



CYBERSECURITY AWARENESS MONTH UNDERScores THE NEED FOR GREATER VIGILANCE IN THE AI ERA

Cybersecurity Awareness Month highlights rising AI-driven threats, APTs, ransomware, and state-sponsored attacks across the Middle East, as industry leaders emphasize resilience, awareness, governance, and proactive defense to strengthen cyber preparedness.

Cybersecurity Awareness Month highlights the growing importance of cyber resilience in an increasingly digital world. In the Middle East, where governments and organizations are accelerating AI adoption, cloud transformation, smart

city initiatives, and digital services, cybersecurity has become a strategic business and national security priority.

The region faces a rapidly evolving threat landscape marked by sophisticated ransomware attacks, Advanced Persistent Threats (APTs), state-

sponsored cyber campaigns, and attacks targeting critical infrastructure, financial institutions, healthcare providers, and government entities. The rise of artificial intelligence has further transformed cybersecurity, enabling attackers to create highly convincing phishing campaigns, deepfakes,

automated malware, and advanced social engineering attacks at scale.

At the same time, expanding digital ecosystems spanning cloud environments, IoT devices, operational technology, and third-party networks have widened the attack surface for organizations. While investments in cybersecurity technologies continue to grow, experts agree that technology alone is not enough. Strong governance, continuous monitoring, employee awareness, identity protection, and a security-first culture are essential

to building resilience. Cybersecurity Awareness Month provides an opportunity for organizations to strengthen preparedness and stay ahead of emerging AI-driven threats.

Biju Unni, Vice President at Cloud Box Technologies said that organizations in the Middle East continue to underestimate the impact of subtle user behaviors, social engineering techniques, privileged account abuse, and credential theft. Attackers increasingly bypass traditional defenses by exploiting legitimate access rather than

attacking technologies directly. The widespread adoption of IoT, remote access, and AI-driven applications has further expanded the security perimeter, increasing organizational exposure. Unni emphasizes that cybersecurity awareness must become an ongoing initiative rather than a periodic activity. Regular phishing awareness sessions, practical security exercises, and executive-led security programs are critical for building stronger cyber resilience. Looking ahead, he believes organizations must adopt adaptive cybersecurity strategies that combine AI-powered analysis, endpoint protection, Zero Trust Network Access (ZTNA), robust data governance, and continuous monitoring, while maintaining human oversight to ensure security decisions remain accountable and effective.

Hadi Anwar, CEO of CPX believes many organizations mistakenly equate technology investments with preparedness. The real challenge, he notes, lies in the gap between perceived readiness and true resilience. Cyber resilience is not solely about preventing incidents but ensuring business continuity when disruptions occur. He advocates



BIJU UNNI
VICE PRESIDENT AT CLOUD BOX
TECHNOLOGIES



HADI ANWAR
CEO OF CPX



RAMKUMAR BALAKRISHNAN
CHIEF EXECUTIVE OFFICER AT AMIVIZ

for stronger visibility, mature security operations centers, governance frameworks, and comprehensive recovery planning.

Anwar also stresses that cybersecurity must be embedded within organizational culture through accountability, ongoing training, and regular crisis simulations. As AI adoption accelerates, organizations must focus on AI governance, security-by-design principles, and readiness assessments to address emerging threats such as deepfake-enabled fraud, AI-powered social engineering, and identity-centric attacks. He argues that cybersecurity must evolve from a technical issue into a business priority supported by leadership and integrated across the organization.

Ramkumar Balakrishnan, Chief Executive Officer at AmiViz warns that many organizations continue to assume their security perimeter remains effective, while lacking visibility into threats that may already be operating inside their environments. He notes that modern attackers increasingly focus on lateral movement after initial compromise, creating risks that traditional perimeter-focused strategies may fail to detect. To



PUSHKAR SINGH
COUNTRY HEAD MEA, PROTECTT.AI



HASANIAN ALKASSAB
SECURITY BUSINESS UNIT DIRECTOR,
GBM

counter this, he advocates moving beyond annual awareness campaigns and building security cultures through consistent employee engagement and leadership accountability. Secure behavior should become the path of least resistance throughout the organization.

Regarding AI, Balakrishnan points out that attackers now benefit from the same technological advances as defenders. Organizations therefore need AI-assisted detection, continuous posture validation, and rapid response capabilities capable of operating at machine speed. In today's environment, he believes speed has become one of the most critical factors determining cybersecurity effectiveness.

Hasanian Alkassab, Security Business Unit Director, GBM identifies geopolitically motivated attacks targeting critical operations as one of the most underestimated risks facing organizations in the region. State-sponsored actors are increasingly focusing on operational technology environments, digital identities, and supply chain ecosystems instead of relying solely on direct attacks against network perimeters.

He highlights the importance of visibility across organizational environments to identify and address hidden exposures before they impact business continuity. To reduce human-related risks, Alkassab recommends role-based training, phishing simulations, privileged access management, and multi-factor authentication. Looking ahead, he believes organizations must secure AI while simultaneously using AI to strengthen defense capabilities. Protecting data, controlling access, and aligning with privacy regulations such as the UAE Personal Data Protection Law (PDPL) will be essential for maintaining resilience and compliance.

For Bassel Khachfeh, Digital Solutions Manager at Omnix International, weak governance remains one of the most significant cybersecurity challenges organizations continue to overlook.



BASSEL KHACHFEH
DIGITAL SOLUTIONS MANAGER AT
OMNIX INTERNATIONAL

Despite major investments in security technologies, many enterprises lack clearly defined ownership, accountability structures, and board-level oversight. This creates opportunities for shadow IT, uncontrolled third-party access, and unmanaged technology adoption.

He believes cybersecurity awareness must become part of everyday operations through regular training, role-specific learning programs, and realistic simulations that reflect current threat scenarios. As cybercriminals increasingly leverage AI to enhance their capabilities, Khachfeh emphasizes three priorities: strengthening identity and privileged access management, adopting AI-powered detection and response capabilities, and implementing stringent governance frameworks that regulate the deployment and use of AI technologies across the enterprise.

Pushkar Singh, Country Head MEA, Protectt.ai highlights a growing challenge facing financial institutions and digital service providers: the false assumption that successful authentication guarantees security. He explains that cybercriminals increasingly exploit screen sharing tools, remote access software, and malicious overlays to manipulate users after login has occurred.

Organizations therefore require continuous visibility into application behavior, device health, and user sessions. He also advocates extending cybersecurity awareness beyond employees to include customers through contextual warnings and real-time guidance when elevated risks are detected.

With AI lowering entry barriers for cybercriminals and enabling more convincing fraud attacks, Singh argues that organizations must deploy AI-driven behavioral intelligence and real-time protection mechanisms. As customer interactions increasingly involve AI agents and automated services, businesses must focus on securing both AI systems and the environments in which they operate.