

Navigating the Cybersecurity Landscape 2024

Trends, challenges, and strategies for the year ahead

ENFOCOM CYBER

Table of Content

01 Introduction

02 Current Threat Landscape

04 Strategies for 2024

06 Cybersecurity Workforce Gap

07 Information Sharing & Collaboration

08 Conclusion



The Cybersecurity Landscape in 2024

From the continuous transformative influence of Artificial Intelligence (AI) to the relentless stream of targeted cyberattacks, going into 2024, the cybersecurity landscape is filled with challenges and opportunities.

- **A**rtificial Intelligence, especially a subset of AI in Machine Learning models, saw explosive growth in the marketshare of cybersecurity in 2023. As we look forward to 2024, we expect AI to play a pivotal role in the rise of cyber criminal capabilities, as well as fortifying defences and predicting cyber threats before they materialize.

- **C**loud environments provide a great deal of flexibility, but they also bring with them several security challenges. By 2024, cloud security will be a top priority for organizations as they secure multi-cloud and hybrid environments.

- **Z**ero-Trust security models are expected to gain momentum in 2024 and beyond, with many organizations moving beyond traditional perimeter-based defence.

30,000+

Common Vulnerabilities & Exploits reported in 2023

459

March 2023

New record for number of reported Ransomware attacks in a month period

Ransomware is expected to become even more sophisticated in the coming years. In 2024, we anticipate more advanced Ransomware-as-a-Service (RaaS) models, double extortion techniques, and an increased focus on targeting critical infrastructure and businesses.

Current Threat Landscape

As 2023 comes to a close, we want to highlight the most significant cybersecurity threats we see affecting our customers

Sophisticated Phishing Campaigns

Phishing is still a highly effective method for infiltrating organizations, and it has become even more sophisticated with the help of AI. The use of AI generated scripts and targeted messages has resulted in a staggering 1,265% increase in successful phishing attacks during the last quarter of 2022.[1]

The use of Large Language Models by threat actors has enabled the creation of highly personalized messages and automated phishing campaigns that are becoming more convincing and difficult to detect. Consequently, even well-trained users are often misled and persuaded to compromise sensitive information, underscoring the need for heightened user awareness and robust email security measures.

Ransomware Rampant

The epidemic of ransomware has spread rapidly since its inception in 1989 with the AIDS trojan. In the last five years, it has affected over 72% of businesses worldwide.[2] Ransomware has become an increasingly insidious and profitable business model for cybercriminals. The advent of Ransomware-as-a-Service (RaaS) platforms has made it easier for non-technical actors to participate in ransomware attacks.

In 2023, there was a significant increase in double extortion tactics, where threat actors not only encrypt data but also threaten to release sensitive information unless a ransom is paid. To mitigate ransomware incidents, organizations must implement strong data loss prevention strategies, including regular data backup, employee cybersecurity training, and effective software toolsets.

Supply Chain Vulnerabilities

The digital ecosystem of today is highly dependent on third-party suppliers, which has created a complex and interconnected network. Unfortunately, this has also led to an increase in supply chain attacks, posing a significant threat to organizations.

In a report by *Sonatype*, it was found that there were 2.1 billion open-source downloads with vulnerabilities known in 2023.[3] This creates a larger attack surface for threat actors to exploit vulnerabilities higher up in the supply chain, often targeting third-party vendors with weaker security postures. These attacks can affect the entire ecosystem, emphasizing the importance of implementing comprehensive supply chain risk management and mitigation strategies to ensure the security of organizations.

[1] https://slashnext.com/wp-content/uploads/2023/10/SlashNext-The-State-of-Phishing-Report-2023.pdf
[2] https://www.sangfor.com/blog/cybersecurity/list-of-top-ransomware-attacks-in-2023
[3] https://www.sonatype.com/en/press-releases/sonatype-9th-annual-state-of-the-software-supply-chain-report

Zero-Day Exploits & Advanced Persistent Threats

The proliferation of cyber threats, including zero-day exploits and Advanced Persistent Threats (APTs), remains a top priority for major organizations and operators of critical infrastructure.

As per a report[4] from EMSISOFT, the MOVEit vulnerability, which has affected a staggering 93 million individuals, has resulted in 2,730 successful cyberattacks as of January 2024. This alarming figure highlights the grave consequences that can arise from a single vulnerability, underscoring the need for robust cybersecurity measures in today's digital landscape. With Cybercrime as a Service (CaaS) becoming more prominent, even less technically sophisticated threat actors now have access to the latest tools and methods, so organizations must remain vigilant.

In today's cybersecurity landscape, it's crucial for organizations to establish a robust security culture that values proactive and comprehensive measures, in addition to enhancing their defensive capabilities.

Organizations must implement rapid incident response mechanisms and the encouragement of collaborative efforts among industry peers. Given the escalating nature of the cyber threats, it is crucial for organizations to exercise prudent and timely action. Thus, it is essential for organizations to constantly adapt, innovate, and reinforce their cybersecurity strategies to remain ahead of the curve.

[4] https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/



Strategies for 2024

Key strategies for a resilient cybersecurity posture in 2024.

AI-Enhanced Threat Detection and Response

It is crucial for organizations to prioritize the integration of artificial intelligence (AI) into their existing security infrastructure. This will fortify their capabilities in detecting and responding to potential threats. The current ease of implementation of AI-driven solutions has made it more feasible to analyze vast datasets, identify anomalies, and predict potential cyber threats before they materialize. The integration of continuous monitoring and real-time analysis has become a critical component in the utilization of AI-enhanced threat detection and response, which is essential in staying ahead of evolving attack vectors.

Supply Chain Risk Management

It is highly recommended that organizations adopt a comprehensive and collaborative approach to managing supply chain risks. This involves conducting a thorough evaluation of third-party vendors, assessing their security postures, and establishing mutually agreed-upon security requirements in contractual agreements. It is crucial to regularly audit and monitor the entire supply chain for vulnerabilities and potential threats, ensuring that security measures are aligned across the entire ecosystem.

Ransomware Resilience and Backup Strategies

The current technological landscape has seen a sharp increase in the threat of ransomware, necessitating the development and regular testing of comprehensive ransomware resilience strategies by organizations. Such strategies should include the implementation of effective backup solutions that ensure data integrity and availability in the event of a ransomware incident. Additionally, clear incident response protocols must be established to minimize downtime and data loss. Organizations at risk must prioritize the use of offline backups to prevent encryption by ransomware.

User-Centric Security Awareness Training

Organizations must prioritize comprehensive and ongoing security awareness training programs, recognizing that users often serve as the first line of defence, as well as a common entry point for threat actors. Equipping users with the knowledge to identify and report the continually evolving phishing attempts, social engineering tactics, and other common attack vectors is increasingly crucial. The growing portfolio of solutions that provide simulated phishing or tabletop exercises can assist in reinforcing security best practices and enhance user resilience.

Zero Trust Architecture Implementation

As the number of cybersecurity offerings in the market continues to increase, it is crucial for organizations to begin to embrace and implement the Zero-Trust model. While the idea of implementing Zero-Trust may seem daunting at first, it is important to note that even taking some initial steps, such as continuous verification, least privilege access, and micro-segmentation, can significantly improve an organization's cybersecurity posture. The Zero-Trust model is also an essential tool in mitigating the impact of potential risks such as insider threats and advanced persistent threats.

Collaborative Threat Intelligence

In today's ever-evolving cybersecurity landscape, it's crucial for organizations to come together and engage in collaborative efforts to share threat intelligence. By sharing information with other entities including industry groups and cybersecurity communities, we can bolster our collective defense capabilities and develop stronger immunity to threats. Timely sharing of threat intelligence allows us to stay ahead of emerging threats and proactively implement security measures to prevent falling prey to them.

As organizations navigate the complexities of the cybersecurity landscape in 2024, we hope that these strategies can serve as a compass, guiding organizations toward cyber resilience, agility, and a proactive stance against the evolving threat landscape. By adopting these strategies, organizations can position themselves not merely as reactive defenders but as proactive innovators and leaders in cybersecurity for the years ahead.

Going into 2024, we want to highlight the following two topics that we see as demanding heightened attention within the evolving landscape of business and technology:

CYBERSECURITY WORKFORCE GAP

3.1 million

global role/position shortage in cybersecurity

COLLABORATION & INFORMATION SHARING

612 CVEs

Common Vulnerabilities & Exploits reported in the first week of 2024

Cybersecurity Workforce Gap

As organizations traverse the intricacies of the cybersecurity landscape of 2024, the shortage of qualified cybersecurity professionals continues to be a critical hurdle toward cyber resiliency.

Promotion of Diversity and Inclusion

Recognizing the importance of diversity in cybersecurity is now as critical as ever. By fostering inclusivity organizations can tap into a broader talent pool, while diversity provides a diverse set of perspectives, assuring a wide knowledge and skill coverage and enhancing innovation. Organizations can take an extra step to rethink traditional recruitment practices and embrace innovative approaches to identify and attract talent. Consider non-traditional pathways, such as aptitude-based hiring and skills assessments. Creating an inclusive recruitment environment that values potential and a willingness to learn can also help to expand the available talent pool and help fill the workforce gap.

Strategic Integration of Artificial Intelligence

Strategic incorporation of AI solutions as part of organizational workflow has recently grown as a go-to solution to address the workforce gap in many fields, including cybersecurity. Organizations can leverage AI-driven tools to facilitate rapid cyber threat detection, mitigation, and innovation in cybersecurity. Additionally, introducing such tools into an organization can assist in reducing the load on the existing workforce and allow it to focus on more urgent matters at hand.

Collaboration with Industry Partners

It is now more critical than ever to forge partnerships with industry organizations, government agencies, and non-profits to address the cyber threats and the skills gap collectively. Pooling resources, sharing expertise, and collaborating on initiatives that promote cybersecurity allows for rapid cyber threat detection, and mitigation, as well as cybersecurity innovation and development. By working together, the cybersecurity community can amplify its impact and address and fill the cybersecurity gaps more effectively.

Focus on Ongoing Training & Education

The ongoing training and education of the existing workforce plays a pivotal role in fortifying defences and closing the skills gap. Recognizing the evolving nature of cyber threats and the growing workforce gap, organizations should invest in comprehensive training programs that equip their teams with the latest knowledge and skills. Leveraging skills-based exercises and virtual environments allows for training realistically and efficiently. By strategically integrating continuous training, organizations not only empower their existing workforce but also contribute to a more adaptive and proficient cybersecurity community overall.

Collaboration & Information Sharing

In a landscape where cyber actors are beginning to collaborate, share information and provide service to each other at never-before-seen scales, collaboration and information sharing emerge as the cornerstone of cyber resilience. By fostering alliances, participating in information-sharing platforms, and embracing collaborative practices, organizations can elevate their defences and collectively can hope to stand against the evolving collective threat of cyber adversaries.

Information Sharing Platforms

Active participation in information-sharing platforms and industry-specific threat intelligence-sharing communities offers the opportunity for organizations to offer their unique take on the current state of the cybersecurity landscape in their area and become cyber leaders in their respective industries. These platforms serve as hubs where organizations exchange real-time threat intelligence, indicators of compromise, situational awareness, and insights into potential future directions. Engaging in these forums enables rapid response to emerging threats and facilitates a more proactive state-of-the-art defence posture.

Incident Response Alliances

Establishing incident response alliances with peer organizations allows your organization, in the event of a cyber incident, to respond swiftly and in a coordinated manner. Such alliances, on top of providing collaborative incident response planning, also offer opportunities for joint tabletop exercises and simulations, ensuring a seamless exchange of information and resources during critical moments.

Conclusion

Organizations in 2024 face the growing convergence of AI and cybersecurity, the persistent threat of evolving cyberattacks, and the challenges posed by cloud environments. Adopting a strategic and comprehensive approach to cybersecurity is as critical as ever. Ransomware, supply chain vulnerabilities, and the ongoing risks of zero-day exploits demand growing urgency from organizations to fortify their defences, improve cybersecurity posture, and embrace the paradigm shift toward Zero-Trust security models.

The observed cybersecurity threats of 2023, ranging from AI-supported sophisticated phishing campaigns to rampant ransomware and supply chain vulnerabilities, emphasize the need for continuous adaptation and innovation. Recognizing the significance of user-centric security, organizations can bolster their readiness against evolving threats through user awareness training, establishing ransomware resilience strategies, and prioritizing supply chain risk management.

Looking forward, there are several strategies we outlined for 2024, including AI-enhanced threat detection, user-centric security training, ransomware resilience, supply chain risk management, and Zero-Trust architecture implementation. All of these strategies serve as a compass for organizations to navigate the evolving cybersecurity landscape. It is also critical to continuously improve collaboration and information sharing, thus providing a collective defence or “immunity” against emerging threats.

We come into 2024 with the ever-expanding cybersecurity workforce gap. To address the gap and reduce its effects on the organization, we propose to look towards collaborative efforts, promotion of diversity and inclusion, strategic integration of AI solutions, and an elevated focus on continuous training and education. By investing in these initiatives, organizations can ensure a continuously robust and adaptive cybersecurity team in their ranks.



ENFOCOM

ENFOCOM was founded in 1999 as a spin-off from General Dynamics Canada by Herbert Fensury and Senior Partners to provide clients with innovative solutions to complex cybersecurity challenges. With a rich history of projects supporting cybersecurity testing and research, ENFOCOM has emerged as a cybersecurity leader with current partners such as Raytheon Canada and the University of Calgary.

Our dedicated and trustworthy team of industry experts work diligently to place the needs of our clients first. The team's origins working for General Dynamics ensure our process follows long-standing defense & aviation military standards to this day.

At the leading edge of cybersecurity in Canada, the ENFOCOM Cyber Range provides a unique service that allows organizations to penetration test their critical infrastructure in a safe environment and allow their IT team to train without compromising their production environment.



GET IN TOUCH WITH US TO DISCUSS YOUR SECURITY

www.enfocomcyber.com

1-888-ENFOCOM (363-6266)

sales@enfocom.com