Cybersecurity Trends & Predictions 2024

CERT-MU

March 2024

Contents

Introduction

Over the past year, the cybersecurity landscape has witnessed significant transformation. The geopolitical upheaval stemming from the Russia-Ukraine war, the Israel-Hamas war and the trade tensions between US and China casted a profound shadow in the cybersecurity world in 2023. The intensification of cyber espionage, disinformation campaigns, and ransomware attacks highlighted the interconnectedness of geopolitics and cybersecurity. As the conflict unfolded, organisations worldwide faced the challenge of safeguarding their digital assets amid heightened global tensions. The year served as a stark reminder that geopolitical events can have far-reaching implications, necessitating a vigilant and adaptive cybersecurity approach in an ever-changing digital world. Simultaneously, we also saw that malicious actors continue to employ new innovative methods to exploit and retool existing tactics and strategies to follow new schemes. The substantial growth in Artificial Intelligence (AI) and AI generative tools in 2023 also helped in this process as these tools are also being used by threat actors to generate malicious content, thereby raising significant cybersecurity and misinformation concerns.

On the regional front, as per a report by Kaspersky in the last quarter of 2023, Africa remains one of the regions most targeted by cybercrime in 2023. Examples of the most reported type of attacks include web threats, phishing, attack on industrial control systems, Internet of Things (IoT) based attacks. However, Africa is among the regions with the highest number of detected attacks on industrial control systems (ICS computers). ICS computers are used in energy and mining sectors, automotive manufacturing, building automation infrastructures and other spheres to perform a range of operational technology functions – from the workstations of engineers and operators to supervisory control and data acquisition servers.

Regarding the local scenario, there was a notable increase in the reported incidents on the Mauritian Cybercrime Online Reporting System (MAUCORS) in 2023 as compared to 2022. Online scams and frauds were the most reported type of incident, followed by online harassment. During 2023, new attack vectors and methodologies were also identified.

Further to the analysis of the cyber events of 2023, we can say that cyber-attacks are increasing and becoming more sophisticated. As we begin the year 2024, organisations should be prepared and have the ability to resist to cyber incidents that have been predicted by security researchers and vendors.

This Report offers a comprehensive summary of the global 2023 cybersecurity threat landscape and provide insights of the type of incidents that have been reported on the Mauritius Cybercrime Online Reporting System (MAUCORS). The report also provides a prediction of the cyber events that we are expecting this year. The information provided facilitates a better understanding of trends, aiding in informed decision-making, prioritization of actions, and the formulation of relevant recommendations.

A Flashback of 2023: Major Cyber Breaches Worldwide

2023 has been another tumultuous year for cyber security, with a number of high-profile breaches and incidents making headlines around the world. From state-sponsored cyber-attacks to extortion campaigns, it is clear that the threat landscape is constantly evolving. Cybersecurity professionals faced new challenges, doing battle deep in the trenches to proactively prevent the next big event. Let's take a look back at the biggest cyberattacks, threats, and data breaches to rock the world in 2023.

1. The Royal Mail Ransomware Attack

In January 2023, the UK's postal service the Royal Mail was hit by a ransomware attack which resulted in a temporary halt to international deliveries. Data was also stolen by the attackers. The Royal Mail refused the pay the £65.7m ($79.85m) demand from the LockBit group to return the stolen data. However, the service revealed it had experienced huge financial costs as a result of the attack, including large revenue losses and the company is said to have spent £10m on ransomware remediation.

2. Enormous Data Breach at T-Mobile

International telecoms giant T-Mobile admitted that 37 million customers had their personal and account information accessed by a malicious actor via an API attack that began on November 25, 2022. The incident was not discovered until January 5, 2023. In a separate incident, T-Mobile USA notified customers of another breach of personal and account data that occurred in February and March 2023. The breaches mean many millions of customers are vulnerable to follow-on fraud attempts.

3. ESXi Ransomware Attacks

In February 2023, the "ESXiArgs" ransomware campaign targeted customers that run the VMware ESXi hypervisor. Around 3800 servers were compromised worldwide. Countries such as US, Canada, France and Germany were affected by this campaign. The ransomware exploited a two-year-old vulnerability (tracked at CVE-2021-21974)

in older VMware ESXi versions. The vulnerability affected the OpenSLP service, and successful exploitation would allow remote code execution.

4. City of Oakland Ransomware Attack

In February 2023, the administration of the City of Oakland, California, declared a state of emergency as a result of a ransomware attack. The incident shut down many non-emergency services, while government buildings were forced to close temporarily. It was later reported that the hackers stole a decade's worth of sensitive data from city servers in the attack, including information about employees in sensitive roles such as the police.

5. GoAnywhere Attacks

In February 2023, a zero-day vulnerability was identified in the GoAnywhere file transfer platform and it was actively exploited by remote attackers to cause execution of remote code on vulnerable systems. The GoAnywhere platform allowed hackers to steal data from numerous other large organizations including Procter & Gamble, the City of Toronto, Crown Resorts and data security firm Rubrik. This vulnerability was also was used against a small number of on-premise implementations running a specific configuration of the GoAnywhere MFT solution.

6. Chinese Espionage Campaign Infiltrates US Government

Microsoft discovered a Chinese cyber-espionage campaign that enabled the Storm-0558 group to gain access to customer email accounts from May 15, 2023. This included employees in the US State and Commerce Departments and other US government agencies. To launch the campaign, the attackers compromised a Microsoft engineer's corporate account, leading to the tech giant being criticised and even accused of negligence by a US lawmaker.

7. MOVEit Hack

In 31st May 2023, a highly critical vulnerability was identified in MOVEit Transfer, a managed file transfer (MFT) service by Ipswitch, Inc. This service is integral to industries such as healthcare, government, finance, and aviation, secures and transmits files via Secure File Transfer Protocol (SFTP). The vulnerability (CVE-2023-34362) consisted of an SQL injection flaw in MOVEit Transfer's web application. This breach allowed intruders to access and potentially alter or delete elements within the database, which varies based on the database engine (MySQL, Microsoft SQL Server, or Azure SQL). Since its first detection, over 2,620 organisations and more than 77 million individuals were impacted. Some of the affected organisations included British Airways, BBC, Aer

Lingus, Bank of America, Avast and hundreds of universities and other government agencies.

8. Indonesia Immigration Directorate General Data Breach

In July 2023, over 34 million Indonesian passports were leaked in a massive data breach impacting the country's Immigration Directorate General at the Ministry of Law and Human Rights. As per the investigators, the hackers also provided 1 million data samples which appear to be valid. The timestamp is from the 2009-2020 period. The exposed data includes full names, passport numbers, dates of issue, expiry dates, dates of birth, and gender of 34.9 million Indonesian passport holders.

9. UK Electoral Commission Cyberattack

On August 8th, 2023, the UK's Electoral Commission became victim to a cyber-attack where adversaries accessed the electoral registers, jeopardizing the personal data of approximately 40 million individuals. The breach was first detected in October 2022, but the suspicious activities were traced back further to August 2021. The attackers infiltrated servers containing emails, control systems, and electoral registers from 2014 to 2022, including overseas voters' data. The registers held voters' names, addresses, and birthdates. Security researchers noted that the Commission was using an unpatched Microsoft Exchange Server, vulnerable to ProxyNotShell attacks. Compromised data also included personal details from the Commission's emails, like names, email and home addresses, phone numbers, and other information from web forms or emails.

10. DarkBeam Data Leak

In September 2023, over 3.8 billion records were compromised due to an oversight by digital protection company DarkBeam. The vulnerability existed due to the unprotected Elasticsearch and Kibana data visualization interface, allowing access to the confidential data held within it. Consequently, about 239,635,000 login credentials pairs were leaked.

11. India's Aadhaar Data Breach

In October 2023, an American cyber security company stated that the personally identifiable information of 815 million Indian citizens, including Aadhaar numbers and passport details, were being sold on the dark web. While threat actors declined to specify how they obtained the data, without which the source of the data leak is difficult to ascertain, threat actors claimed they had access to a 1.8 terabyte data leak impacting an unnamed "India internal law enforcement agency".

12. Indian Council of Medical Research (ICMR) Data Breach

On 9 October 2023, the Indian Council of Medical Research (ICMR) became victim to a data breach, impacting 815 million Indian residents. The stolen data included victims' names, ages, genders, addresses, passport numbers, and Aadhaar numbers. The breach involved data from the ICMR's Covid-testing database and was offered for sale on the dark web.

13. New York Real Estate Wealth Network Data Breach

In December 2023, a non-password protected database that held 1.5 billion records containing real estate ownership data of millions of people, including celebrities, politicians were discovered by security researchers. The database belonged to New York-based Real Estate Wealth Network. The exposed database contained a total 1,523,776,691 records with a size of 1.16 TB. The data was organized in various folders according to: property history, motivated sellers, bankruptcy, divorce, tax liens, foreclosure, home owner association (HOA) liens, inheritance, court judgments, obituary (death), vacant properties, and more. The folders contained information on property owners, sellers, investors, and what appeared to be internal user logging data that included name, physical address, phone number, provider, and what was downloaded from the database.

The Evolution of Cyber Threats in 2023

In 2023, we saw significant development in the evolution of cyber threats, ranging from ransomware, hacktivism, rising mobile threats to the wide use of AI by the bad actors. New cyber threats were born with sophisticated attack methodologies. Based on the findings of different cybersecurity research, the most dominating threats that we have seen in 2023 are described below:

1. Malware

In 2023, we saw the apparition of various malware families with different purposes, from dropping additional malware and data theft to establishing command and control to enrolling the infected device in a botnet. Security experts responded to a variety of malware infections, such as Raccoon Stealer, IcedID, Cobalt Strike, ngrok usage, and malicious script executions. This diverse range of threats underscores the need for continuous vigilance and advanced security measures in the ever-changing landscape of cyber threats. Some of the notable malware attacks are as follows:

- *Exploiting OneNote for malicious payloads*

Cybercriminals leveraged Microsoft OneNote to deliver many malicious payloads to victims, including Redline, AgentTesla, Quasar RAT, and others. This previously underutilized Office program became a favoured tool due to its low suspicion and widespread usage.

- *SEO poisoning and Google Ads*

Malicious actors resorted to SEO poisoning tactics, deploying phishing links through Google Ads to deceive unsuspecting victims. These links led to cloned, benign web pages, avoiding Google's detection and remaining active for extended periods. Prominent malware families, including Raccoon Stealer and IcedID, capitalized on this strategy.

- *Exploiting geopolitical events*

Cybercriminals exploited the geopolitical climate, particularly the Middle East conflict, as a lure for their attacks. This trend mirrored the previous year's Ukraine-related phishing campaigns and crypto scams.

- *Advanced Persistent Threats (APTs): State-sponsored espionage*

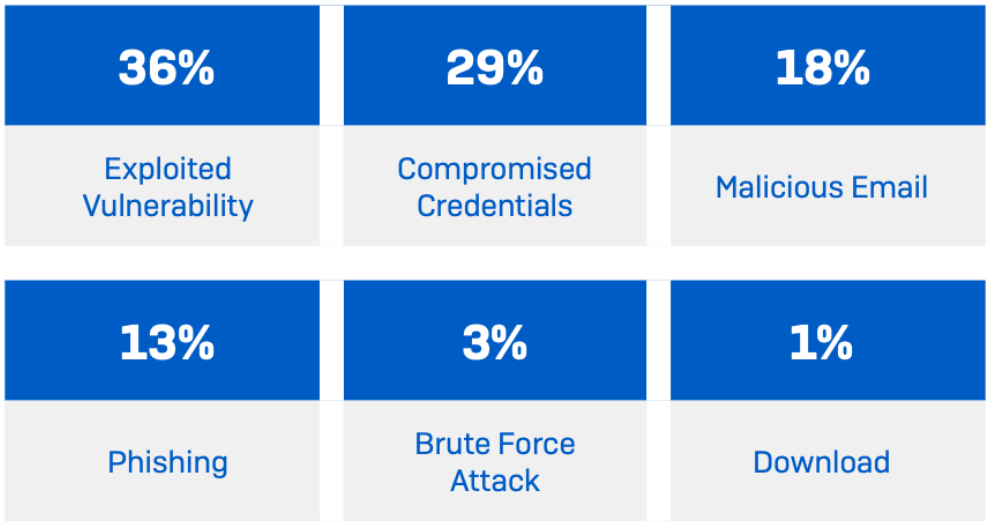
    - CISA reported on the Snake APT, an advanced cyber-espionage tool associated with the Russian Federal Security Service (FSB). This malware had been in use for nearly two decades.
    - Volt Typhoon: A campaign targeting critical infrastructure organizations in the United States was attributed to Volt Typhoon, a state-sponsored actor based in China. Their focus lay on espionage and information gathering.
    - Storm-0558: This highly sophisticated intrusion campaign, orchestrated by the Storm-0558 APT from China, infiltrated the email accounts of approximately 25 organizations, including government agencies.

2. Ransomware

In 2023, ransomware attacks reached peak levels according to security researchers. Several factors contributed to this spectacular increase. One of them is due to the proliferation of Cybercrime-as-a-service (CaaS). CaaS enables cybercriminals to outsource various attack elements, making more complex techniques accessible to less tech-savvy individuals. According to the "*2023 ThreatLabz State of Ransomware Report"*, ransomware attacks increased by 37% in 2023 with the average enterprise ransom payment exceeding US$100,000. The *"Sophos State of Ransomware 2023*

Report" also states that ransomware is one of the biggest cyber risk facing organisations today and these types of attacks will not slowdown in 2024, especially with the wide adoption of AI.

While it was a successful year for the entire ransomware industry, three families were far ahead of the pack. As per *CyberInt 2023 Ransomware Report*, LockBit3.0 remains the most dominant ransomware group with 252 new victims, 17.7% of all ransomware cases. Second is Cl0p Ransomware, which was able to claim a significant number of 177 victims. Third is the group ALPHV with 120 victims. These ransomware groups have been targeting a number of organisations in different sectors, including finance, education, IT amongst others. The *"Sophos State of Ransomware 2023 Report"* further highlights the root causes of these ransomware attacks which is 36% through exploited vulnerability, followed by 29% comprised credentials, 18% malicious emails, 13% through phishing, 3% brute force attacks and 1% through downloads.



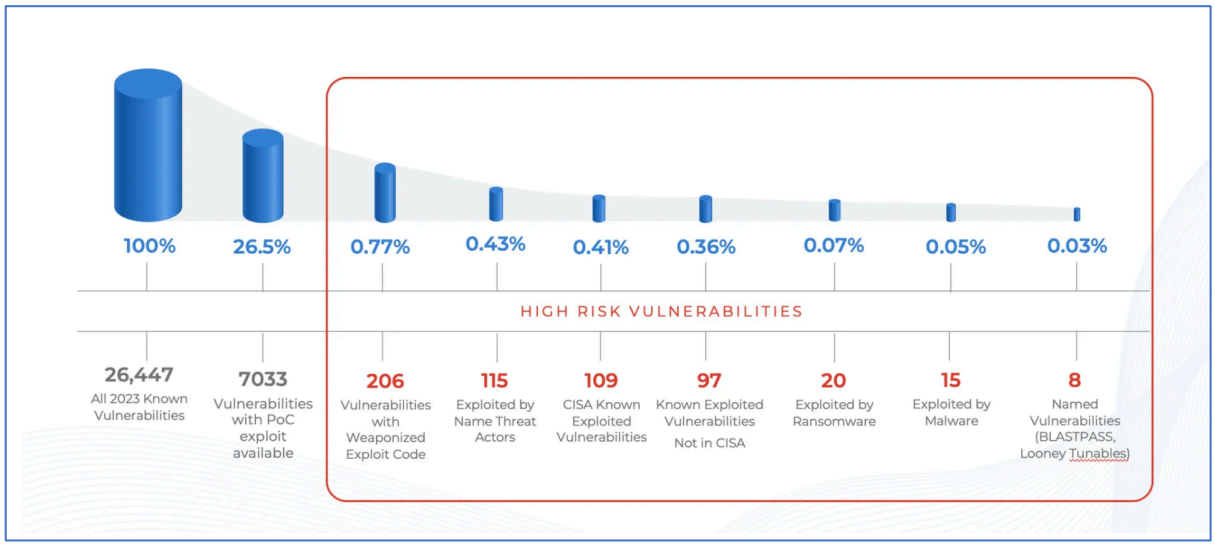
Source: Sophos: 2023 State of Ransomware Attacks

3. Vulnerabilities in Systems and Applications

According to the Qualys Threat Research Unit (TRU), a total of 26,447 vulnerabilities were disclosed in 2023, surpassing the previous year by over 1500 CVEs. Key findings revealed that 97 high-risk vulnerabilities, likely to be exploited, were not part of the CISA Known Exploited Vulnerabilities catalog. Additionally, 25% of high-risk vulnerabilities were exploited the same day they were published. The deep dive into the vulnerability threat landscape also highlighted that over 7000 vulnerabilities had proof-of-concept exploit code, while 206 had weaponized exploit code, increasing the likelihood of successful compromises. The report also revealed that 32.5% of high-risk

vulnerabilities affected network devices and web applications, emphasizing the need for a comprehensive vulnerability management strategy.

The chart below shows the high-risk vulnerabilities that were analysed by TRU in terms of their attack methodologies, tactics and defense strategies.



Source: Qualys Threat Research Unit, December 2023

4. Hacktivism

An increase in hacktivism was noted in 2023 amidst the prevailing geopolitical tensions between Israel-Hamas, Ukraine-Russia, and Taiwan-China. As per security reports, an increase in 11% was noted in the first half of 2023 alone. This rise in cyberattacks is defining a new trend in the operations of hacktivist groups. Cybersecurity researchers have noted that the trend in hacktivism is shifting towards financial motivations, as demonstrated by the actions of several prominent groups such as:

- The Five Families Telegram Channel, a collective threat actor drawn from the groups ThreatSec, GhostSec, Stormous, Blackforums, and SiegedSec, marks an interconnected network of diverse hacktivist cells.

- SiegedSec, identified as a Russian-aligned hacktivist group, reportedly launched attacks on NATO and Atlassian this year alone. This group's activities indicate the increasing audacity of hacktivist operations and their capacity to challenge large institutions.

- Similarly, Anonymous Sudan, an unofficially aligned hacktivist group with the nation of Sudan, has been seen to target significant corporations, including

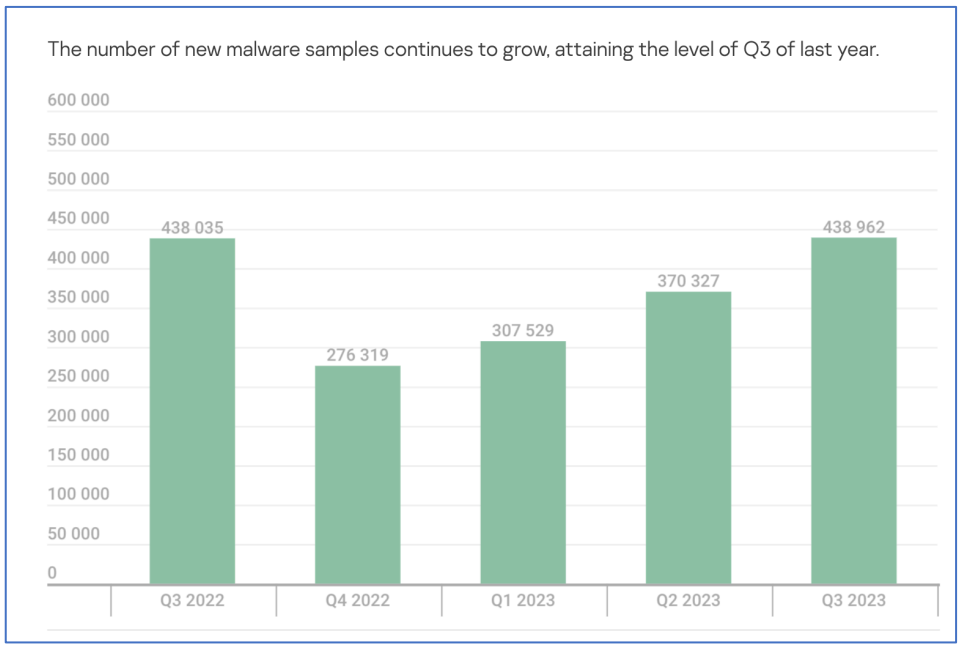
Microsoft and Riot Games, furthering their scope by partnering with other threat groups, namely REvil and KillNet.

- KillNet, another Russian-aligned hacktivist group, appears to target US corporations specifically. A significant attack on US airlines, which led to 24 airline websites experiencing downtime, underlines this objective.

Investigating the intricate web of hacktivism and its evolving strategies, the transition from ideological to financial motivations, and the affiliations with national allies sheds light on the rapidly changing landscape of global cybersecurity threats.

5. Mobile Threats

In 2023, mobile malware has reached unprecedented levels of sophistication, targeting both Android and iOS platforms with a variety of malicious software, including ransomware, spyware, and banking Trojans. As per Kaspersky Q3 Mobile Threat Report 2023, more than 400,000 samples of mobile malware were detected.



Source: Kaspersky IT threat evolution in Q3 2023. Mobile statistics

These advanced malware variants can compromise user data, device functionality, and financial assets, emphasizing the need for robust endpoint security solutions, regular software updates, and user education to mitigate the risks associated with mobile malware attacks.

6. IoT Vulnerabilities

The proliferation of Internet of Things (IoT) devices connected to mobile networks has introduced new security vulnerabilities, creating an expansive attack surface for cybercriminals. Inadequately secured IoT devices can serve as entry points for sophisticated cyberattacks, enabling attackers to infiltrate mobile devices, networks, and critical infrastructure systems. Securing IoT devices, implementing network segmentation, and conducting regular vulnerability assessments are essential steps to mitigate IoT-related security risks in 2024.

7. 5G Security Concerns

The telecommunication sector is undergoing a transformation with the introduction of 5G technology, presenting vast potential and a myriad of opportunities. However, as technology advances, threat actors are becoming more sophisticated, posing a significant challenge for communication service providers (CSPs) in maintaining robust security measures. The Nokia Threat Intelligence Report 2023 sheds light on the trends surrounding 4G and 5G security attacks, malware incidents, Distributed Denial-of-Service (DDoS) attacks, and other telco cyber threats affecting fixed and mobile networks worldwide. According to the report, the global rollout of 5G networks has presented new security challenges, including increased attack surfaces, potential vulnerabilities in network infrastructure, and sophisticated cyber threats targeting high-speed mobile connectivity.

8. Supply Chain Attacks

A supply chain attack occurs when cybercriminals target a weaker link in a company's supply chain network. This could be a supplier, vendor, a customer or a third-party software library that the company is dependent upon. As per the Gartner 2023 Supply Chain Risk Management Survey Report, supply chain attacks are on the rise, with 63% of respondents reporting that their organization has experienced a supply chain attack in the past year. Some of the most notable supply chain attacks in 2023 are:

- Applied Materials Supply Chain Attack (February 2023): A key partner of Applied Materials was targeted, resulting in a staggering $250 million loss in Q1 2023. The attack caused significant shipment delays and financial turmoil.

- University of San Francisco Attack (February 2023): Think about a scenario where a doctor cannot perform life-saving surgeries because the system is offline for several days. In this attack, staff members could not access records or schedule surgeries, and personal information belonging to clinical trial participants was stolen.

- MOVEit Supply Chain Attack (June 2023): Personal data and flight safety were compromised in a massive breach, putting travel security for thousands at risk.

- 3CX Supply Chain Attack (March 2023): Malware was silently delivered to and hidden within several client organizations, acting as a ticking time bomb with hackers in control of the detonator switch.

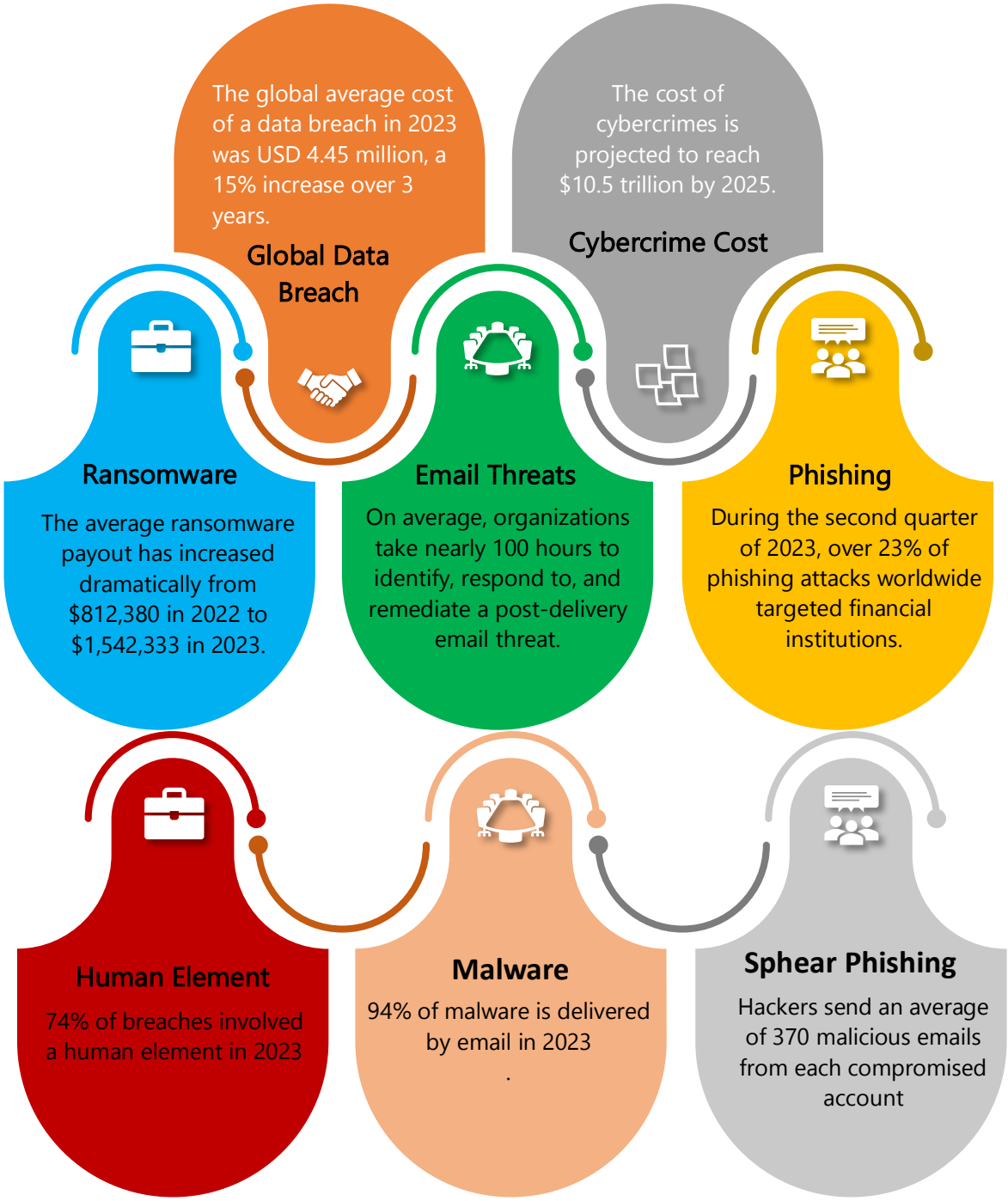
9. The Boom of AI

The year 2023 witnessed substantial growth in AI, highlighted by OpenAI's ChatGPT's rapid user increase and the emergence of multiple generative AI tools. These tools have been incorporated into threat actors' toolset to generate malicious content, raising significant cybersecurity and misinformation concerns. These developments indicate an evolving landscape where AI not only facilitates content creation, but also intensifies cybersecurity threats and misinformation campaigns on social media by streamlining processes and lowering the barrier to entry. A research carried out by Kaspersky revealed that AI has firmly positioned itself at the forefront of global conversations. With the increasing spread of large language models (LLMs), the surge in security and privacy concerns directly links AI with the cybersecurity world. As per Kaspersky security researchers, AI tools have helped cybercriminals in their malicious activity in 2023. The company's experts also reveal the evolving landscape of AI-related threats in the future that might include more complex vulnerabilities, the use of neural networks to generate visuals for scams, amongst others.

10. Social Engineering Attacks

The human element still makes up the overwhelming majority of incidents, and is a factor in 74% of total breaches, even as enterprises continue to safeguard critical infrastructure and increase training on cybersecurity protocols. One of the most common ways to exploit human nature is social engineering, which refers to manipulating an organization's sensitive information through tactics like phishing, in which a hacker convinces the user into clicking on a malicious link or attachment.

Useful Statistics: Cyber Security in 2023



Sources:

1. *SC Magazine - Report: Ransomware payouts and recovery costs went way up in 2023*
2. *https://www.scmagazine.com/resource/report-ransomware-payouts-and-recovery-costs-went-way-up-in-2023*
3. *IBM Report https://www.ibm.com/reports/data-breach*
4. *Verizon - 2023 Data Breach Investigations Report: https://www.verizon.com/business/en-nl/resources/reports/dbir/*

Cyber Happenings in Mauritius

In 2023, the Computer Emergency Response Team of Mauritius (CERT-MU), which is the national focal point for incident response and coordination, observed a rise in the number of cyber incidents reported by citizens and organisations. The CERT-MU responded to more than 4000 incidents that were reported through the Mauritius Cybercrime Online Reporting System (MAUCORS). The collective analysis of these incidents allowed the national CERT to identify cyber threat trends targeting citizens and carry out risk profiling.

It is to be noted that cyber incidents are also reported to other agencies such Cybercrime Unit of the Mauritius Police Force, the Data Protection Unit and the Information Communications Technology Authority (ICTA) and regulatory bodies of critical sectors.

Moreover, CERT-MU being an established and SIM3 accredited CERT, also operates the Government Security Operations Centre (SOC) to better monitor and coordinate cyber-threats responses at the level of the Government. Through this establishment, the Government's ICT infrastructure is monitored for threat detection. When an incident is detected, it is triaged to determine the severity and impact. The CERT-MU then takes appropriate action to address the incident.

In terms of strengthening its regulatory frameworks and ensuring that Mauritius remains capable and resilient in this fast-moving digital world, the Government has released the 2023-2026 National Cybersecurity Strategy, which is built on the foundations of the 2014-2019 National Cybersecurity Strategy and 2017-2019 National Cybercrime Strategy. Through the new cybersecurity strategy, the Government's aim is to strengthen the security and resilience of critical information infrastructure against cyber threats, ensure that our legal framework remains strong and resilient to cybercrime, promote collective responsibility for cybersecurity, promote innovation, enterprise security and cybersecurity education and finally strengthen regional and international partnership.

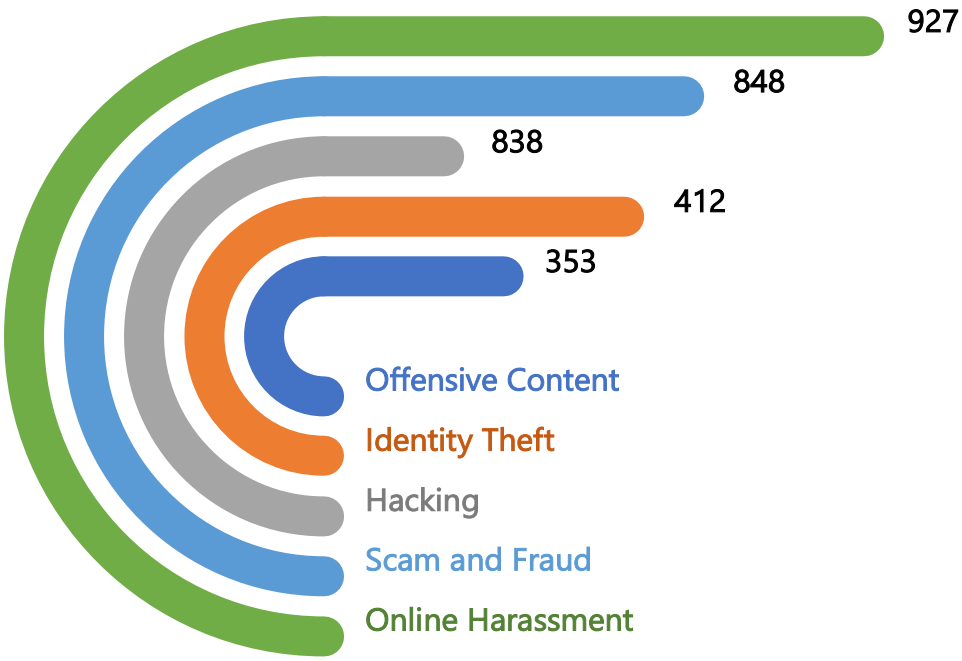
Analysis of Cyber Incidents 2023

1. Social Media Threats

Social media has become a popular platform in Mauritius for communicating, sharing life experiences, pictures, videos and even buying and selling stuffs. The most popular social media platforms used in the country are Facebook, Instagram, WhatsApp and TikTok. Professionals prefer LinkedIn for job postings and developing networks.

While the number of Mauritian users using social media has increased significantly, so is the number of cyber incidents on these platforms. In 2023, the top 5 most reported cyber threats on the MAUCORS are social media threats, with 21 % as online harassment, followed by 22% as scam and frauds and hacking with 21%. Identity theft and offensive content also join the league of top most reported type of cyber. These cyber threats have become worrying trends in Mauritius.

Top 5 Most Reported Incidents – Social Media based threats

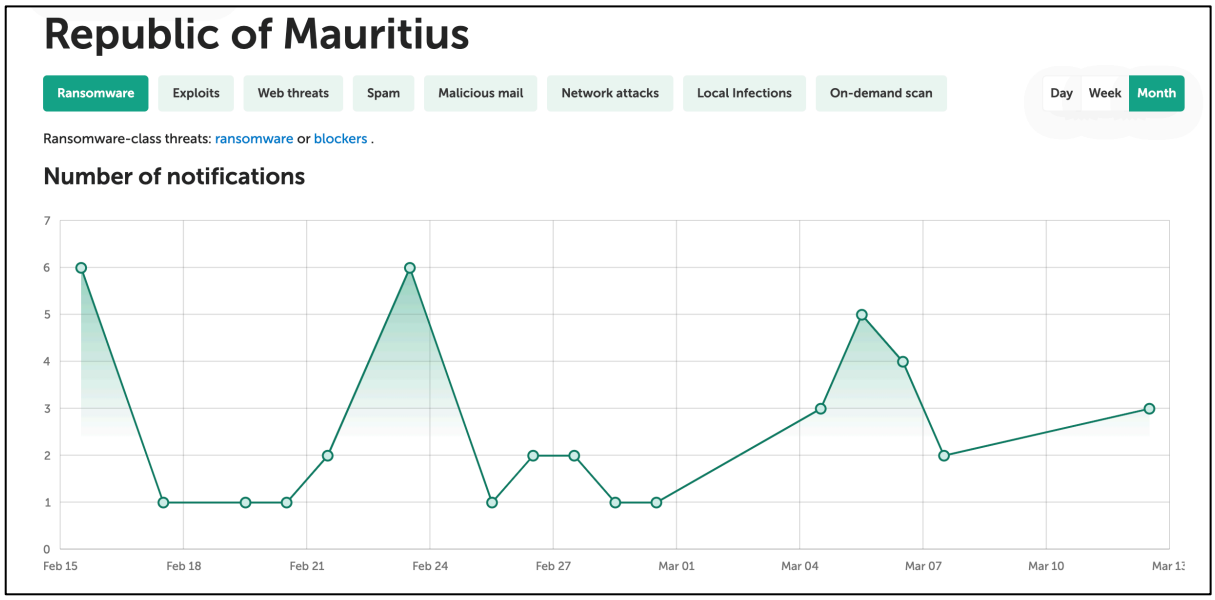


2. Ransomware

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 2023, only 10 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 2024 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.

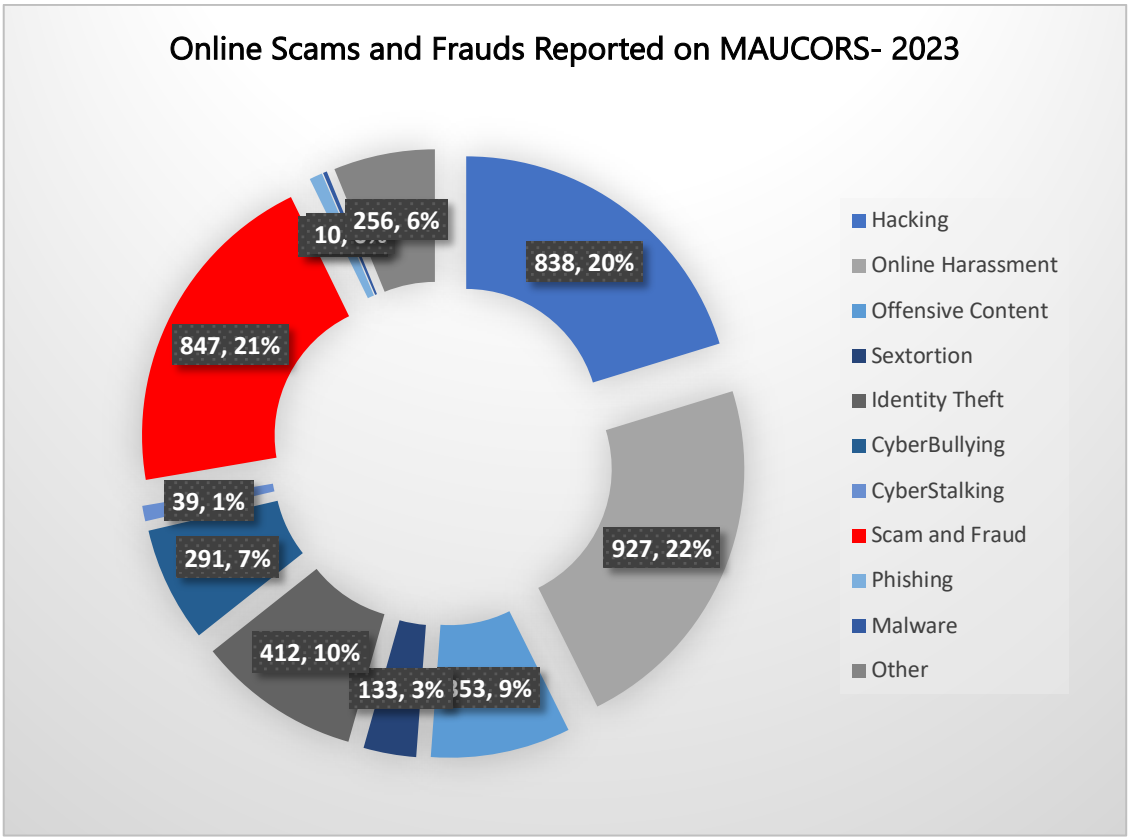
3. Online Scams and Frauds

Since the COVID-19 pandemic, Mauritius has been witnessing a rise in the number of incidents related to online scams and frauds. Individuals, both young professionals and retirees, are falling victim to cybercriminals, losing significant sums of money. The promise of quick financial gains has lured many into the web of deception. Moreover, scammers are becoming increasingly sophisticated with their tactics in order to gain trust. Previously used tactics such as winning lottery are no longer used.

The trend now is that younger and more educated individuals are falling for scams in which scammers build trust with their victims first before cheating them in fraudulent investment schemes. Such scammers target users on online chat groups or dating apps, and groom them over months, giving them profits from the first few investments to appear genuine. But eventually, victims wind up losing thousands by pouring more

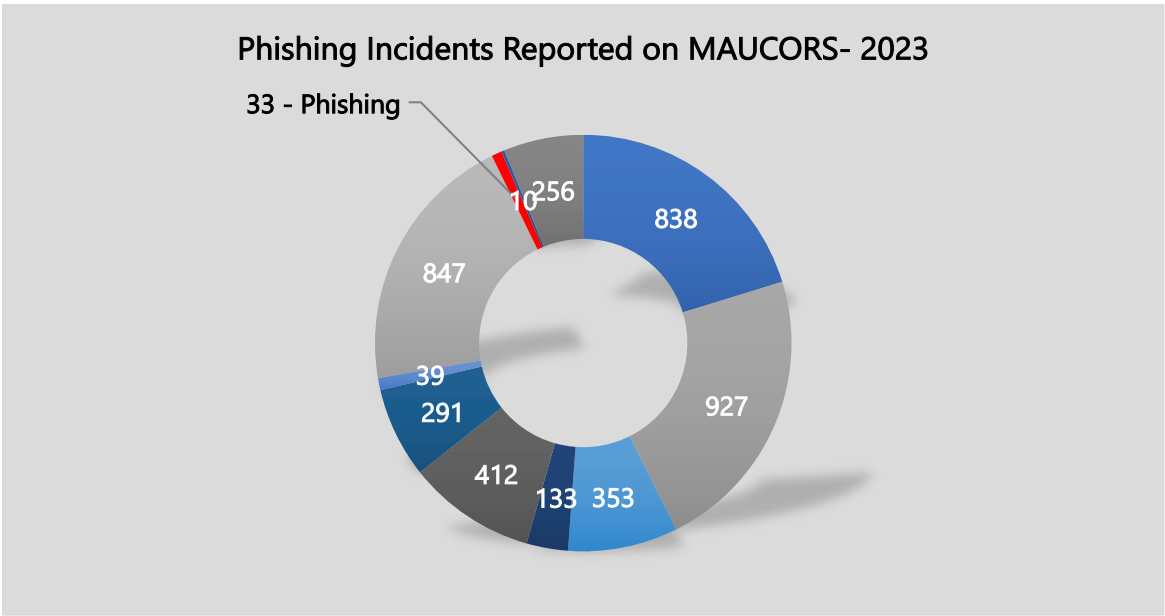
and more money into the bogus scheme – and the scammer disappears once victims realise they have been duped.

Mauritius is also facing the same issues where citizens have fallen for different types of scams, which have resulted in transfer of money. Examples of these scams are described below:



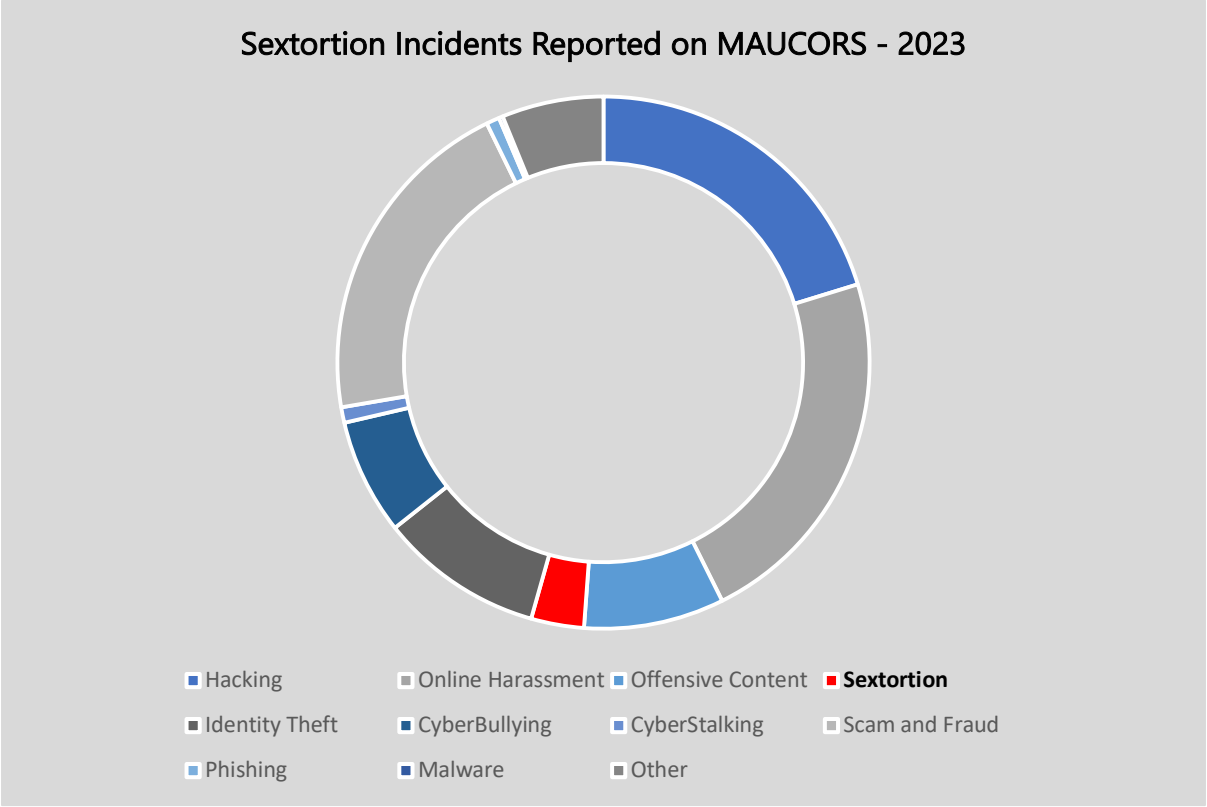
4. Phishing

33 phishing cases were reported on MAUCORS in 2023, whereby most of the phishing links were taken down by CERT-MU. The majority of incidents consisted of attacks that were sent via email. Some of the phishing incidents consisted of messages pretending to be from trusted entities. The victims were requested to user to perform certain actions such as installing a malicious file, clicking a malicious link, or divulging sensitive information. The phishing emails use a sense of urgency, or a threat, to cause a user to comply quickly without checking the source or authenticity of the email.



5. Sextortion

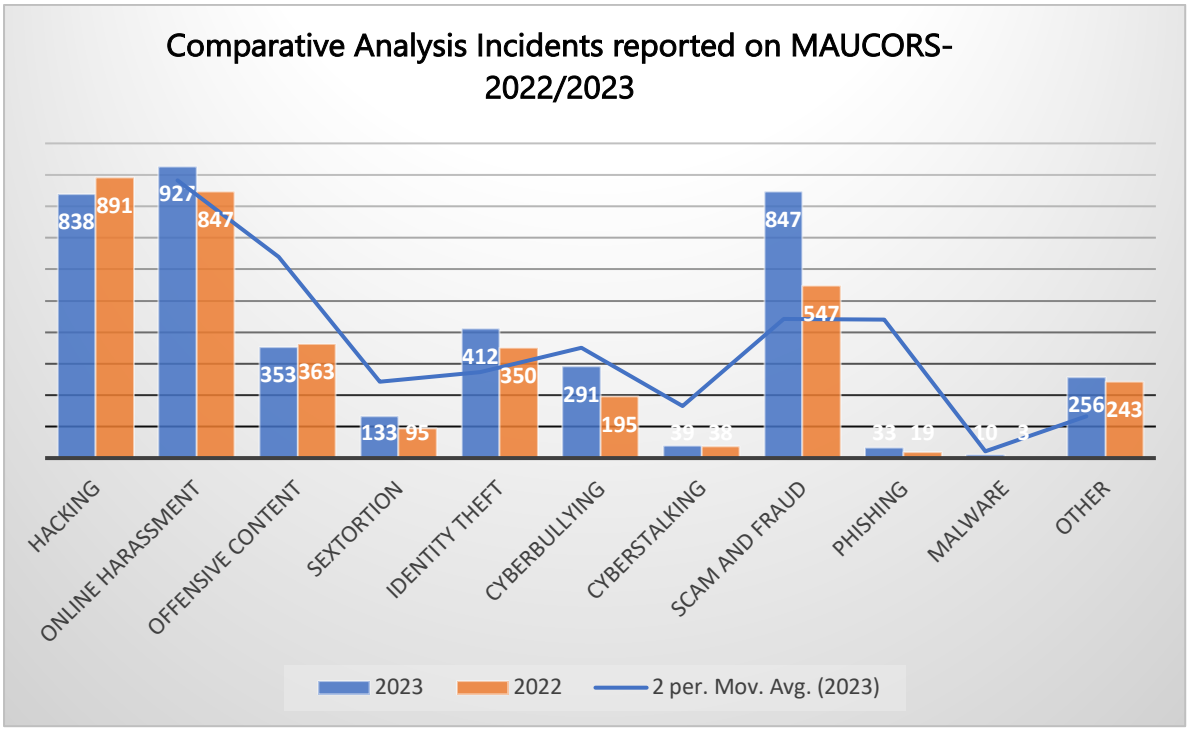
Sextortion is another type of cybercrime which were reported on MAUCORS. Sextortion occurs when an online predator tricks someone into giving them nude images or videos, and then demands money, more images, or makes other demands such as threatening to share the images with the victim's friends and family if they do not comply. More than 100 sextortion incidents were registered on MAUCORS in 2023. An increase of 10 % also is noted as compared to 2022. It is also to be noted that both female and male users became victims of sextortion.



Comparative Analysis: 2022 and 2023

1. Comparative Analysis - Number of Incidents Reported on MAUCORS for 2023 and 2022

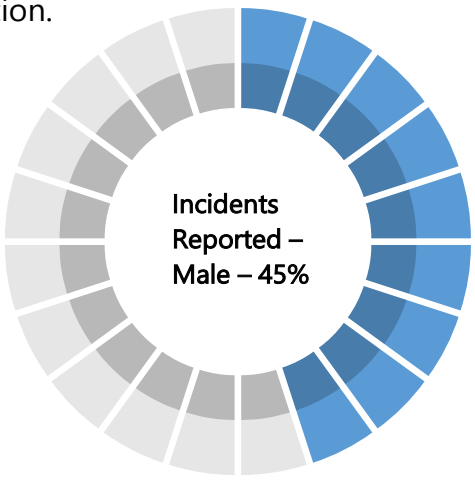
A comparative analysis was made for 2023 and 2022 with regards to the types of incidents reported and their attack vectors. It was noted that for some types of incidents, the number of reports has decreased such as hacking and offensive content. However, we have also seen a significant increase in incidents regarding scams and online fraud. This has become one of the major cyber threats affecting Mauritians.

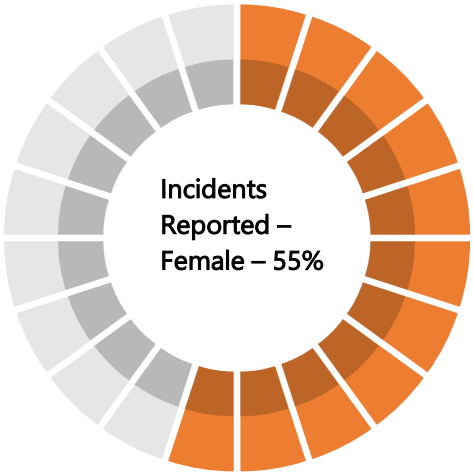


2. List of Incidents Reported by Gender

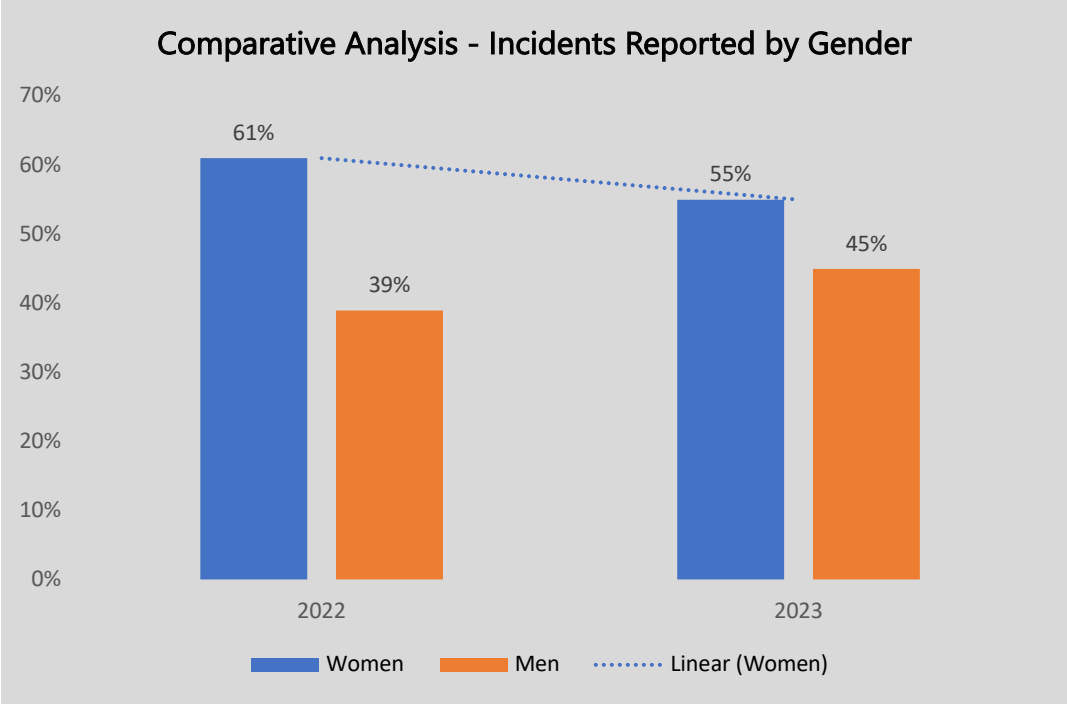
Digital platforms have often been celebrated for allowing equal opportunities for public self-expression, regardless of one's identity and status. Yet, not everyone is welcomed in the cyberspace. The digital arena has become a breeding ground for a range of exclusionary and violent discourses and beliefs, expressed and disseminated in a context of anonymity and impunity. Both women and men can be victims of cyber violence.

Based on the incident statistics reported on MAUCORS for the year 2023, it is to be noted that 55% incidents were reported by women as compared to men with a percentage of 45%. The type of incidents which were reported by women are mostly online harassment, cyber bullying, revenge pornography, online scams and frauds and sextortion.





However, a decrease of 6% has been noted in the number of incidents reported by women in 2023 as compared to the year 2022. CERT-MU has also observed a rise of incidents reported by men.



Cybersecurity Predictions 2024 - New Trends and Attacks

In 2023, we have seen the AI boom and how organisations are quickly integrating this new technology into their existing processes. Well, the cybersecurity world has not been left behind either. Organizations are incorporating AI models into their anti-malware systems and leveraging extensive vulnerability data to streamline operations and minimize manual efforts. As we anticipate continued innovation in 2024, it is crucial to acknowledge that threat actors are also keeping pace with this rapid evolution, emphasizing the ongoing need for vigilance and adaptive security measures. In this context, it becomes imperative to anticipate the top cybersecurity trends that will shape the narrative in 2024.

1. Attacks Against Cloud Services

Over the past few years, there has been a significant migration of business data, processes, and infrastructure to cloud computing. The advantages are clear: faster time-to-market, increased productivity, cost reduction, and improved flexibility. In

2023, Gartner predicted that public spending on cloud services will grow by a staggering 20.7%, reaching a remarkable $600 billion. However, this shift is not without its challenges.

Cybersecurity experts predict that cloud-based threats such as reduced visibility and control, misconfigured cloud storage and settings, vulnerable cloud applications, incomplete data deletion, compliance issues, and migration concerns will continue to impact businesses.

It is therefore important for organizations to implement security measures to safeguard their critical data in the face of attacks on cloud services. The key to success lies in implementing a mature and streamlined cloud governance model, which can significantly accelerate their security response capabilities.

2. Evolution of Phishing Attacks

Phishing attacks have long been a persistent threat in the cybersecurity world, and it is expected that this year, in 2024, they continue to evolve in sophistication and effectiveness. Modern phishing attacks have become adept at bypassing traditional security measures, using more personalized and technically advanced tactics to deceive users. In the face of these advanced phishing attacks, robust authentication systems are key to enhancing security. It is also important to sensitise users about phishing attacks so that they can protect themselves against such attacks.

3. Ransomware Attacks

It is expected that ransomware attacks will become more common and easier for threat actors to launch. This increase will result in a greater impact on organizations of all sizes. Ransomware defense, remediation, and recovery plans should be on every business leader's radar.

4. AI and Machine Learning

AI and Machine Learning (ML) have rapidly brought massive changes to the community. However, these technologies have raised many challenges as well. These technologies will be used to react to rapid malware development, deepfakes, privacy concerns, and advanced social engineering. Moreover, as AI becomes more integrated into the daily operations, security leaders will need to become knowledgeable about

frameworks, such as the NIST Artificial Intelligence Risk Management Framework (AI-RMF), that can help them identify and evaluate risks of AI to their operations.

Security leaders will have to work to prevent proprietary data from being fed into public AI engines. Cyber hygiene, robust controls, and thorough evaluation mechanisms around AI will be required to limit this unintentional risk exposure.

5. Enhanced Focus on Mobile Security

As mobile devices become increasingly integral to both personal and professional life, the focus on mobile security must be intensified. The enhanced reliance on mobile devices for various tasks, including remote work, financial transactions, and personal communications, makes them attractive targets for cyber threats. It is expected that cyber threats affecting mobile devices will increase and become more sophisticated. Organisations and citizens should employ security measures to protect sensitive information stored on and transmitted by laptops, smartphones, tablets, wearables, and other portable devices. At the root of mobile device security is the goal of keeping unauthorized users from accessing the device or enterprise network.

6. Increasing Threat of Deepfakes

Deepfake technology, which involves manipulating audio and video to create realistic but fabricated content, is a rising concern. Deepfakes can be used for social engineering attacks, impersonating individuals, and spreading disinformation. As the threat of deepfakes grows, organizations will need to invest in deepfake detection tools and strategies to protect their reputation and data integrity. Awareness and education are key in countering this emerging threat.

7. Cybersecurity Skills Gap and Education

The cybersecurity sector continues to deal with a significant challenge: the skills gap. As cyber threats become more sophisticated, the demand for skilled cybersecurity professionals' surges. However, there is a noticeable shortage of individuals equipped with the necessary skills and knowledge to effectively combat these evolving threats. This gap poses a risk not only to individual organizations but also to global cyber infrastructure.

It is therefore important to address this issue by offering specialised degrees and certifications designed to equip students with the latest knowledge and skills in cyber

security. These programs increasingly focus on practical, hands-on training, preparing students for the real-world challenges they will face in the world of cyber.

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 2024, 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. Current State Assessment

To stay ahead of cyber threats, 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. Proactive Measures and Effective Incident Response

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.

3. Employee 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.

4. Continuous Improvement and Adaptation

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

In the face of a rapidly evolving threat landscape, defending against cyber threats demands constant vigilance and adaptation. Organisations and individuals must stay up to date with emerging threats and refine their defense strategies accordingly. The collaboration of technology, education, and proactive planning form the foundation of a robust cyber defense.

Countering cyber threats necessitates a multi-pronged approach that encompasses diverse strategies. From thwarting phishing attacks to mitigating the impact of ransomware incidents, the key lies in educating users, implementing advanced security measures, and preparing for effective incident response. In this age of digital interconnectedness, safeguarding against cyber threats is not just a responsibility but a crucial imperative to protect sensitive information, preserve operational integrity, and maintain trust in digital interactions.

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