HealthManagement
Promoting Management and Leadership

Gartner Identifies the Top Cybersecurity Trends for 2024

When it comes to cybersecurity, there's no single playbook to follow. However, looking to experts and analysts who spend their days laser-focused on the latest threats and trends can offer valuable direction. Generative AI (GenAI), unsecured employee behaviour, third-party risks, continuous threat exposure, boardroom communication gaps and identity-first approaches to security are the driving forces behind the top cybersecurity trends for 2024, according to Gartner, Inc. 2024 will see security leaders respond to the combined impact of these forces by adopting a range of practices, technical capabilities and structural reforms within their security programmes to improve organisational resilience and the cybersecurity function's performance. Gartner has identified its six top cybersecurity trends for the year, which healthcare leaders should consider.

Continuous Threat Exposure Management Programs Gain Momentum.

Gartner predicts that organisations prioritising security investments through Continuous Threat Exposure Management (CTEM) programs will experience a two-thirds reduction in breaches by 2026. CTEM is an approach aimed at managing vulnerabilities and exposures to defend organisations effectively in the face of rapid changes in the threat landscape. This strategy is particularly relevant in the healthcare sector, where breaches can have significant financial implications and even threaten lives, yet CTEM programs are not widely adopted.

CTEM represents a departure from traditional reactive approaches to cybersecurity, such as Security Information and Event Management (SIEM) and endpoint security solutions. Instead, it focuses on proactively identifying and mitigating potential threats before malicious actors can exploit them. By continuously scanning for vulnerabilities and exposures, organisations can gain a comprehensive understanding of their security posture and prioritise remediation efforts accordingly.

Critical components of a CTEM program include continuous external scanning, penetration tests, vulnerability scans, and third-party supply chain scans. These activities help organisations identify potential vulnerabilities and exposures across their infrastructure, applications, and third-party relationships. Once identified, organisations can prioritise and remediate these exposures, thereby reducing their attack surface and minimising the risk of breaches.

The success of a CTEM program hinges on consistent and ongoing testing and scanning, as the threat landscape is constantly evolving. Point-in-time assessments are insufficient, as new code, systems, and technologies are continually introduced into production environments, necessitating regular reassessment and remediation. By adopting a CTEM approach, organisations can proactively manage their security risks and enhance their resilience against cyber threats.

Cybersecurity Outcome-Driven Metrics: Bridging Boardroom Communication Gap

Gartner highlights the increasing adoption of Outcome-driven Metrics (ODMs) in cybersecurity, which serve as a vital tool for establishing a clear connection between cybersecurity investments and the level of protection they deliver. This becomes particularly pertinent when conveying complex technical concepts to executive leaders and the board, who may lack a deep understanding of cybersecurity intricacies.

ODMs essentially quantify the impact of security investments, providing a tangible way to measure the effectiveness of security measures. For instance, metrics like mean time to detect or mean time to respond offer insights into the efficiency of incident response plans. Improving these metrics indicates strengthening the overall security posture, while a decline may signify vulnerabilities or inefficiencies that need addressing.

Contrary to the traditional focus on cyber maturity, which assesses the presence of security measures, ODMs centre on evaluating their

performance. This shift in mindset allows organisations to align cybersecurity efforts more closely with business objectives. ODMs can demonstrate how security measures contribute to broader goals, such as maintaining customer trust or safeguarding intellectual property.

Presenting these metrics to the board and executive leadership may initially seem daunting, especially if they reveal areas of immaturity or weakness. However, successful organisations leverage such insights as opportunities to advocate for the necessary resources, funding, and staffing to bolster their ODMs. Rather than concealing shortcomings, they use them as a catalyst for improvement, ultimately fostering stronger, more resilient security programmes.

Resilience-Driven, Resource-Efficient Third-Party Cybersecurity Risk Management

Gartner advises healthcare organisations to prioritise cybersecurity risk when partnering with third parties, moving away from traditional due diligence practices. The focus should be on establishing mutually beneficial relationships and ensuring continuous safeguarding of valuable assets. This shift involves developing a resilience-driven strategy and collaborating closely with vendors to implement incident response plans and resource optimisation measures. Automation tools should be leveraged to streamline backup and failover processes. Education plays a crucial role in strengthening cybersecurity posture, emphasising collaboration and information sharing with industry peers, regulatory bodies, and cybersecurity firms to learn from shared experiences and avoid combating threats in isolation.

Generative AI - Short-Term Scepticism, Longer-Term Hope

Gartner emphasises the importance of preparedness for the swift evolution of Generative AI (GenAI), cautioning against unrealistic expectations while acknowledging its long-term potential. They stress the importance of readiness, urging organisations to thoroughly understand the data points and sources that will make AI tools valuable and to configure them correctly for specific use cases. Drawing parallels to the advent of cloud computing, they emphasise the need to understand AI's capabilities and potential outcomes before expecting productivity gains. Education is key, with various sources—from AI developers to third-party partners—providing insights and guidance to ensure successful adoption of Generative AI tools.

Security Behaviour and Culture Programs Gain Increasing Traction to Reduce Human Risks

Security leaders are shifting their focus from increasing awareness to fostering behavioural change to reduce cybersecurity risks. By 2027, 50% of large enterprise CISOs are expected to adopt human-centric security design practices to minimise friction and maximise control adoption. Security behaviour and culture programs (SBCPs) offer an enterprise-wide approach to mitigating cybersecurity incidents related to employee behaviour. Organisations implementing SBCPs report better employee adoption of security controls, reduced unsecure behaviour, increased speed and agility, and more effective use of cybersecurity resources as employees become proficient at making independent cyber risk decisions.

Extending the Role of Identity & Access Management (IAM) to Improve Cybersecurity Outcomes

As organisations transition to an identity-first approach to security, the emphasis shifts from traditional controls to Identity and Access Management (IAM), crucial for cybersecurity and business success. Gartner predicts an expanded role for IAM in security programmes, with a focus on enhancing fundamental hygiene and system hardening to bolster resilience. Security leaders are advised to strengthen their identity fabric and utilise identity threat detection and response to ensure IAM capabilities effectively support the broader security programme.

Source: Gartner

Image Credit: iStock

Published on : Wed, 8 May 2024