial impact on organizations (Source: Secureframe).

2024: The Cyber Threat Landscape in Figures

Below are some of the statistics of how cyber threats evolved in 2024:

Ransomware Payment
2024 saw the largest ransomware payment ever recorded — approximately $75 million paid to the Dark Angels ransomware group[1].

Data Breach
The average cost of a data breach reached an all-time high in 2024 of $4.88 million, a 10% increase from 2023. [2]

Ransomware Attack
59% of organizations globally experienced a ransomware attack in 2024.[1]

Social Engineering
68% of data breaches in 2024 were attributed to human error, including social engineering scams. [3]

Human Element
More than 70% of employees admit to risky behaviour that leaves their organizations vulnerable. [4]

Phishing
94% of businesses are reported to have experienced a phishing attack in 2024, with most of them experiencing negative impacts from these attacks. [5]

Deepfakes
75% of Deepfakes impersonated a CEO or other C-suite executive. [4]

AI Powered Cyber attacks
74% of IT security professionals report their organizations are suffering significant impact from AI-powered threats. [6]

IoT attacks
Security attacks on IoT devices have surged by 107% in the first five months of 2024, compared to the same period in 2023 [7].

Cloud Security
61% of organisations experienced cloud security incidents over the past 12 months, a significant increase from 24% in the previous year. [8]

Malware
81% of organizations faced malware threats in 2024. [9]

Cost of Cybercrime
The cost of cybercrime is expected to continue rising, potentially reaching $10.5 trillion annually by 2025. [9]

Source:

1. https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-1/
2. https://www.ibm.com/reports/data-breach
3. https://www.verizon.com/business/resources/Te3/reports/2024-dbir-data-breach-investigations-report.pdf
4. https://www.deepinstinct.com/voice-of-secops-reports
5. https://www.proofpoint.com/us/resources/threat-reports/state-of-phish
6. https://darktrace.com/resources/state-of-ai-cyber-security-2024
7. https://www.sonicwall.com/resources/white-papers/2025-sonicwall-cyber-threat-report
8. https://engage.checkpoint.com/2024-cloud-security-report/
9. https://keepnetlabs.com/blog/171-cyber-security-statistics-2024-s-updated-trends-and-data

Cyber Happenings in Mauritius

In 2024, the Computer Emergency Response Team of Mauritius (CERT-MU), serving as the national hub for incident response and coordination, recorded an increase in cyber incidents reported by both citizens and organizations. CERT-MU handled over more than 5000 incidents submitted via the Mauritius Cybercrime Online Reporting System (MAUCORS). It is to be noted that on 17th February 2025, an enhanced version of the MAUCORS has been launched, now known as MAUCORS+. The platform has been reinforced with new features and functionalities that will allow CERT-MU to analyse cyber trends more effectively. One of the key features of MAUCORS+ is the integration of a chatbot "MAIA+" based on AI to improve exchanges between users and support teams.

Cyber incidents are increasing in Mauritius and it has been observed by CERT-MU that children and youngsters are also being targeted. In this context, a National Sensitisation Campaign on Internet Safety was launched on 17th February 2025 in Mauritius. The objective of this campaign is to sensitise and educate children and young people on the dangers of the Internet and how they can use online technologies responsibly. In addition, an educational video clip on 'The Safer Internet' was also launched for primary and secondary school students. The video clip was aligned with the theme of SID 2025 "*Too good to be true? Protecting yourself and others from scams online".*

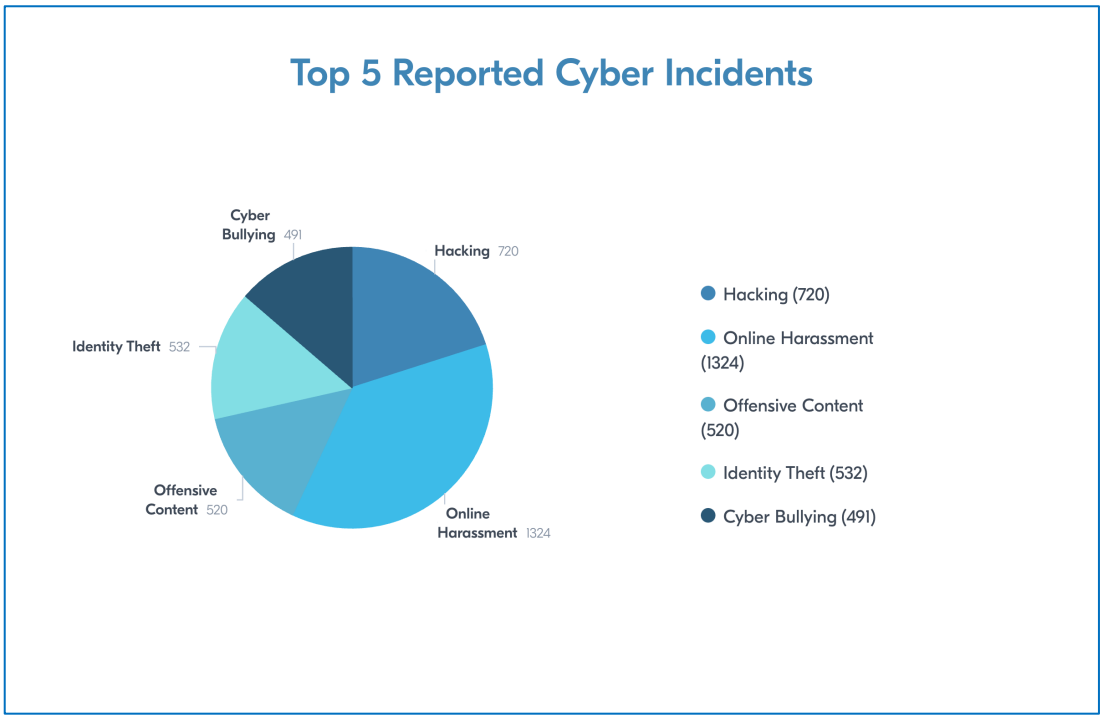
Moreover, prior to the launching of the National sensitisation campaign, ICT teachers of primary and secondary schools were trained through a Train-the-Trainers programme on Internet safety. More than 300 teachers from primary and secondary schools attended the training online. The aim of this training programme was to provide ICT educators with a comprehensive understanding of the dangers of the Internet and other cybersecurity threats so that they could sensitise their students on the safe and responsible use of the Internet. It is to be noted that following the launch

of the National sensitisation campaign on 17th of February by the Honourable Minister, an awareness session was also organised in all the primary and secondary schools between 1-2 p.m. for sensitising the students. All the primary and secondary schools were provided with the presentation on Internet Safety and video clip to play during the session. The video is available on CERT-MU's YouTube Chanel https://youtu.be/DXWPyJ6-PZY

Analysis of Cyber Incidents 2024

1. Social Media Based Threats

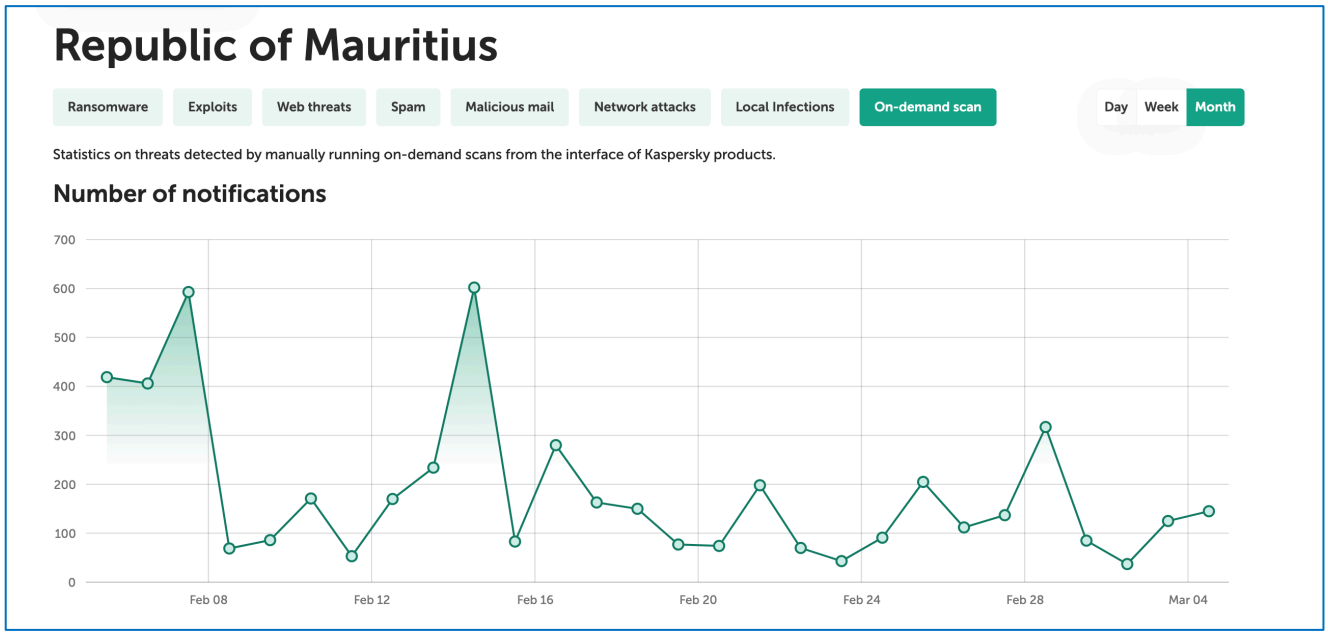
Social media-based threats remain one of the most dominant threats in Mauritius. This is due to the wide adoption of social media platforms in Mauritius, which include Meta (Facebook), TikTok and Instagram. Moreover, the increase use of mobile platforms such as WhatsApp and Telegram also act as contributing factors. As the number of Mauritian users using social media continue to rise, so is the number of cyber incidents on these platforms. In 2025, the top 5 most reported cyber threats are online harassment with 1324 cases, followed by 720 cases of hacking. Identity theft is the third most reported type of incident with 532 cases, followed by offensive Content with 520 cases and Cyber bullying with 491 cases respectively.



2. Ransomware

Ransomware continues to be a significant cyber threat to businesses and the general public – but it is difficult to know the impact of attacks because many victims does not come forward to report them. Looking back at the incident statistics for 2024, only 11 such incidents have been reported on MAUCORS+. Ransomware is an "ever present" threat and a major challenge to businesses and public services. However, the true impact of ransomware remains unclear, because many organizations that fall prey to ransomware attacks are not disclosing them.

As depicted in Kaspersky's graph for the months of February and March 2025 below, it indicates the presence of ransomware infection in Mauritius. However, these incidents were not reported on MAUCORS+.

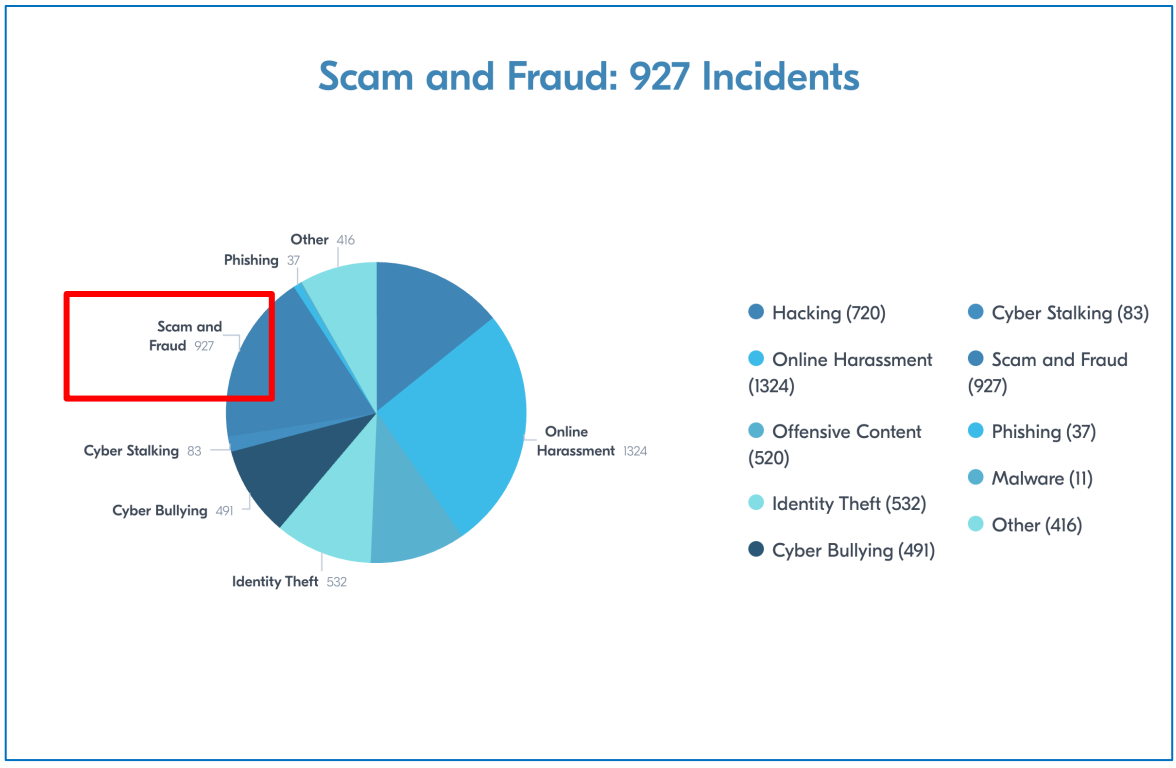


Source: https://statistics.securelist.com/

Ransomware and malware attacks have genuine real-world consequences and are a reminder to all organizations of the importance of taking mitigation measures to address these threats. It is therefore important that organizations treat cyber security as a genuine, board-level risk to be managed and report to authorities for the necessary guidance and resolution.

3. Online Scams and Frauds

Online scams and frauds remain one of the most dominant cyber threat affecting citizens and businesses in Mauritius, with more than 900 reported incidents in 2024. CERT-MU has observed that these cases involved fake online stores, romance scams, and financial fraud, where victims unknowingly share personal or banking information. Additionally, scammers leverage on social engineering tactics to manipulate users into making unauthorised transactions or revealing sensitive data. This threat is a major cybersecurity concern as cybercriminals are exploiting digital platforms to deceive individuals and businesses. Cybercriminals are increasingly using social media, emails, and messaging apps to carry out phishing attacks, impersonation scams, and fraudulent investment schemes.

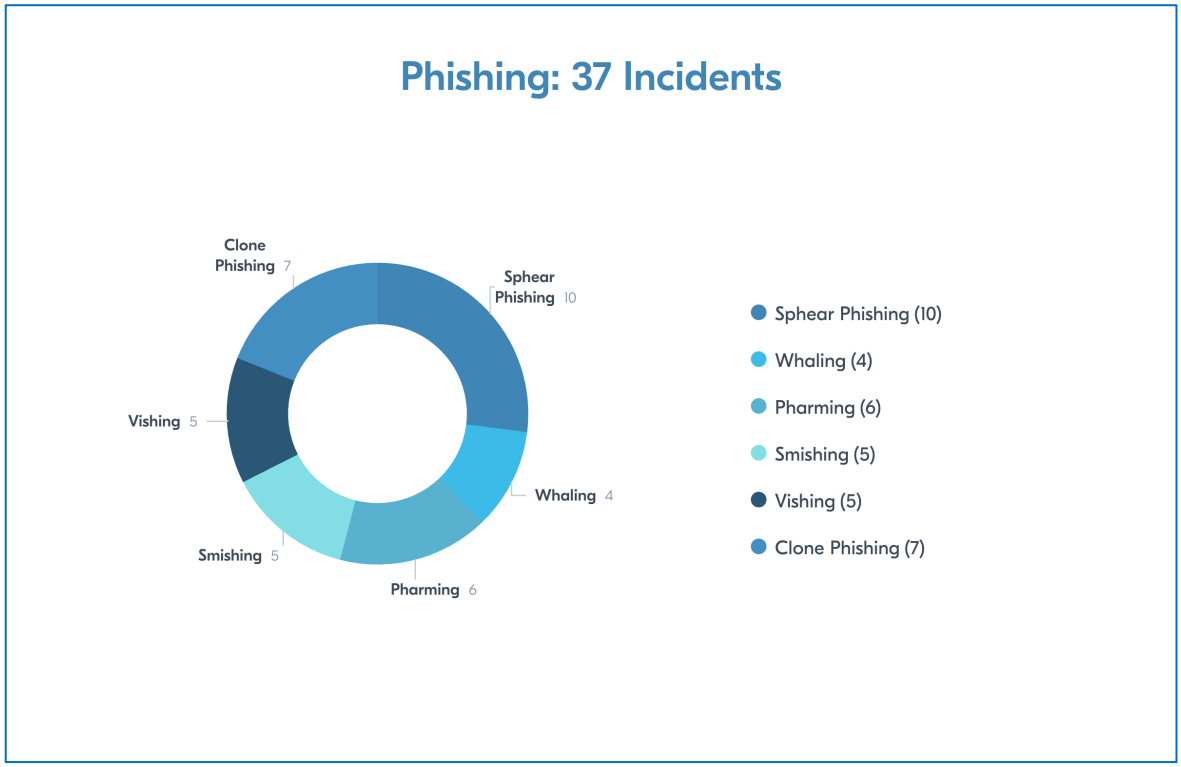


4. Phishing

Phishing remains one of the most prevalent cyber threats, targeting individuals and organizations through deceptive emails, messages, and websites designed to steal sensitive information. In 2024, 37 phishing incidents were reported to CERT-MU. These incidents comprised of the following types of phishing:

- Spear Phishing (Personalized Emails)
- Whaling: Emails Targeting High-Profile Individuals such as CEO
- Pharming: Redirecting Traffic to Fake Websites
- Smishing: Phishing Attacks via SMS
- Vishing: Phishing Attacks via Voice Calls
- Clone Phishing: Attacks that Use Duplicated Emails

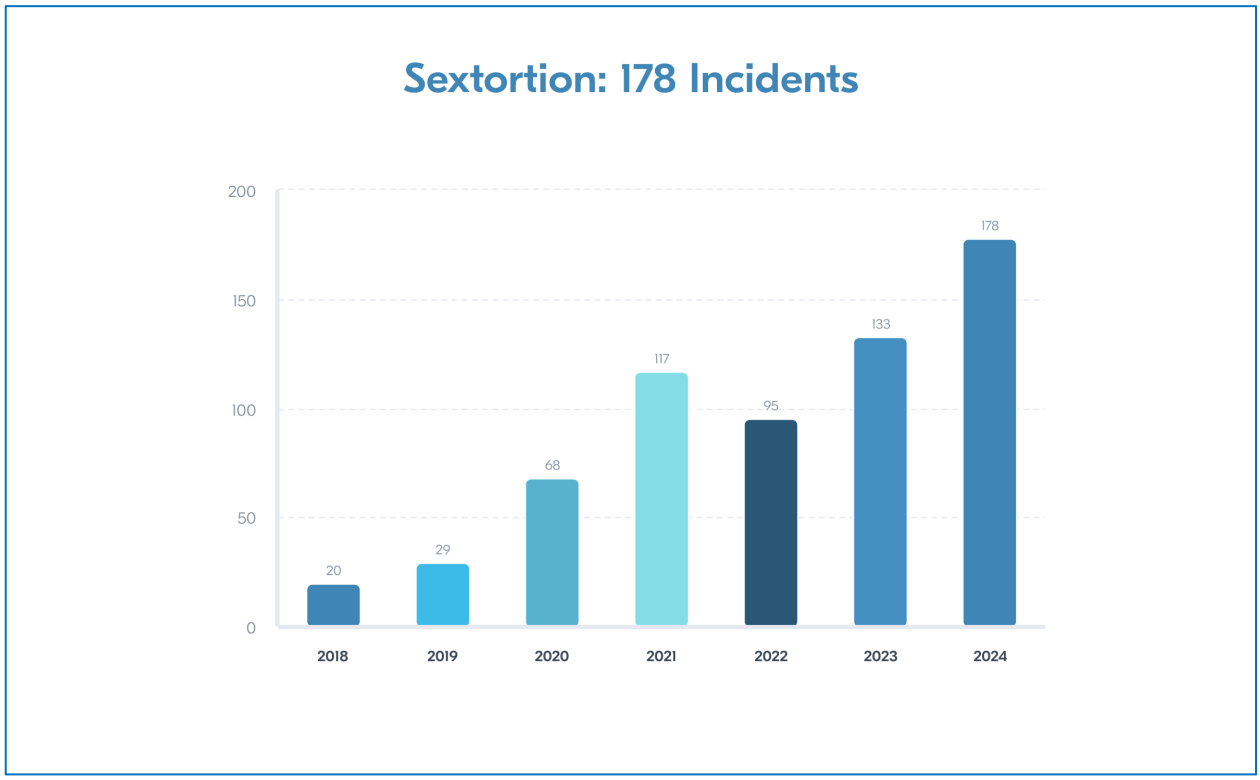
The most reported type of phishing incidents is spear phishing with 10 cases, followed by 7 cases of clone phishing. On the third position, there is pharming with 6 cases, followed by 5 cases of smishing and vishing respectively. Last, there are 4 cases of whaling which were reported.



5. Sextortion

Sextortion is another type of cybercrime which is increasing in Mauritius, especially targeting the youth. This type of crime is especially prevalent on mobile platforms such as WhatsApp and Telegram. In 2024, 178 cases of sextortion were reported on the MAUCORS+ platform. Sextortion occurs when an online predator tricks someone into giving them nude images or videos, and then demands money, more images, or makes

other demands such as threatening to share the images with the victim's friends and family if they do not comply. In 2024, an increase of 33.8% also is noted as compared to 2023.

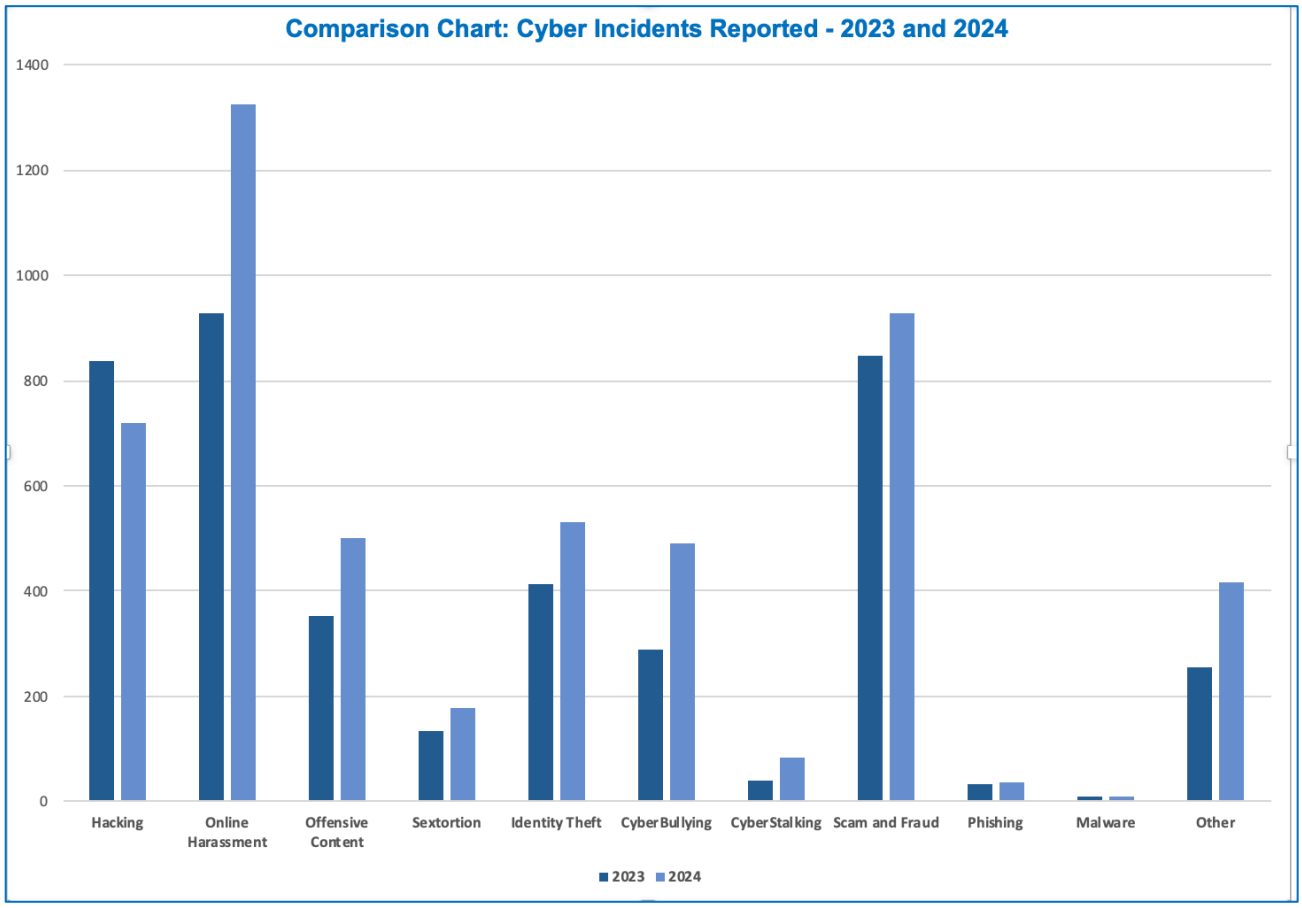


Comparative Analysis of Incidents Reported for 2023 and 2024

1. Comparative Analysis - Number of Incidents Reported on MAUCORS for 2023 and 2024

Every year CERT-MU conducts a comparative analysis to analyse the incident trends prevailing in Mauritius and also to identify the attack vectors, techniques and motivations used by cyber criminals. This allows to better anticipate and defend against such types of threats. For the year 2024, CERT-MU noted an increase in the total number of incidents reported. Certain types of incidents such as online harassment, scams and frauds, sextortion, cyber bullying and offensive content kept on increasing. However, new attack methodologies were employed to trick users.

However, we have also seen a significant increase in incidents regarding scams and online fraud. This has become one of the major cyber threats affecting Mauritians.

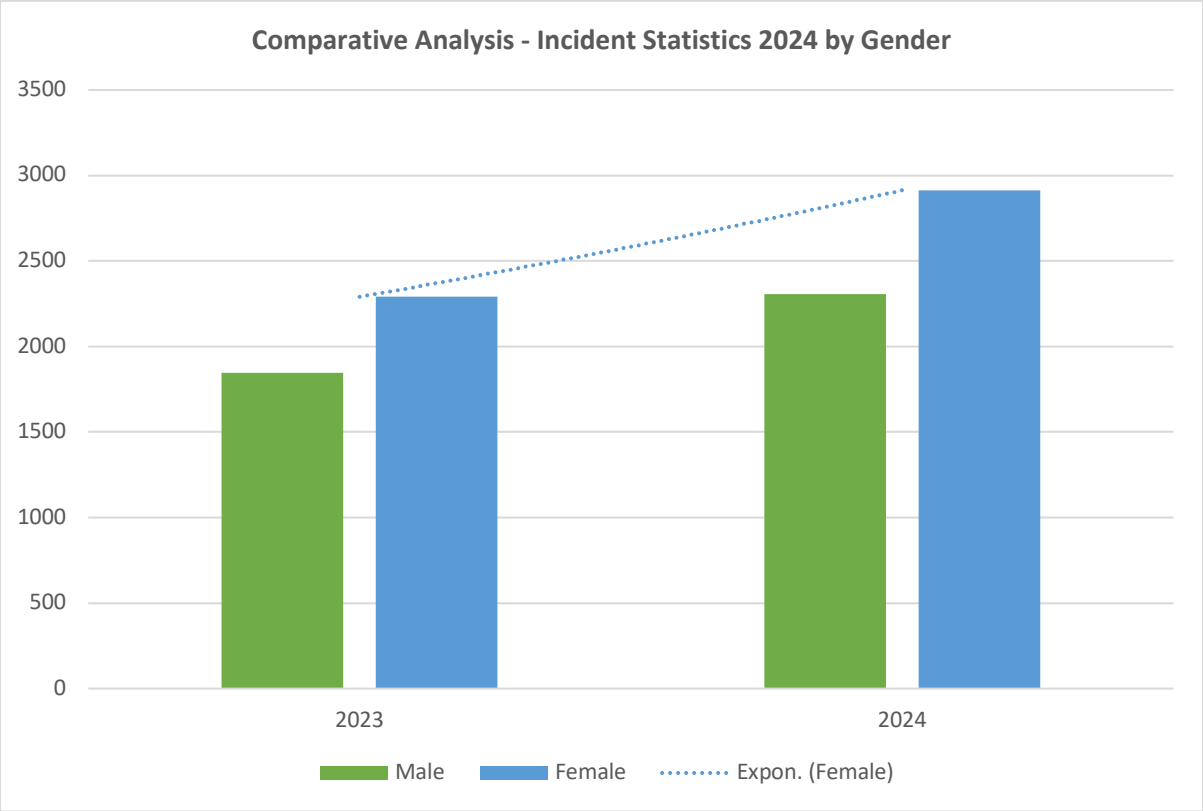


2. List of Incidents Reported by Gender

The rapid expansion of the digital realm has brought immense benefits, from connectivity to education and economic opportunities. However, it has also created a fertile ground for gender-based violence to evolve and proliferate. Studies across the world reveal that 16 to 58 per cent of women and girls have been targeted by violence online. Cyberviolence against women and girls is a pervasive issue, encompassing a wide range of harmful behaviours that exploit the anonymity and reach of digital platforms.

Based on the incident statistics reported on MAUCORS for the year 2024, it is to be noted that 2914 incidents were reported by females and 2305 by males respectively.

This also indicate a percentage increase of 27% as compared to the year 2023. For the past few years, CERT-MU noted that females are more prone to cyber incidents, such as online harassment, cyberstalking, sextortion, financial fraud, identity theft, and social engineering attacks, where attackers exploit trust to deceive the victims. Similarly, a rise has also been noted in the number of incidents reported by males, with 2291 incidents as compared to 1845 in 2023.



Cybersecurity Predictions 2025 - New Trends and Attacks

As the threat landscape grows, predicting cyber security trends 2025 becomes more important. These emerging issues range from AI-driven malware to concerns about quantum computing and require forward-thinking strategies. Below, some cybersecurity trends and threats are highlighted that could change digital defenses in the next few years. Understanding the motivations behind these latest cyber security trends will help businesses adapt their tools and training to not be left behind. To that end, let's take a closer look at each trend, explaining why it matters and how organizations can respond.

1. AI-Driven Malware

Machine learning is now being used by criminals to mutate malicious code in real-time to avoid being statically detected. As a result, this technology enables malware to deepen its installation, detect sandbox environments, and adapt to endpoint defenses. Manual threat hunting is outdated by AI-based infiltration, so defenders have to use advanced anomaly detection. Cyber security trends reveal that zero-day attacks, enabled through the use of automated tooling, are the most urgent threats.

2. Zero Trust Architectures

With perimeter-based security becoming obsolete, zero trust becomes the new hot thing. Zero trust gives blanket access only after initial authentication and then revalidates every request. Against the backdrop of lateral movement, a hallmark of advanced breaches, this approach provides an important option for defenders. Zero trust is one of the top cyber security trends in 2025, with more and more organizations adopting micro-segmentation, user context checks, and continuous session monitoring

3. Quantum Computing Threats

While mainstream yet, quantum computing has the potential to break contemporary encryption. Today, intercepted data may be stockpiled by cybercriminals or nation-states in the hope that they can decrypt it with quantum hardware in the future. Latest trends in cyber security discussions lead to quantum-resistant algorithms for critical data. By adopting post-quantum cryptography early, you'll be safe when quantum machines reach maturity.

4. Ransomware-as-a-Service Evolution

More and more ransomware groups are turning into service providers, providing affiliates with easy-to-use toolkits for a cut of the profits. This reduces the barrier to skill, creating a surge of attacks that weaken organizations and demand large payouts. RaaS has been flagged by many experts as a focal point within the cyber security trends 2025, with cost of recovering from a ransomware attack now averaging USD 2.73 million, according to research data. As such, offline backups and segmented networks become necessary resilience strategies.

5. 5G and Edge Security Risks

With 5G networks taking off, data volumes increase, and real-time use cases extend to IoT and industrial control systems. These new vulnerabilities at the edge are exposed, where sensitive tasks are performed without robust perimeter defenses. Disruptions of 5G infrastructure or edge computing nodes could impact supply chains, healthcare, or consumer applications. To thoroughly manage risk, from firmware updates to identity checks at the edge, the cyber security trends and challenges around 5G need to be observed.

6. Insider Threats Amplified by Hybrid Work

Insiders, such as a mix of remote staff, contractors, and distributed teams, are responsible for raising severe threats. Though employees may not intend to, when they misconfigure sharing links for cloud-based collaboration tools, they can expose

sensitive files. Disgruntled staff could steal intellectual property in the meantime. The latest cyber security trends in workforce security are tools that combine behavioural analysis and data loss prevention to mitigate insider-driven compromises.

7. Supply Chain Attacks

Attackers target vendors or third-party software and thereby compromise multiple downstream organizations at once. The ripple effect of compromised updates is brought to light by high-profile events, such as SolarWinds. This continues to be a top cyber security trend, forcing companies to thoroughly vet the security posture of their suppliers. Increasingly standard are contract clauses demanding continuous compliance and real-time monitoring of partner connections.

8. Cloud Container Vulnerabilities

Agility comes with containers and microservices, but so do new attack avenues if misconfigurations or unpatched images remain. It can pivot to the main environment from a single infected container to exfiltrate data or inject malicious code. Embedding checks in DevOps pipelines is an essential practice ("shift-left" security). Container security is a front and center cyber security trend and challenge for 2025 as businesses speed up DevOps.

9. Social Engineering via Deepfakes

Scammers can convincingly impersonate executives or celebrities through sophisticated audio-video manipulation. Voice calls based on deepfakes can fool employees to transfer funds or disclose credentials. As video conferencing has become the norm of remote work, deep fake phishing is a potent threat. These forms of manipulated social engineering are combated with awareness training and advanced verification steps.

10. Convergence of IT and OT Security

Traditionally, Operational technology (OT) domains such as manufacturing or critical infrastructure remained air-gapped from IT networks. However, as data driven insight and OT get merged in the context of Industry 4.0, new vulnerabilities emerge. Integration of specialized solutions is required because attackers can disrupt production lines or override safety systems. The latest trend in cyber security is to monitor both IT and OT for end-to-end coverage from enterprise apps down to the factory floors.

11. The increasing importance of supply chain security

Supply chain security breaches are indeed on the rise, with attackers exploiting vulnerabilities in third-party vendors to infiltrate larger networks. Monitoring of these third-party relationships is often insufficient. Most companies do not know all the third parties that handle their data and personally identifiable information (PII) and almost all companies are connected to at least one third-party vendor that has experienced a breach. This lack of oversight poses significant risks, as supply chain attacks can have cascading effects across industries.

Unsurprisingly, even prominent organizations fall victim to attacks via their suppliers' vulnerabilities. In 2025, organizations will need to prioritize investing in solutions that can vet and monitor their supply chain. AI-driven and transparency-focused solutions can help identify vulnerabilities in even the most complex supply chains. Organizations should also examine SLAs to select suppliers that maintain strict security protocols themselves, thereby creating ripples of improved security further down the ecosystem.

Staying Ahead with the Evolving Cyber Threats

In an era where digital transformation is reshaping industries, cybersecurity stands as a critical safeguard against evolving threats. As we step into 2025, the landscape of cyber risks continues to morph, driven by advancements in technology and the ever-growing sophistication of threat actors. From AI-powered cyber-attacks to the relentless surge in ransomware incidents, organizations face an array of challenges that demand proactive defense strategies such as:

1. Conduct a Gap Assessment

To cope with this dynamic cyber threat landscape, it is important to assess your current situation and identify your strengths and weaknesses. Tools such as self-assessments, audits, vulnerability scans, or penetration tests can be used to evaluate the security posture and find gaps or weaknesses. Policies, procedures, and training programs could also be reviewed to ensure they are up to date and aligned with your goals and industry standards.

2. Threat Monitoring and Analysis

Establishing a robust threat monitoring and analysis system is important for detecting and responding to potential attacks or breaches quickly and effectively. A comprehensive strategy against cybersecurity threats incorporates various tools and actions. These can include the implementation of Security Information and Event Management (SIEM) tools to detect abnormal or suspicious activities. These tools detect much faster than humans can and generate alerts. SIEM tools can also be integrated with other technologies, such as vulnerability scanners. Other technologies to leverage on include vulnerability management and assessment platforms, asset discovery and inventory tools, network scanning and mapping tools, and web application scanners.

3. Effective Incident Response Strategy

Be proactive and take actions to prevent or mitigate attacks as they occur. This could be done by implementing measures such as encryption, firewalls, antivirus, backups, and multi-factor authentication. The network and systems could also be monitored for any signs of suspicious activity or breaches. If an incident is detected, response should be quick and effective. In addition, employees should be trained and educated on the latest trends and threats, and encouraged to follow the best practices for security hygiene and awareness.

4. Implement Zero Trust Architecture

Zero Trust Architecture (ZTA) is a modern cybersecurity approach that eliminates implicit trust and continuously verifies every access request to an organization's network, applications, and data. Unlike traditional perimeter-based security models, ZTA enforces strict identity verification, least privilege access, micro-segmentation, and continuous monitoring to prevent unauthorized access and lateral movement within networks. By integrating multi-factor authentication (MFA), encryption, and AI-driven anomaly detection, organizations can proactively mitigate cyber threats and ensure data security. Implementing ZTA requires a strategic shift in security policies, advanced access controls, and robust endpoint security, making it an essential component of a resilient cybersecurity framework.

5. Cybersecurity Education and Training

Employee education and training can help employees understand and recognize common cyber threats, such as phishing and social engineering. This includes educating employees on how to identify suspicious emails and links and how to avoid falling victim to social engineering attacks. Moreover, it can also help employees understand and implement best practices for protecting sensitive information and systems. This includes educating employees on how to use strong passwords and how

to handle sensitive information securely. Regular training and education are the best ways to keep employees informed on the latest cyber threats and best practices.

6. Ensure Compliance with Regulatory Frameworks

As cybersecurity threats continue to evolve, governments and regulatory bodies are implementing stricter cybersecurity regulations to enhance data protection, privacy, and organizational resilience. Organizations must align their security policies with frameworks such as GDPR, PCIDSS, amongst others, to meet compliance requirements. Regular audits, vulnerability assessments, and compliance checks should be conducted to identify and remediate gaps in security posture. Additionally, maintaining thorough documentation, implementing governance frameworks, and fostering a culture of regulatory awareness can help organizations stay ahead of evolving legal obligations while reinforcing their cybersecurity defenses.

7. Continuous Monitoring and Improvement

Cyber threats are constantly evolving. As such, cybersecurity safeguards and strategies must also adapt and improve over time. Stay ahead of cyber threats by testing and improving your security performance and resilience. This can be done by conducting regular reviews, audits, or drills, that can measure the security level and identify areas for improvement. Feedbacks, data or reports could help in understanding the security strengths and weaknesses, and track progress and results. Additionally, changes could be implemented or improved that could further can help to address the security challenges and achieve security goals.

Conclusion

The cyber threat landscape in 2025 continues to evolve, driven by the increasing sophistication of cybercriminals, the proliferation of AI-driven attacks, and the expanding attack surface due to digital transformation. The analysis of notable cyber-attacks in 2024 has revealed critical vulnerabilities across industries, with ransomware, supply chain attacks, and data breaches being among the most prevalent threats. The statistics and trends highlight a surge in targeted attacks against critical infrastructure, financial institutions, and emerging technologies, reinforcing the urgent need for enhanced cybersecurity measures.

Looking ahead, predictions for 2025 indicate that adversaries will further exploit AI for advanced threat automation, leverage deep-fake technology for deception, and continue targeting cloud environments and IoT devices. As cyber threats become more adaptive, organizations must adopt a proactive and resilience-focused approach.

To mitigate future risks, this report recommends prioritizing cybersecurity measures, strengthening cyber threat intelligence capabilities, implementing Zero Trust Architecture, and fostering a culture of cybersecurity awareness. Additionally, collaboration between governments, private sector entities, and threat intelligence-sharing communities will be crucial in staying ahead of emerging threats.

By taking a strategic and proactive stance on cybersecurity, organizations can enhance their defense mechanisms, minimize business disruptions, and safeguard critical assets against the evolving cyber threat landscape in 2025 and beyond.

Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation
Level 3, Wing A
Shri Atal Bihari Vajpaye Tower
Cybercity Ebene
Email: contact@cert.govmu.org