CSEAN

CYBER SECURITY EXPERTS ASSOCIATION OF NIGERIA

National Cyber Threat Forecast 2024

DECEMBER 2023

About CSEAN

Cyber Security Experts of Nigeria (CSEAN) was established as an advocacy group on all matters and challenges faced by information security in Nigeria to be an enabler focused on improving the standards and practices of information security in the country. CSEAN is a non-profit organisation centered on a collective purpose and vision to be a vehicle championing the cause and awareness of Information security best practices, acting as an agent of change to address cybercrime phenomena through engaging intellectual minds, business, and political leaders. As cybersecurity protagonists, we look to hold a healthy debate to expand the audiences' knowledge, awareness, and understanding of cyber-crime issues. Through workshops and seminars, we wish to share knowledge and grow the information security industry in the country while creating youth forums to breed future generations of information security professionals and to hold broader discussions with government officials on tackling cybercrime.

Authors

Oluwafemi Osho
John Odumesi
Hamzat Lateef
Olajumoke Oloyede
Jonathan Ayodele

Contact

For further inquiries, please contact CSEAN's Director of Research and Development at rd@csean.org.ng.

Legal Notice

This publication reflects the views and interpretations of CSEAN unless stated otherwise. It is not intended as a legal action on the part of CSEAN. CSEAN reserves the right to update this publication from time to time. External sources used in the report are referenced as appropriate, and CSEAN is not responsible for the content of such sources. This publication is provided for informational purposes only and must be accessed free of charge. CSEAN and any person acting on its behalf are not responsible for any use of the information contained in this publication.

Copyright Notice

Introduction

In 2023, the global landscape witnessed a substantial rise in cyber-attacks, with notable incidents involving Ransomware, Credential and Information stealer malware, and website defacement. Nigeria, like many other countries, faced its share of these challenges. Drawing insights from diverse sources, including cyber threat reports and incident analyses, we present a forecast for 2024.

This forecast considers various factors that will influence the cybersecurity landscape, encompassing current economic conditions, transparency issues, negligence at both individual and organisational levels, and insufficient adherence to security practices in private and public sectors. Others include limited information sharing on cybersecurity incidents, reliance on outdated computing resources, a prevalent absence of incident response plans in numerous organisations, and a shortage of cybersecurity experts. The evolving threats and trends in cyberspace further contribute to the complex scenario we anticipate in the upcoming year.

The Menace of Mis/Disinformation will Persist

As predicted in our Nigeria cyber threat forecast for 2023[1], Nigeria experienced a deluge of fake news in the periods leading up to and during the 2023 general elections[1,2]. In 2014, the persistent issue of misinformation and disinformation is expected to continue. These deceptive practices have become a common strategy among politicians to influence public opinion and manipulate electoral outcomes. The ease of spreading false information through digital platforms, mainly social media, makes it a prevalent issue that extends beyond politics, impacting social stability and national security.

The forecast highlights the crucial need for individuals to remain vigilant and critically evaluate information. The ability to discern between genuine and misleading content is essential in combating the influence of fake news.

Moreover, the role of social media platforms and government agencies is essential in addressing this challenge. Practical measures, including stringent fact-checking, public education campaigns, and regulatory actions, are necessary to curb the spread of false information. These efforts require collaboration between individuals, tech companies, and governmental bodies to ensure a well-informed public and a secure digital environment in Nigeria.

There Will be a Surge in Ransomware Attacks

In 2023, the cybersecurity sector in Nigeria experienced a dramatic rise in ransomware attacks, establishing it as the primary cyber threat of the year. This increase was fueled by the widespread availability of ransomware-as-a-service, which allowed even those with minimal technical expertise to launch sophisticated cyberattacks. Various ransomware groups and variants, such as ALPHV, 0XXX Virus, DJVU, and the Cobalt Strike exploit toolkit, were active, highlighting the diversity and complexity of these attacks[4,5]. These ransomware campaigns affected the public and private sectors, leading to significant financial losses in the billions of Naira, primarily due to operational disruptions and costly recovery efforts. Factors like the use of outdated or unpatched software and systems, reliance on cracked software, insufficient proactive monitoring, and unaddressed security vulnerabilities contributed to the success of these attacks.

For 2024, the forecast indicates an increase in ransomware attacks in Nigeria, impacting both public and private entities. The accessibility of ransomware-as-a-service and the success of previous campaigns suggest a persistent and growing threat[6]. To mitigate this, organisations are urged to update software and systems regularly, avoid unauthorised software, implement strong monitoring practices, and swiftly patch security flaws. Adopting these proactive cybersecurity measures is essential to lessen the anticipated impact of the expected surge in ransomware attacks.

[1] https://cybersecurenigeria.org/wp-content/uploads/2023/07/CSEAN-Cyber-Threat-Forecast-2023.pdf

[2] https://www.bbc.com/news/world-africa-66647768

[3] https://www.aljazeera.com/features/2023/2/15/nigeria-election-triggers-deluge-of-fake-news-on-social-media

Many Government's Online Assets will Continue to be Vulnerable to Common Exploits

The vulnerability of many Nigerian government online assets to common exploits is expected to persist in 2024, continuing the trend observed in 2023. Last year, numerous public organisations in Nigeria were found to be operating Internet-facing servers with known vulnerabilities, particularly those with legacy systems. The availability of public exploit code for these vulnerabilities makes them attractive targets for threat actors, often serving as initial entry points for malicious attacks. This vulnerability was highlighted by incidents such as a notable regulatory agency falling victim to Mallox ransomware, exploiting a Microsoft vulnerability in their public-facing digital systems.

To mitigate these threats, government entities must implement several countermeasures. Firstly, updating and upgrading legacy servers to more secure and modern systems is essential. Regularly patching known vulnerabilities is also critical to prevent malicious actors' exploitation. Additionally, implementing robust cybersecurity protocols, including proactive monitoring and intrusion detection systems, can significantly reduce the risk of successful cyberattacks. Adopting these measures will be vital in securing government online assets against the prevalent threat of common exploits in 2024.

There is a Rising Potential For Crypto Scams

With the Central Bank of Nigeria (CBN) lifting restrictions on banks facilitating cryptocurrency transactions[7], 2024 is poised to be a pivotal year for the crypto landscape in Nigeria. This decision opens the door for an influx of cryptocurrency service providers, significantly increasing market accessibility. However, this development also sets the stage for a potential rise in crypto scams.

Nigeria's position as the country with the most cryptocurrency-aware population, as revealed by the Consensys and YouGov Global survey, coupled with 90% of Nigerian respondents planning to invest in cryptocurrencies within the next 12 months[8], highlights an enthusiastic and rapidly growing investor base. While positive for the crypto market's growth, this enthusiasm also presents lucrative opportunities for scammers. Inexperienced and new investors eager to participate in the burgeoning crypto economy might fall prey to sophisticated scams, including fraudulent ICOs, Ponzi schemes, and phishing attacks

The combination of heightened market accessibility, a large, eager investor base, and the complexities in effectively regulating and monitoring crypto transactions creates an environment ripe for the proliferation of crypto scams in Nigeria. This situation necessitates urgent and concerted efforts to implement robust educational campaigns, enhance security measures, and establish vigilant regulatory frameworks. The focus must be on protecting investors and maintaining the integrity of Nigeria's rapidly evolving crypto market.

[4] https://nairametrics.com/2022/04/07/bet9jas-website-allegedly-hacked-by-russian-blackcat-group/

[5] https://twitter.com/RBiakpara/status/1680546604443488256

[6] https://www.forbes.com/sites/forbesbusinesscouncil/2023/12/18/the-rise-of-ransomware-as-a-service-raas-and-implications-for-business-security/?sh=331805c66621

More Benefit and Employment Scams

In 2024, Nigeria can be expected to witness a surge in employment and benefit scams, a trend that has been prevalent in 2023. The last quarter of 2023 saw the Nigerian military issuing warnings against fake online job recruiters who scammed people through advertisements of fraudulent recruitment exercises[9]. These scams often lure victims with promises of financial inducements and part-time job offers, primarily disseminated through various digital platforms[10].

The anticipated increase in these scams in 2024 can be attributed to Nigeria's challenging economic situation, which may drive more individuals to seek financial opportunities online.

Several measures are crucial to counter this rising threat. These include public awareness campaigns, improved monitoring and vetting by digital platforms, law enforcement collaboration for reporting and prosecution, and promoting safe job search practices with thorough recruiter verification and caution against sharing personal details or making payments.

Another Year of Information and Crendential Theft

Nigeria's cybersecurity arena, in 2023, experienced a dramatic increase in information and credential theft, marked by advanced malware attacks. These attacks, characterized by high sophistication, were a significant step up from previous challenges. Managed Security Service Providers (MSSPs) and Security Operations Centers (SOCs) encountered numerous cases involving potent malware variants like RedLine, Racoon, and Lumba, adept at evading traditional cybersecurity measures. The dark web also played a role, with stolen credentials from Nigerian platforms being sold for as low as $10[11], highlighting the ease and profitability of these cybercrimes.

The forecast for 2024 suggests a continuation and escalation of these threats, with sophisticated malware attacks expected to rise. The persistent evolution of cybercriminal tactics, especially in bypassing conventional security, indicates an impending wave of more complex information and credential theft incidents. This situation is exacerbated by the economic incentives for cybercriminals, evidenced by the thriving dark web market for stolen credentials.

A robust and comprehensive cybersecurity approach is crucial to counter this growing menace. This includes collaborative efforts in threat intelligence sharing and strengthening of digital defences, emphasizing the need for constant vigilance and proactive measures to combat the sophisticated strategies of cyber adversaries.

[7] https://cointelegraph.com/news/nigerian-exchanges-discouraged-by-sec-crypto-license-requirements

[8] https://consensys.io/blog/whats-the-most-crypto-savvy-country-in-the-world-hint-its-not-the-usa

[9] https://dailypost.ng/2023/09/01/nigerian-army-warns-public-against-fake-recruitment-online-scams/

[10] https://punchng.com/employment-scam-cybercriminals-spread-fake-alerts-fleece-desperate-jobseekers/

AI-powered Threats will be More Prevalent

While organisations in Nigeria are deploying AI in various ways, such as providing innovative solutions in healthcare[12], attackers are also employing AI technology to perpetrate more sophisticated and targeted cyber-attacks. This exploitation by cybercriminals presents a significant challenge.

We envisage an increase in the use of AI for malicious purposes in 2024. Attackers will leverage the capabilities of AI to enhance the efficiency and effectiveness of their cybercriminal activities. This will manifest in more personalized phishing attacks, personalized malware, automated large-scale attacks, and sophisticated social engineering attacks.

To mitigate AI exploitation for cybercrimes, individuals should stay informed and practice cybersecurity hygiene. Organisations must invest in AI-driven security solutions and staff training. Governments should enforce robust cyber laws, support research in AI security, and foster public-private partnerships for sharing intelligence and best practices in cybersecurity.

Individuals and Organisations Will Experience More Impersonation Scams

In 2024, Nigeria is poised to continue facing the challenge of impersonation scams. This trend gained prominence in 2023 with notable cases like the impersonation of the Director General of the National Automotive Design and Development Council (NADDC)[13] and PwC Nigeria[14]. These scams involve creating fake websites and social media profiles, using the names and images of well-known figures to deceive the public.

Public awareness campaigns and educating people on recognizing and reporting such scams are crucial to combating impersonation scams. Social media platforms and websites must enforce stricter verification processes for profiles claiming organisational or individual identities. Additionally, collaboration with law enforcement will be vital in addressing and legally pursuing these frauds.

Organisations must regularly monitor their online presence and encourage public reporting of suspicious activities. Implementing robust cybersecurity measures will also be vital in protecting against these threats. By integrating these strategies, Nigeria can effectively mitigate the risks of impersonation scams in 2024.

[11] Whitehat.NG, “Nigeria-Cyber-Incidents: https://github.com/ngwhitehat/Nigeria-Cyber-Incidents/tree/main

[12] https://www.mondaq.com/nigeria/new-technology/1309534/artificial-intelligence-ai-and-ai-attacks-in-nigeria-a-call-to-action-for-nigerian-policymakers

Insider Threat will Surge

Due to rising economic challenges, we predict Nigeria will face an upsurge in insider threats in 2024. Amid these economic hardships, cybercrime has become an increasingly attractive option, offering substantial illegal earnings.

Reports revealed that insider fraud cases in the financial sector, particularly, have increased in 2023[15,16]. Several instances of insider fraud, including executive-level involvement, were reported[17]. Employees with access to sensitive data and systems may view collusion with cybercriminals as a viable way to supplement their meager incomes.

Businesses and organisations must adopt various measures to combat this growing threat. These include increasing employee pay to better align with the cost of living, offering financial incentives for loyalty, conducting ethics training emphasizing cybersecurity responsibilities, monitoring employee behaviour, and implementing robust cybersecurity protocols like multifactor authentication.

Cyber Hacktivists will Likely be More Active

In light of the events of 2023, where Nigeria witnessed the disruptive force of cyber hacktivism following the coup d'état in Niger, it is highly likely that 2024 will see an increase in similar activities. The intervention of various African countries, including Nigeria, through ECOWAS, catalyzed the emergence of groups like "Anonymous Sudan." These hacktivists, driven by political and religious motives, have demonstrated their capacity to target critical infrastructure, such as major telecommunication providers in Nigeria[18].

To mitigate this escalating threat of cyber hacktivism in 2024, Nigeria must adopt a multi-faceted approach. Strengthening cybersecurity infrastructure is paramount. This involves investing in advanced security technologies and enhancing the capability of cybersecurity personnel. Additionally, there's a need for increased intelligence gathering and monitoring to identify and counter potential cyber hacktivist threats preemptively. Collaborative efforts between government, private sectors, and international bodies are essential to share knowledge and strategies effectively.

[13] https://citybusinessnews.com/naddc-raises-alarm-over-dgs-impersonation-fraud/

[14] https://www.pwc.com/ng/en/press-room/disclaimer-notice-impersonation-and-fraudulent-acts.html

[15] https://www.newsmart.com.ng/2018/03/fraud-cases-by-bank-staff-rises-ndic.html

[16] https://www.google.com/url?q=https://nairametrics.com/2023/01/17/nigerian-bank-workers-involvement-in-frauds-is-on-the-rise-report-shows/&sa=D&source=docs&ust=1704103296536440&usg=AOvVaw3MLXyHpsd3uMsMBC9nfMXS

[17] https://punchng.com/banks-sack-110-top-executives-others-over-n82bn-fraud/

There will be a Rising Tide of Website Defacement

The cybersecurity landscape in Nigeria in the year 2023 witnessed a significant surge in web defacement attacks, affecting various sectors, including over a hundred government (.gov.ng) websites. Educational institutions were particularly hard hit[19], marking a notable shift in attackers' focus from primarily government targets to broader sectors. This trend indicates a growing sophistication among cyber adversaries, not just defacing websites for ideological reasons but potentially seeking access to sensitive data.

Looking ahead to 2024, the forecast suggests an escalation in the severity and frequency of web defacement incidents, affecting a diverse range of industries. The high incidence of attacks on academic institutions highlights the urgent need for all sectors, especially education, to reassess and bolster their cybersecurity measures.

The upcoming year demands a proactive and comprehensive approach to cybersecurity, emphasizing the importance of strengthening protocols, adopting advanced technologies, and cultivating a vigilant cybersecurity culture. This approach is critical for businesses, healthcare organisations, educational institutions, and government entities to protect their digital assets and counter the evolving strategies of cyber adversaries in the face of increasing web defacement risks.

[18] https://punchng.com/coup-pro-niger-hackers-back-junta-attack-mtn-nigeria/

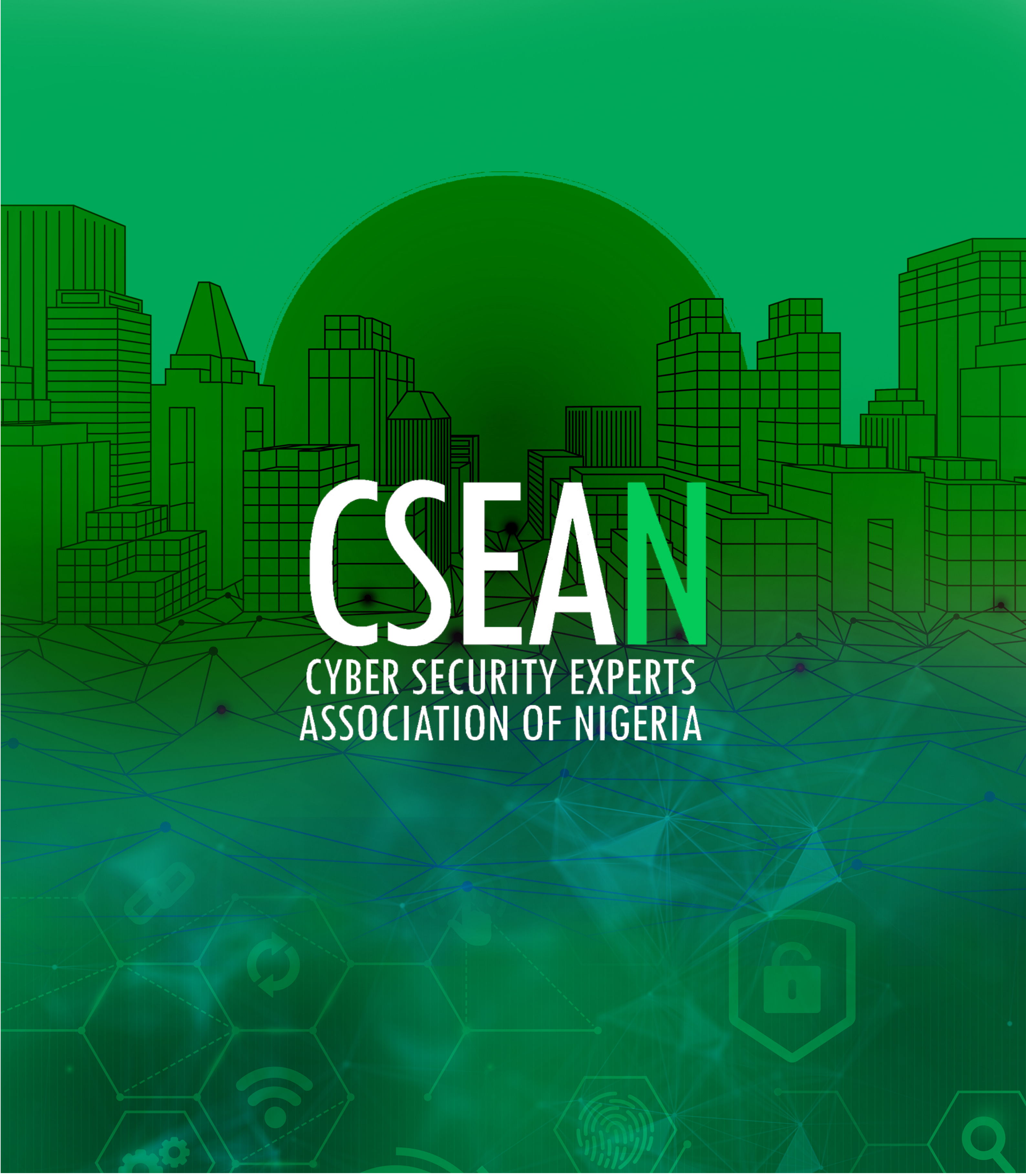
[19] https://www.premiumtimesng.com/news/top-news/589716-management-apologises-as-hackers-upload-porn-videos-on-babcock-university-website.html

Conclusion

As we reflect on the dynamic cybersecurity landscape of 2023 and look forward to the challenges and opportunities in 2024, several key themes emerge. The prevalence of cyberthreats underscores the evolving tactics of cyber adversaries. The year 2023 witnessed a notable shift, thus serving as a wake-up call for robust cybersecurity measures. In anticipating the road ahead, the forecast for 2024 points to a continued surge in Mis/disinformation, ransomware attacks, attacks against vulnerable government's online assets, crypto scams, benefit and employment scams, information and credential theft, AI-enabled threats, impersonation scams, insider threats, cyber hacktivism, and web defacement.

Addressing the complex cybersecurity challenges necessitates a proactive and comprehensive approach, considering factors such as economic conditions, transparency levels, and the diligence demonstrated by individuals and organisations. Collaboration between public and private sectors, the adoption of updated computing resources, and a commitment to cybersecurity best practices are imperative.

In essence, the evolving digital threats demand a united front. Organisations, irrespective of sector, must strengthen their defences, invest in cutting-edge technologies, and prioritize education to mitigate vulnerabilities. As we navigate the uncertainties of the upcoming year, a shared commitment to cybersecurity resilience will be the cornerstone of a secure and resilient digital future.



Learn more at www.csean.org.ng

CSEAN
Suite C4, HCR Plaza
521 Sylvester U. Ugoh Crescent,
Jabi, Abuja, Nigeria
info@csean.org.ng