IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

What are the Top Cybersecurity Trends to Look Out for in 2024?

Johnny Carpenter

Johnny Carpenter
General Manager EMEA
11:11 Systems

Biography

Johnny Carpenter, General Manager of EMEA at 11:11 Systems (https://www.1111systems.com) has worked in IT, addressing network and cloud challenges, for nearly three decades. With a history of consistently delivering sound commercial judgement, Johnny has a reputation for acute market insight.

Joining iland (now 11:11 Systems) over a decade ago, Johnny's close relationships with other technical experts and customers across a wide range of industries have shaped his deep understanding of the trends, nuances and concerns around digital transformation strategies.

Johnny blogs at https://1111systems.com/blog/

Keywords Cybersecurity, Cybersecurity Trends, 11:11 Systems, 2024, Predictions, Ransomware, Data breached, Resilience, Cyber-attack, Network, Phishing, Generative AI (genAI)
Paper type Research

Abstract

Across the board, 2023 was a challenging year for IT security professionals. Regardless of organizational size, reports of ransomware attacks and data breaches dominated the headlines. A perfect storm of economic uncertainty, rapidly emerging technologies, fragmented regulations and ever-widening workforce and skills gaps continues to create huge uncertainty for a profession whose role it is to protect global infrastructure and systems from attack. The use of Artificial Intelligence (AI) in cybersecurity solutions can shape the future of cybersecurity, but with the cyber landscape ever changing, IT security professionals will need to stay focused if they are to protect their organizations from attack, says the author of this article.

Introduction

Many organizations are looking back on 2023 to try and gain some insight into what the next 12 months could hold. The past year has been particularly interesting in the world of cyber security, with ransomware and data breaches dominating the headlines, the rise to prominence of AI strengthening cybercrime's arsenal, and the shift of focus to cyber resilience causing businesses to question what comes next for the industry. For security professionals across organizations of all sizes we anticipate the following issues will be a key focus for the year ahead.

Increased focus on cyber resilience

With the reality that every organization will almost inevitably suffer a cyber-attack at some point, the ability to recover with the least amount of downtime and data loss will be a priority. Organizations are coming around to the harsh reality that focusing on cybersecurity that centres on preventing attacks is not infallible. The ability to quickly recover from an attack, while minimizing the impact on the organization will be a strategic objective.

Cyber skill shortage outpaces talent pool

The shortage of talent with the necessary knowledge and skills to protect organizations from cyber threats continues to be an ongoing concern. According to the 2023 ISC2 Cybersecurity Workforce Study[1], the cybersecurity workforce has grown by 8.7%, but the gap between the number of workers needed to the number of available openings grew 12.6% year-on-year. This indicates that growth in the number of cybersecurity roles is still outpacing talent pool growth.

According to research[1], 67% of respondents report that their organization has a shortage of cybersecurity staff needed to prevent and troubleshoot security issues, whilst 92% report having skills gaps in their organization – the most common being cloud computing security, AI/Machine Learning (AI/ML) and Zero Trust implementation.

Increasingly sophisticated phishing and social engineering attacks

Malicious actors will continue to up their game when it comes to manipulating users through social engineering. Generative Artificial Intelligence (genAI) enables these bad actors to carry out more intelligent and personalized phishing campaigns against their unwitting victims. In addition, deepfake technology is continuing to advance, making it increasingly more difficult to discern whether something such as an image or video is real.

Increased focus on cybersecurity by corporate boards

Cybersecurity is increasingly recognized as a business risk, becoming a strategic priority for organizations. Coupling this with the trend toward board members having explicit accountability for cybersecurity necessitates an increased focus by corporate boards. By 2026, Gartner predicts that 70% of boards will include one member with cybersecurity expertise[2].

Increased adoption of Zero Trust Frameworks through ZTNA and SASE

With the ever growing remote and mobile workforce, coupled with application sprawl across on prem, public cloud and SaaS, organizations are finding it hard to maintain secure, consistent, and performant policy across their remote users and applications.

Leveraging Zero Trust Network Access (ZTNA) and Secure Access Service Edge (SASE) allows an organization to extrapolate their access layer from their data centre, allowing users to ingress to the closest onramp wherever they are in the world. Through a single interface, organizations can granularly control application, network and internet access while enhancing security protection such as secure web gateway and browser isolation.

Couple the ability to prevent malicious scripts with the ability to onramp to clouds, enforce data loss prevention, and secure inbound application traffic through reverse proxy, web application firewall and DDoS protection, more companies will most likely be moving to centralized ZTNA and SASE designs in 2024.

Conclusion

Cybersecurity professionals worry about keeping their organizations safe during times of economic uncertainty but remain steadfastly focused on defending their organizations. As threat actors gear up to use the new technologies that are at their disposal, companies will need to explore ways to stay a step ahead while preparing to withstand potential breaches and attacks with minimal downtime.

Reference

[1] ISC2 Cybersecurity Workforce Study: Looking Deeper into the Workforce Gap (3 November 2023). ISC2. Available at: https://www.isc2.org/Insights/2023/11/ISC2-Cybersecurity-Workforce-Study-Looking-Deeper-into-the-Workforce-Gap

[2] Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024: Analysts Explore the Future of Cybersecurity at the Gartner Security & Risk Management Summit (28 March 2023). Gartner. Available at: https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024