

SPECIAL SUPPLEMENT BY

**Enterprise**  
CHANNELS **MEA**

VOLUME 07 | ISSUE 2 | **OCTOBER 2024**

# CYBER SENTINELS

**SAEED AGHA**

VP-Emerging Markets  
Zscaler

## SECURING TOMORROW

Zscaler Helps Businesses Navigate the Evolving Threat Landscape with an AI-Powered Zero Trust Platform

# Lexar

Come  
*visit* us

Experience the award-winning  
#WOWLexar storage & memory solutions



**GITEX**  
GLOBAL  
**2024**

**14<sup>th</sup>-18<sup>th</sup>** | **HALL-1**  
October 2024 | **Booth-A30**  
📍 Dubai World Trade Centre



## CISOs at the helm

*What does mean to be a CISO these days?*

*Given the growing importance of cybersecurity in modern businesses, this role has never been more critical. Cybersecurity has rightfully become a business enabler, with enterprises expanding their security budgets to keep pace with the ever-evolving threat landscape. The Middle East, with its strategic geography and oil-rich economies, has become a prime target for cybercriminals, with ransomware and DDoS attacks becoming increasingly common in the region.*



**JEEVAN THANKAPPAN**  
jeevan@gcemediagroup.com

*This is why the role of the CISO, transitioning from gatekeeper to guardian, is now under the spotlight. Beyond deploying robust technologies, security leaders have the responsibility to quantify business risks and communicate these to the board in a way that resonates. In other words, they must avoid technical jargon and clearly explain the potential risks to the business if cybersecurity measures are not strengthened.*

*The CISO role is already a precarious one, with studies showing that the average tenure for this position is less than four years. When a cybersecurity incident occurs, it is often the CISO who takes the fall. This dynamic needs to change. Cybersecurity is a collective responsibility that must start from the top. Instead of placing blame on the CISO, business leaders must cultivate a culture of security within their organizations and devise proactive strategies to stay ahead of threat actors.*

*In this issue of Cyber Sentinels, we spotlight some of the brightest minds in the industry and showcase their innovative approaches to cybersecurity. We hope their insights inspire you and provide valuable lessons for your own security strategies.*

# CYBER SENTINELS

## PUBLISHER

TUSHAR SAHOO  
TUSHAR@GECMEDIAGROUP.COM

## CO-FOUNDER & CEO

RONAK SAMANTARAY  
RONAK@GECMEDIAGROUP.COM

## GLOBAL HEAD, CONTENT AND STRATEGIC ALLIANCES

ANUSHREE DIXIT  
ANUSHREE@GECMEDIAGROUP.COM

## MANAGING EDITOR

JEEVAN THANKAPPAN  
JEEVAN@GECMEDIAGROUP.COM

## ASSISTANT EDITOR

SEHRISH TARIQ  
SEHRISH@GECMEDIAGROUP.COM

## CHIEF COMMERCIAL OFFICER

RICHA S  
RICHA@GECMEDIAGROUP.COM

## PROJECT LEAD

JENNEFER LORRAINE MENDOZA  
JENNEFER@GECMEDIAGROUP.COM

## SALES AND ADVERTISING

SALES@GECMEDIAGROUP.COM  
PH: + 971 562 151 157

## DIGITAL TEAM

## IT MANAGER

VIJAY BAKSHI

## PRODUCTION, CIRCULATION, SUBSCRIPTIONS

INFO@GECMEDIAGROUP.COM

## CREATIVE LEAD

AJAY ARYA

## DESIGNERS

SHADAB KHAN, JITESH KUMAR, SEJAL SHUKLA

## PRODUCTION

RITURAJ SAMANTARAY  
S.M. MUZAMIL

## DESIGNED BY



## SUBSCRIPTIONS

INFO@GECMEDIAGROUP.COM

## PRINTED BY

Al Ghurair Printing & Publishing LLC.  
Masafi Compound, Satwa, P.O.Box: 5613, Dubai, UAE

Office No #115  
First Floor, G2 Building  
Dubai Production City, Dubai  
United Arab Emirates  
Phone : +971 4 564 8684



31 FOXTAIL LAN,  
MONMOUTH JUNCTION, NJ - 08852 UNITED STATES OF AMERICA  
PHONE NO: + 1 732 794 5918

## A PUBLICATION LICENSED BY

International Media Production Zone, Dubai, UAE  
©copyright 2013 Accent Infomedia. All rights reserved.  
while the publishers have made every effort to ensure the accuracy of all information in this magazine, they will not be held responsible for any errors therein.



# CONTENTS

OCTOBER 2024



## CISO OPINION CORNER



**SARITH BHAVAN**  
Mubadala



**DR. MOHAMMED HUNAIDI**  
AD Ports Group



**NISHA RANI**  
MMI ELR



**BILAL BAIG**  
Trend Micro



**ILYAS MOHAMMAD**  
AmiViz



**MOHAMMED ALSHAMRANI**  
Cyberani



**MOHAMMED FEROZ KHAN**  
TOTAL



**KANESAN PANDI**  
Galadari Group

# BUILDING THE CISO OF THE FUTURE

## ? What emerging cybersecurity threats do you believe pose the greatest risk to organizations globally in the coming years?

Organizations worldwide are facing an increasingly complex and sophisticated threat landscape, where emerging cybersecurity challenges have the potential to disrupt operations and compromise sensitive data on a global scale. AI, while a powerful tool for defense, is also being leveraged by attackers for sophisticated phishing, deepfakes, and malware. Ransomware continues to be a persistent and pervasive threat, exacerbated by the rise of Cybercrime-as-a-Service. Organizations need to prioritize prevention, preparedness, and robust backup and recovery strategies. The increasing prevalence of IoT devices expands the attack surface, necessitating the extension of security principles to these devices and a focus on network segmentation. While still on the horizon for many, quantum computing poses a significant risk to current encryption standards, requiring proactive planning for a post-quantum world. Finally, supply chain attacks highlight the interconnected nature of today's business environment. As a data-driven organization, Mubadala understands the criticality of these measures and is committed to staying ahead of the curve in cybersecurity.

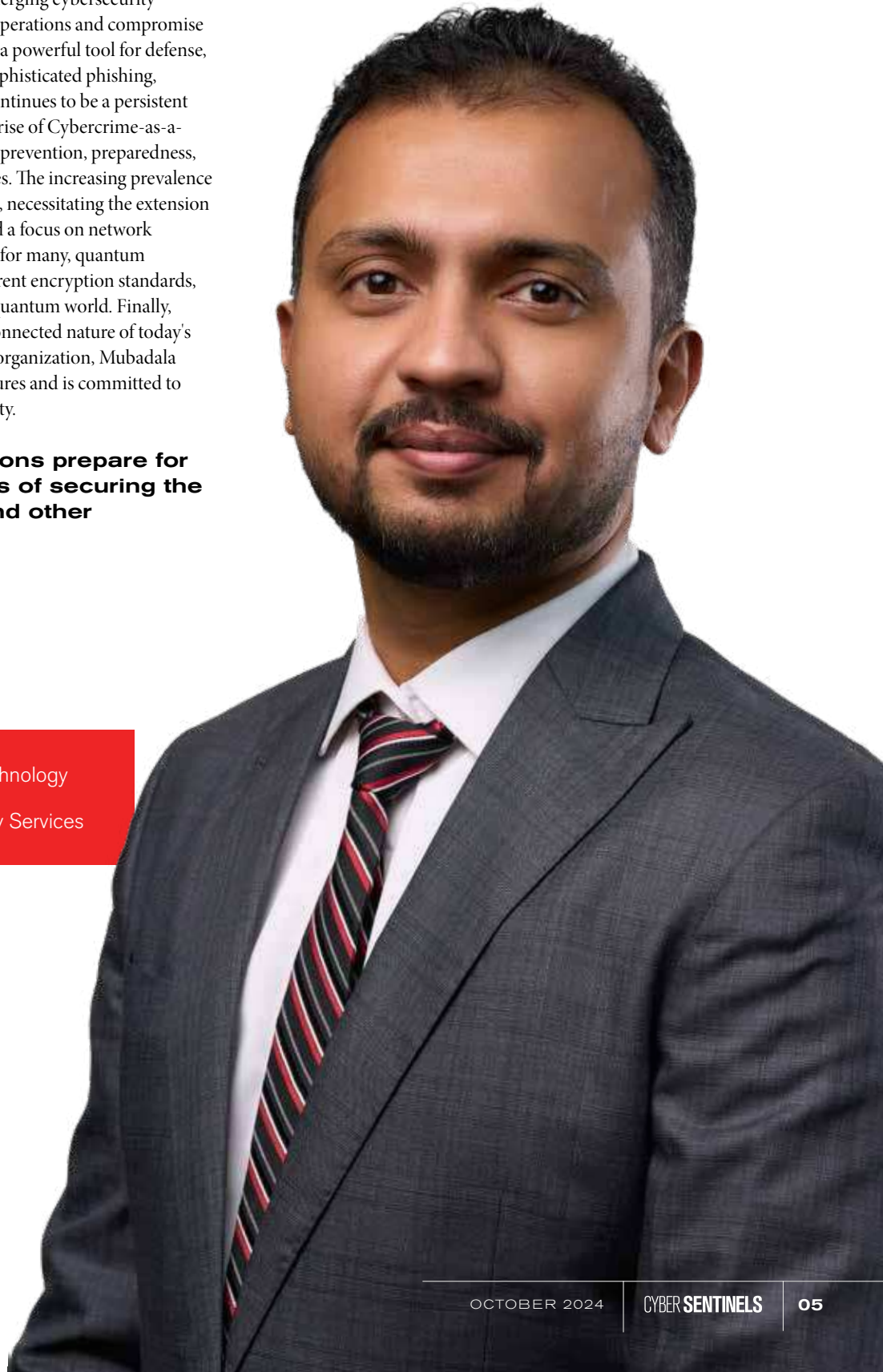
## ? How should organizations prepare for the growing challenges of securing the Internet of Things (IoT) and other

## connected devices?

With IoT devices becoming an integral part of most organizations' technology stacks, securing them is as crucial as safeguarding any other system within the environment. However, we recognize that the maturity of IoT security technologies and controls may not yet

### SARITH BHAVAN

Cybersecurity & Technology  
Platform Operations  
Digital & Technology Services  
Mubadala







be on par with the broader cybersecurity landscape. Therefore, a hybrid approach that combines legacy security principles with modern strategies is essential. This involves incorporating security right from the design phase of IoT devices, implementing strong authentication and access controls, and maintaining rigorous update and patch management practices. Adopting a Zero-Trust architecture, where every device and user are verified, is also crucial in this evolving landscape. Additionally, continuous monitoring and proactive security assessments play a vital role in identifying and addressing vulnerabilities before they can be exploited. At Mubadala, we are committed to applying these comprehensive security strategies to our IoT environment, ensuring that our connected devices are as secure as any other technology system within our organization.

**? What role do you see artificial intelligence and machine learning playing in both enhancing and compromising cybersecurity efforts?**

- AI and machine learning are undeniably playing a transformative role in the cybersecurity landscape. They offer immense potential for enhancing our defenses, enabling us to detect threats faster, automate responses, and even predict attacks

before they happen. At Mubadala, we're embracing this potential with the introduction of Microsoft Security Copilot, which is already streamlining our operations and enhancing our decision-making capabilities. However, we must also acknowledge that attackers are leveraging these same technologies for malicious purposes, including advanced phishing, deepfakes, and attacks on AI models themselves. This creates a dynamic and evolving threat landscape that requires constant vigilance and adaptation. To navigate this complex reality, organizations must invest in AI security, ensuring that AI systems themselves are resilient against attacks. Continuous monitoring and updating of AI models are also critical to stay ahead of emerging threats. Furthermore, adopting ethical AI practices is important to ensure that AI is used responsibly and transparently, both within our organizations and in the broader cybersecurity community.

**? How can companies ensure effective collaboration between the public and private sectors to tackle large-scale cyber threats?**

Effective collaboration between the public and private sectors is paramount in tackling large-scale cyber threats. We need to foster an environment where open communication, information sharing, and joint efforts are the

norm. This means establishing dedicated communication channels, holding regular meetings, and utilizing secure platforms to facilitate seamless information exchange. Joint training exercises and simulations can help build trust and improve coordination between sectors, enabling a more unified response to cyber incidents. Governments also play a crucial role in promoting collaboration by offering incentives for private sector participation and creating supportive regulatory frameworks that encourage information sharing without imposing undue burdens. Moreover, collaborative public awareness campaigns can educate the broader community about cyber threats and best practices, fostering a more cyber-aware society.

**? What are the key considerations for organizations when it comes to protecting sensitive data in a multi-cloud environment?**

Protecting sensitive data in a multi-cloud environment presents unique challenges, but with careful planning and execution, organizations can maintain a strong security posture. A crucial first step is comprehensive data classification, understanding the sensitivity of data based on its nature, regulatory requirements, and business value. This allows organizations



to prioritize security measures and tailor controls accordingly. Encryption, both at rest and in transit, is essential for protecting data confidentiality and integrity, utilizing industry-standard algorithms and cloud key management services. Strict identity and access management (IAM) policies are also critical to control who can access sensitive data. Leveraging cloud IAM solutions, enforcing role-based access controls, multi-factor authentication, and the principle of least privilege help ensure that only authorized individuals have access. Network segmentation and isolation techniques, such as virtual private clouds and firewalls, create secure boundaries within the multi-cloud environment, further enhancing security. Continuous monitoring and threat detection are essential for identifying and responding to potential threats in real-time. Organizations should deploy advanced security monitoring tools and leverage machine learning algorithms to proactively detect suspicious activity. Regular security audits and compliance checks ensure that the multi-cloud environment adheres to industry standards and regulatory requirements. Integrating security into DevOps processes is crucial for protecting sensitive data throughout the software development lifecycle. Embracing cloud-native security features offered by cloud providers can simplify security management and access control. By adopting these best practices, organizations can effectively safeguard their

sensitive data in a multi-cloud environment, ensuring confidentiality, integrity, and availability.

### **? How do you foresee the role of the CISO evolving as cybersecurity becomes more integral to business strategy?**

The Chief Information Security Officers (CISO) role is rapidly evolving from a technical expert to a strategic leader. Today's CISOs are not only responsible for implementing security measures, but also for aligning cybersecurity strategies with broader business objectives, particularly as cyber threats become a top priority for businesses. They are proactive risk managers, ensuring that the organization is prepared for and can respond effectively to cyber incidents. Collaboration across departments is essential for fostering a culture of security awareness and compliance. CISOs also play a crucial role in building trust with stakeholders and ensuring regulatory compliance. To succeed in this complex threat landscape, future CISOs will need a blend of technical expertise, strategic thinking, and strong communication and leadership skills. They must stay ahead of emerging technologies and threats, and continuously adapt to protect their organizations.

### **? What steps can organizations take to**

### **mitigate the risks associated with supply chain cybersecurity vulnerabilities?**

Mitigating supply chain cybersecurity vulnerabilities requires a proactive and multifaceted approach. It starts with thorough risk assessments of each supplier, evaluating their security practices, compliance, and potential vulnerabilities. Implementing strong access controls and continuous monitoring are crucial to limit and oversee supplier activity. Developing a comprehensive supply chain map helps identify critical vulnerabilities, while diversifying suppliers reduces the impact of potential incidents. Creating and regularly updating incident response plans ensures preparedness. Finally, incorporating cybersecurity requirements in contracts with suppliers establishes clear expectations. By taking these proactive steps, organizations can significantly reduce supply chain risks and strengthen their overall cybersecurity posture.

### **? In your opinion, what are the most critical skills and competencies future CISOs will need to succeed in an increasingly complex threat landscape?**

In today's complex threat landscape, it's not enough to simply be a technical expert, future CISOs need to be strategic thinkers who can bridge the gap between cybersecurity and business objectives. They need to be able to understand the big picture and articulate cybersecurity risks in a way that resonates with the boardroom. Of course, a deep understanding of cybersecurity principles and emerging technologies is still essential. But it's equally important to be a proactive risk manager, someone who can anticipate threats and develop effective mitigation strategies. When incidents inevitably occur, CISOs need to be prepared to lead the response and ensure the organization can recover quickly. Collaboration and communication are also key. CISOs need to work closely with other departments to foster a culture of security awareness and compliance. They need to be able to build trust with stakeholders and ensure regulatory compliance. And finally, in a field that's constantly changing, CISOs need to be lifelong learners. They need to stay ahead of the curve on emerging technologies and threats and be willing to adapt their strategies as needed. ➡

# AMPLIFY YOUR VOIZE WITH US AND EXPLORE OUR SERVICES.



DESIGN  
SERVICES



PHOTOGRAPHY &  
VIDEOGRAPHY



2D & 3D  
ANIMATION



EVENT  
MANAGEMENT



MEDIA  
BUYING



DIGITAL  
MARKETING



LOYALTY  
SOLUTIONS



TELE-  
CALLING



CORPORATE  
GIFTS



CONTENT  
GENERATION



SOCIAL  
MEDIA



BRAND  
ACTIVATION



BOOTH  
BUILDING



REWARD  
PROGRAM



EVENT STAFF-  
ING SERVICES



RETAIL STAFFING  
SERVICES



HOSTESS  
SERVICES

[WWW.GECMEDIAGROUP.COM](http://WWW.GECMEDIAGROUP.COM)

[WWW.BRANDVOIZE.COM](http://WWW.BRANDVOIZE.COM)



# FROM GUARDIAN TO LEADER

## ? What emerging cybersecurity threats do you believe pose the greatest risk to organizations globally in the coming years?

The cybersecurity landscape is constantly evolving, with new threats emerging regularly. Here are some of the most pressing concerns for organizations worldwide:

### 1. Artificial Intelligence (AI) and Machine Learning (ML) Driven Attacks:

- Advanced Malware: AI can be used to create highly sophisticated malware that can learn and adapt to defenses.
- Deepfakes: AI can generate realistic fake content, such as videos or audio recordings, that can be used for social engineering attacks or disinformation campaigns.

### 2. Internet of Things (IoT) Security:

- Botnets: IoT devices can be compromised and turned into botnets, which can be used for distributed denial-of-service (DDoS) attacks or other malicious activities.
- Data Privacy Violations: IoT devices often collect and store

sensitive data, making them a prime target for data breaches.

### 3. Cloud Security Threats:

- Misconfigurations: Cloud environments can be vulnerable to misconfigurations, which can expose sensitive data or systems to unauthorized access.

#### DR. MOHAMMED HUNAIDI

Manager-Cyber Information  
Security  
Risk and Compliance, AD Ports  
Group





• **Supply Chain Attacks:** Third-party cloud providers can be targeted by attackers, who can then gain access to their customers' data.

#### 4. Supply Chain Attacks:

• **Compromised Software:** Attackers can target software supply chains to introduce malicious code into widely used applications.

• **Third-Party Vendor Breaches:**

Organizations that rely on third-party vendors can be exposed to risks if those vendors experience data breaches.

#### 5. Social Engineering Attacks:

• **Phishing:** Phishing attacks continue to be a major threat, with attackers becoming increasingly sophisticated in their tactics.

• **Business Email Compromise (BEC):** BEC attacks target businesses by impersonating senior executives or other trusted individuals to trick employees into sending money or sharing sensitive information.

#### 6. Ransomware:

• **Ransomware-as-a-Service (RaaS):** Ransomware attacks have become more accessible, with attackers offering ransomware-as-a-service to anyone who wants to launch an attack.

• **Extortion:** Ransomware attackers are increasingly threatening to release stolen data if their demands are not met.

**To mitigate these risks, organizations must:**

- Stay informed: Keep up-to-date on the latest cybersecurity threats and trends.
- Implement strong security controls: Use

a combination of technical, administrative, and physical controls to protect their systems and data.

• **Train employees:** Educate employees about cybersecurity best practices and how to recognize and avoid phishing attacks.

• **Conduct regular risk assessments:** Identify and address vulnerabilities in their systems and processes.

• **Have a robust incident response plan:** Be prepared to respond effectively to security incidents.

### **? How should organizations prepare for the growing challenges of securing the Internet of Things (IoT) and other connected devices?**

As the number of connected devices continues to grow exponentially, organizations must prioritize the security of their IoT infrastructure. Here are some key strategies to consider:

#### 1. Risk Assessment and Inventory:

• **Identify IoT Devices:** Conduct a thorough inventory of all IoT devices in your organization, including those that may be hidden or overlooked.

• **Assess Vulnerabilities:** Evaluate the security risks associated with each device, considering factors like connectivity, data storage, and processing capabilities.

#### 2. Secure Device Configuration:

• **Default Password Changes:** Ensure that

all IoT devices are configured with strong, unique passwords.

• **Firmware Updates:** Regularly update device firmware to address known vulnerabilities.

• **Network Segmentation:** Isolate IoT devices on a separate network segment to limit potential damage in case of a breach.

#### 3. Data Privacy and Security:

• **Data Minimization:** Collect only the necessary data and avoid storing sensitive information on IoT devices.

• **Encryption:** Implement strong encryption protocols to protect data transmitted between devices and the network.

• **Access Controls:** Restrict access to IoT devices and data to authorized personnel.

#### 4. Network Security:

• **Firewalls:** Use firewalls to filter traffic and prevent unauthorized access to IoT devices.

• **Intrusion Detection Systems (IDS):** Monitor network traffic for suspicious activity and alert administrators to potential threats.

• **Secure Protocols:** Employ secure communication protocols like HTTPS and TLS to protect data in transit.

#### 5. Incident Response Planning:

• **Develop a Plan:** Create a comprehensive incident response plan that outlines steps to be taken in case of a security breach.

• **Test the Plan:** Regularly test the incident response plan to ensure that it is effective and up-to-date.

#### 6. Employee Training and Awareness:

• **Educate Employees:** Provide employees

with training on IoT security best practices, including how to recognize and avoid phishing attacks.

- **Promote Awareness:** Foster a culture of security awareness within the organization, encouraging employees to report any suspicious activity.

#### 7. Vendor Management:

- **Evaluate Vendors:** Carefully evaluate IoT vendors to ensure that they have strong security practices in place.

- **Contracts:** Include security clauses in contracts with IoT vendors to outline their responsibilities.

By implementing these strategies, organizations can significantly reduce the risks associated with IoT security and protect their valuable assets.

### ? What role do you see artificial intelligence and machine learning playing in both enhancing and compromising cybersecurity efforts?

AI and ML are Double-Edged Sword in Cybersecurity

#### Enhancing Cybersecurity:

- **Threat Detection and Prevention:** AI and ML algorithms can analyze vast amounts of data to identify patterns and anomalies that may indicate a cyberattack. This can help detect threats early on and prevent them from causing significant damage.

- **Automated Response:** AI-powered systems can automate certain security tasks, such as patching vulnerabilities or blocking malicious traffic, reducing the workload for human security teams.

- **Behavioral Analytics:** AI can analyze user behavior to identify unusual patterns that may indicate a compromise, such as unauthorized access or data exfiltration.

- **Vulnerability Assessment:** AI can help identify vulnerabilities in software and systems that could be exploited by attackers.

#### Compromising Cybersecurity:

- **Advanced Malware:** AI can be used to create more sophisticated and evasive malware that can learn and adapt to defenses.

- **Social Engineering:** AI-powered tools can generate highly realistic fake content, such as deepfakes, that can be used to deceive individuals and organizations.

- **Automated Attacks:** AI can automate the process of launching attacks, making it easier for malicious actors to target a large number

of victims.

- **Data Privacy Violations:** AI can be used to analyze and exploit personal data, leading to privacy breaches and identity theft.

**To maximize the benefits of AI and ML in cybersecurity while mitigating the risks, organizations should:**

- **Invest in AI and ML expertise:** Hire skilled professionals who can develop and deploy AI-powered security solutions.

- **Adopt a proactive approach:** Use AI and ML to continuously monitor and analyze their security posture and identify potential vulnerabilities.

- **Consider ethical implications:** Develop ethical guidelines for the use of AI and ML in cybersecurity to ensure that these technologies are used responsibly.

- **Stay informed:** Keep up-to-date on the latest developments in AI and ML, as well as the potential threats they pose.

By carefully considering the potential benefits and risks of AI and ML, organizations can leverage these technologies to enhance their cybersecurity defenses and protect against emerging threats.

### ? How can companies ensure effective collaboration between the public and private sectors to tackle large-scale cyber threats?

Effective collaboration between the public and private sectors is essential to combatting large-scale cyber threats.

Foster such partnerships will be of a huge benefit like Information Sharing governance, Joint Research, unified Policy Development, Cybersecurity Training and Education programme; Incident Response Coordination, Regulatory Compliance and shared Cyber Security infrastructure. In my book Cyber Security in UAE Public Sector; I talked about the amazing efforts done on this subject making UAE leading by example.

### ? What are the key considerations for organizations when it comes to protecting sensitive data in a multi-cloud environment?

Key considerations for protecting sensitive data in a multi-cloud environment would be Data Classification based on sensitivity

and criticality; Access Control Management; Encryption, Data Loss Prevention; CSA best practises; Regular Audits and Assessments; Incident Response Planning and Vendor Management.

### ? How do you foresee the role of the CISO evolving as cybersecurity becomes more integral to business strategy?

As cybersecurity becomes increasingly critical to business success, the role of the Chief Information Security Officer (CISO) is evolving from a purely technical position to a strategic one by playing a leading role as business enabler; Risk Management; Innovation; Compliance and strategic advisor.

### ? What steps can organizations take to mitigate the risks associated with supply chain cybersecurity vulnerabilities?

Supply chain cybersecurity vulnerabilities pose significant threats to organizations; some counter measures to protect includes vendor management (Due Diligence; Contracts and NDAs, and Regular Assessments); By implementing these measures, organizations can significantly reduce the risks associated with supply chain cybersecurity vulnerabilities and protect their sensitive data and operations.

### ? In your opinion, what are the most critical skills and competencies future CISOs will need to succeed in an increasingly complex threat landscape?

As the cybersecurity landscape becomes increasingly complex, CISOs will need to possess a diverse range of skills and competencies. Some of the most critical would-be strategic thinking; Risk Management; Technical Expertise; Communications Skills; Leadership; Negotiations Skills; Regulatory Compliance; Innovation; Ethical Consideration; Adaptability.

By developing these skills and competencies, CISOs can position themselves as strategic leaders who can effectively protect their organizations in the face of increasing cyber threats. ➡



# CYBERSECURITY THREAT EVOLUTION

## ? What emerging cybersecurity threats do you believe pose the greatest risk to organizations globally in the coming years?

Emerging cybersecurity threats include AI-driven attacks, where cybercriminals leverage artificial intelligence to automate and enhance phishing and impersonation attempts, making them increasingly difficult to detect. The rapid expansion of Internet of Things (IoT) devices adds another layer of risk, as many of these devices lack robust security, creating potential entry points for attackers. Additionally, the growing reliance on cloud services and remote work environments introduces new challenges, such as securing remote endpoints and preventing data breaches. To effectively address these risks, organizations must continuously adapt their cybersecurity strategies to stay ahead of evolving threats.

## ? How should organizations prepare for the growing challenges of securing the Internet of Things (IoT) and other connected devices?

To secure the growing number of IoT and connected devices,

organizations must adopt a multi-layered approach to cybersecurity. First, it's crucial to implement strong authentication and access controls, ensuring that only authorized users and devices can access the network. Regularly updating and patching IoT devices is also

**NISHA RANI**  
CISO  
MMI ELR



essential, as many devices are shipped with vulnerabilities that can be exploited if not addressed.

Network segmentation is another key strategy, isolating IoT devices from critical systems to limit the impact of a potential breach. Organizations should also monitor IoT traffic for unusual patterns, which can help detect and respond to threats in real-time.

Finally, educating employees about the risks associated with IoT devices and promoting a culture of cybersecurity awareness can prevent many common vulnerabilities. By taking these proactive steps, organizations can better prepare for the challenges posed by the growing number of connected devices.

### **? What role do you see artificial intelligence and machine learning playing in both enhancing and compromising cybersecurity efforts?**

Artificial intelligence (AI) and machine learning (ML) are transforming the cybersecurity landscape in both positive and challenging ways. On the enhancement side, AI and ML can significantly improve threat detection and response times. They can analyze vast amounts of data to identify patterns and anomalies that may indicate a security breach, enabling quicker and more accurate detection of threats. These

technologies can also automate routine security tasks, freeing up human resources to focus on more complex issues.

However, AI and ML can also be weaponized by cybercriminals. Attackers are increasingly using AI to develop more sophisticated and targeted attacks, such as deepfake phishing and automated malware. These AI-driven threats can bypass traditional security measures, making it more difficult for organizations to defend themselves.

In essence, while AI and ML offer powerful tools to enhance cybersecurity, they also introduce new risks that require vigilant management. Organizations must stay ahead of these advancements, leveraging AI and ML to bolster their defenses while being prepared to counter AI-driven threats.

### **? How can companies ensure effective collaboration between the public and private sectors to tackle large-scale cyber threats?**

Effective collaboration between the public and private sectors is essential to address large-scale cyber threats. Companies can foster this collaboration by participating in information-sharing initiatives, where they exchange threat intelligence with government agencies and other organizations. This helps create a unified response to emerging threats and ensures that critical information is

disseminated quickly.

Building strong relationships with government bodies and industry groups is also crucial. Companies should actively engage in public-private partnerships, working together to develop cybersecurity standards, policies, and best practices. Regular joint exercises and simulations can further enhance preparedness, ensuring that both sectors are aligned in their response strategies.

Transparency and trust are key to successful collaboration. Companies should be open about their cybersecurity challenges and work closely with public entities to develop solutions that benefit all parties. By prioritizing these efforts, organizations can contribute to a more resilient cybersecurity ecosystem that is better equipped to handle large-scale threats.

### **? What are the key considerations for organizations when it comes to protecting sensitive data in a multi-cloud environment?**

To secure the growing number of IoT and Protecting sensitive data in a multi-cloud environment requires a comprehensive and strategic approach. First, organizations must implement strong encryption practices, ensuring that data is encrypted both at rest and in transit across all cloud platforms. This





protects data even if a breach occurs. Access management is another critical consideration. Organizations should adopt a Zero Trust model, where access to data and resources is granted based on strict identity verification and is continuously monitored. Using multi-factor authentication (MFA) and robust identity and access management (IAM) solutions can further strengthen security.

Visibility and control over data are essential. Organizations need to deploy tools that provide centralized monitoring and management across multiple cloud environments. This includes tracking data movement, detecting anomalies, and ensuring compliance with data protection regulations.

Lastly, organizations should regularly assess and update their security posture. As cloud environments evolve, so do the threats. Regular security audits, continuous monitoring, and collaboration with cloud service providers are necessary to adapt to new risks and protect sensitive data effectively.

### **? How do you foresee the role of the CISO evolving as cybersecurity becomes more integral to business strategy?**

As cybersecurity becomes increasingly central to business strategy, the role of the Chief Information Security Officer (CISO) is evolving from a purely technical

function to a more strategic leadership position. CISOs are now expected to be key contributors to business decisions, ensuring that cybersecurity is integrated into the organization's overall strategy and operations.

In this evolving role, CISOs will need to bridge the gap between technical teams and executive leadership, translating complex security issues into business risks and opportunities. This requires a deep understanding of the business, industry, and regulatory landscape, enabling the CISO to align cybersecurity initiatives with the company's goals and objectives.

Furthermore, the CISO will play a critical role in fostering a culture of security across the organization. This involves not only implementing robust security measures but also promoting cybersecurity awareness and best practices at all levels of the company.

As digital transformation and emerging technologies continue to reshape industries, the CISO's role will expand to include overseeing risks associated with AI, IoT, and cloud environments, making them a pivotal figure in driving innovation while safeguarding the organization.

### **? What steps can organizations take to mitigate the risks associated with supply chain cybersecurity vulnerabilities?**

Mitigating supply chain cybersecurity risks

requires a proactive and comprehensive approach. First, organizations should conduct thorough risk assessments of their supply chain partners, evaluating their security practices and identifying potential vulnerabilities. This includes understanding how sensitive data is handled and ensuring that third parties comply with security standards.

Implementing strict access controls is also crucial. Organizations should limit the access that suppliers and vendors have to their systems, ensuring that each partner only has the necessary permissions to perform their tasks. Regularly reviewing and updating these access controls helps minimize the risk of unauthorized access.

Continuous monitoring and real-time threat detection are key to identifying and responding to potential supply chain threats quickly. By leveraging advanced security tools and technologies, organizations can gain visibility into their supply chain and detect anomalies that may indicate a breach. Additionally, fostering strong communication and collaboration with supply chain partners is vital. Organizations should establish clear cybersecurity expectations and work closely with suppliers to address any identified risks. Regular audits, security training, and incident response planning can further enhance the resilience of the entire supply chain.

### **? In your opinion, what are the most critical skills and competencies future CISOs will need to succeed in an increasingly complex threat landscape?**

Future CISOs will need a mix of technical expertise and strategic insight. Key skills include:

- **Technical Acumen:** Understanding the latest cybersecurity threats and technologies.
- **Strategic Vision:** Aligning security initiatives with business goals and anticipating future threats.
- **Leadership and Communication:** Effectively conveying security risks and strategies to both technical teams and executives.
- **Risk Management:** Assessing and managing risks across the enterprise, including third-party and supply chain risks.
- **Adaptability and Continuous Learning:** Staying updated on evolving threats and technologies to lead the organization effectively. ➡





# DRIVING OPERATIONS AND PERFORMANCE EXCELLENCE

YOUR PARTNER FOR



Cloud & Digital  
Transformation



Enterprise  
Applications



Analytics &  
Automation AI &  
ML as a Service



Cyber  
Security  
Solutions



Management Consulting,  
Advisory and Quality Assurance

An unit of



“Delivery centres in US, Middle East and India”

# SECURING TOMORROW

Saeed Agha, VP-Emerging Markets at Zscaler, discusses the evolving threat landscape and explains why adopting a Zero Trust security framework is crucial in today's remote and cloud-driven environment.



**SAEED AGHA**  
VP-Emerging Markets  
Zscaler

## ? Is ransomware defense still a top priority for CISOs, and which industries are the most targeted?

Ransomware defense must remain a top priority for CISOs in 2024 and beyond. The increasing use of ransomware-as-a-service models, coupled with numerous zero-day attacks on legacy systems, a rise in vishing attacks, and the emergence of AI-powered attacks, has led to record-breaking ransom payments—nearly double the highest publicly known ransomware payout so far. Organizations must prioritize Zero Trust architectures to strengthen their security posture against ransomware attacks. This is where an AI-powered Zero Trust platform like Zscaler helps organizations fast-track their segmentation journeys, reducing the blast radius and shutting down unknown vectors for future AI-driven attacks.

Ransomware attacks pose significant risks to businesses of all sizes and industries. However, a few sectors stand out, according to our annual Zscaler ThreatLabz 2024 Ransomware Report, which showed an overall increase of 18% in attacks year over year. The manufacturing industry was by far the most targeted, facing more than twice as many attacks as any other industry, followed by healthcare, the technology sector, education, and financial services. Industries face unique ransomware challenges based on how they operate, handle data, and structure their technology infrastructure. Despite these variables, ransomware extortion attacks have consistently surged, with the number of victim companies listed on data leak sites increasing by nearly 58% since last year's ransomware report.

## ? How has the nature of ransomware attacks evolved in recent years, particularly with the rise of ransomware-as-a-service (RaaS)?

The popularity and success of ransomware attacks have led to the rise of Ransomware-as-a-Service (RaaS). Similar to legitimate software-as-a-service offerings, RaaS is available to malicious actors on a subscription basis, providing a platform that allows anyone, even without programming skills, to launch an attack and hold computer files, information, or systems hostage. If an attack succeeds, the ransom is divided among the service provider, coder, subscriber, and



affiliates. This distribution mechanism contributes to the growing threat potential, as RaaS tools (such as Dark Angels or LockBit) are often inexpensive and readily available on the dark web.

Additionally, the double extortion mechanism in ransomware attacks continues to evolve. In double extortion, machines are not only encrypted to demand ransom, but data is also stolen before encryption. Attackers infiltrate an environment, find sensitive data, and exfiltrate it before taking servers offline. This way, backups won't help organizations recover, as the attackers threaten to publish the stolen data unless a ransom is paid.

## ? Why has Zero Trust become a critical framework in today's security landscape, particularly with the rise of remote work and cloud adoption?

Currently, many organizations are still trying to maintain the status quo without adapting to the changing world of workloads in multi-cloud environments and users working from everywhere. Adopting a Zero Trust-based approach helps organizations to secure

their exposed assets, interfaces, devices, or network-based appliances by design. The only way to truly secure today's digital businesses is to adopt a Zero Trust security model, where validated user identity is combined with business policies for direct access to authorized applications and resources. Zero Trust delivers a distinct architecture based on the principle of least-privileged access, ensuring users access only the resources they need—rather than receiving access to the entire network and its connected resources. The Zscaler Zero Trust Exchange platform offers a Zero Trust architecture that secures users, workloads, IoT/OT devices, and B2B partners. It acts as an intelligent switchboard, providing secure, any-to-any connectivity without extending network access, and offers additional cyber threats and data protection.

## ? What are the biggest challenges organizations face when transitioning to a Zero Trust architecture?

The biggest challenge with Zero Trust is the necessary mindset shift to transform security wholeheartedly. According to our recent State of Zero Trust Transformation Survey,





70% of organizations globally are either rolling out Zero Trust security or are in the strategic planning process. Additionally, 21% of organizations have already implemented Zero Trust-based tools, which have reduced their attack surface and made them safer than before. However, many organizations are not following their transformation efforts thoroughly.

Organizations often fail to remove outdated ways of connecting to the internet or workloads when implementing new technologies. As long as parallel efforts exist, they lose efficiency and create dangerous attack vectors. Over the next two years,

organizations must leverage the full potential of their Zero Trust-based architectures to support their digitization efforts. Zero Trust is not just a security technology; it can form the foundation for secure connectivity between users, workloads, and IoT/OT infrastructures, enabling true, secure digitization.

### **? Do you leverage AI and ML within the portfolio?**

AI requires a large, relevant data set from which it can learn to understand and solve problems effectively. Zscaler has access to such a data set, with 500 billion daily platform transactions and 500 trillion

daily telemetry signals. This data is further enhanced by research from ThreatLabz, our global threat research team, data from over 60 threat intelligence feeds, and prebuilt integrations with more than 150 other technologies serving as additional data sources. As a result, Zscaler offers various powerful security and business solutions leveraging AI for increased automation and effectiveness.

For example, Zscaler's AI Auto Data Discovery leverages the reach of our Zero Trust architecture alongside AI-driven automation and precision. This solution automatically finds and classifies data across SaaS apps, private apps, end-user devices, email, and even encrypted traffic. This capability not only enhances data security but also saves time for administrators.

### **? What is your advice to CISOs in the region embarking on cybersecurity transformation?**

One of the fundamental elements of security for an organization is understanding its risk and choosing the right tools to control and protect that risk. IT teams need to elevate their security hygiene to keep pace with the changing nature of ransomware, particularly ransomware-as-a-service models, as complacency is the biggest enemy in fighting these attacks.

Currently, two major obstacles to strong cyber hygiene and resilience are the lack of a consistent security framework and a lack of transparency from IT teams regarding the actual dangers an organization faces daily. Many organizations are reactive and have a mix of strategies and technologies built up over years. As a result, they may "feel" prepared but often lack awareness of gaps in their framework and have no formal methods for testing readiness and resilience. CISOs and security teams are often seen as part of IT and are not involved in strategic business planning. This must change to improve cyber preparedness—aligning the security function with business strategic goals is no longer negotiable. In 2024 and beyond, cyber hygiene should be a priority for business leaders, with CISOs becoming central to business strategy to align security functions with business outcomes. The next level of cyber preparedness requires a clear security framework, enhanced employee cyber awareness, and measurable outcomes aligned with business objectives. ➡



# PROTECT WHAT MATTERS MOST

Check Point Infinity Platform delivers AI-powered and cloud-delivered cyber security across your entire enterprise: network, cloud, and workspace

## JOIN CHECK POINT AT GITEX GLOBAL

Dubai World Trade Centre  
Booth B20, Hall 24  
14-18, October 2024

**GITEX**  
GLOBAL



CHECK POINT SOFTWARE  
TECHNOLOGIES MIDDLE EAST  
[infogcc@checkpoint.com](mailto:infogcc@checkpoint.com)  
[www.checkpoint.com](http://www.checkpoint.com)







SOUTH AFRICA



# A celebration of technology leadership and innovation

The 2024 World CIO 200 Summit Grand Finale, hosted in Johannesburg and Cape Town, South Africa, set a new standard for excellence in celebrating global technology leadership.

More than 200 CIOs, CISOs, and visionaries from all corners of the world came together in a dazzling show of collaboration, innovation, and leadership, igniting the future of digital transformation like never before.

Hosted by the Global CIO Forum, this summit was the pinnacle of a 50-country journey. It was a gathering of tech pioneers, the brightest minds in the industry, who didn't just meet to talk but to redefine the future of business.

Here is how it unfolded over four days.

## Day zero

Day zero saw guests welcomed and checked in, collecting their event badges, access passes, and merchandise in preparation for the exciting activities and networking sessions ahead. A key highlight of the opening day was the Archery Challenge 2024, powered by Sentient Archery.

Over 100 CIOs participated in this thrilling test of precision and leadership, aiming to hit the bullseye and claim the title of Archery Champion.

The activity not only tested physical prowess but also symbolized the sharp decision-making and accuracy required of top IT leaders in today's fast-evolving tech landscape. This activity was sponsored by Quixy.

Following the adrenaline-pumping archery competition, the day shifted to a more relaxed and celebratory tone with a spectacular tribute show, "SIMPLY THE BEST", celebrating the greatest musical icons of all time at The Barnyard Theatre, Emperors Palace. Attendees were treated to an unforgettable performance, bringing a blend of music, entertainment, and nostalgia to close out the first day of the summit.

The evening concluded with the World CIO 200 2024 Grand Finale Welcome Dinner held at the iconic Tribes African Steakhouse & Grill. Guests savored the finest in African cuisine while reflecting on the day's accomplishments and gearing up for the summit's key discussions and presentations over the following days.

## Day one

Day one of the prestigious World CIO 200 Grand Finale unfolded at the Birchwood Hotel & OR Tambo Conference Centre, marking an extraordinary gathering of global CIOs, IT thought leaders, and industry innovators. The event kicked off with an early morning Breakfast &



# THE WORLD CIO 200 SUMMIT

15-19 SEPT, 2024



Networking session, where attendees engaged in meaningful conversations and exchanges over coffee. The relaxed networking atmosphere set the tone for a day packed with enriching content and discussions, all centered on technology leadership and innovation.

The day officially began with a welcome note delivered by Ronak Samantaray, Co-founder and CEO of GEC Media Group, who set the stage for the remarkable sessions that followed. His welcome speech highlighted the significance of global collaboration in addressing the evolving technological landscape, emphasizing the role of CIOs as strategic enablers of digital transformation.

Jeevan Thankappan, Managing Editor of GEC Media Group, followed with an Editor's Note, offering a deep dive into the event's core theme and discussing how technology can transcend borders and create a global impact. He recognized the growing importance of digital leadership in the face of emerging global challenges, reinforcing the need for innovation and collaboration.

The morning sessions continued with Charbel Zreiby, Regional Director, Channel Data Center Specialists at Dell Technologies, delivering a keynote focused on the transformative power of AI across industries and the importance of

embracing AI to stay competitive in a rapidly evolving technological landscape.

His presentation was followed by the next keynote by Ricky Kej, three-time Grammy Award Winner and United Nations Goodwill Ambassador, who shared his thoughts on "Uniting Cultures, Transcending Borders."

Sharing his journey as a musician and environmentalist, Ricky emphasized the interconnectedness of music and nature. After 13 years of producing over 3,500 commercials, he decided to stop producing commercial music and instead focus on creating music that addresses social and environmental issues.

This was followed by thought-provoking session by Alan McSmith, a wilderness guide from South Africa, who discussed the importance of connectivity and being human, emphasizing the inclusion of future generations and non-human entities as stakeholders.

His presentation invited the audience to reflect on their perceptions and navigate through existential crises by facing fears and changes





beneath the surface, using an anecdote from the Okavango Delta to illustrate this concept.

Ali El Kontar, CEO of Zero&One, took the stage next, emphasizing leadership and personal accountability. To foster change in an organization, leaders must be the change they wish to see in others, taking ownership of problems and actively seeking solutions. This modeling of behavior will encourage others to follow suit, improving teamwork and performance, he said.

This was followed by a presentation from Amit Veer, Founder & CEO, Coffee.io-merchandise sponsor of the event- focused on offshoring with AI-powered tech recruitment, addressing the global tech talent shortage, particularly in industries like software engineering. He highlighted the key benefits







of offshoring, especially to India, which offers a large pool of skilled tech professionals at lower costs, 24/7 operations, and no language barriers. The presentation from Raif Abou Diab, Country Manager - South Gulf & Sub Saharan Africa at Nutanix highlighted the significance of Nutanix's hybrid multi-cloud platform and its role in simplifying IT environments. The key message is that Nutanix enables organizations to run applications and data across various environments, including on-premises, private, and public clouds, with a unified platform. The afternoon kicked off with a sumptuous lunch and networking session, allowing attendees to connect further and reflect on the discussions from the morning. Following lunch, the Leadership Masterclass was led by Dr. Antoine Eid, founder of Meet YourSelf, which is the world's first science-based workplace DNA assessment and reporting tool that combines three key scientific areas together to deliver the most comprehensive and applicable results for performance at the workplace. In the evening, the spotlight turned to the much-awaited Ambassadors Meet, an invite-only session that brought together ambassadors of the World CIO 200 2024 initiative. The

exclusive gathering fostered deep discussions on leadership challenges and opportunities, with ambassadors sharing their experiences in driving technological advancements across various industries.

As the day transitioned into night, the event's grand Gala Dinner commenced, starting with an opening note by Richa S, Chief Commercial Officer of GEC Media Group. The dinner provided a perfect blend of celebration and recognition, highlighted by a stellar performance from Manoj George, an internationally renowned violinist and music composer, alongside Ricky Kej, whose uplifting melodies symbolized the spirit of positivity and cultural diversity. The event continued with the Ambassadors Recognition ceremony, where outstanding global leaders were honored for their exceptional contributions to the GCF community and the broader IT industry. This was followed by the presentation of the GCF Preferred Partner Awards, recognizing key partners who played a significant role in advancing the goals of the Global CIO Forum.

#### Day two

The day commenced on a serene note with a Mental Wellbeing Program led by world-

renowned Yoga Guru Sumit Manav. His session, titled "Mindful Meditation – An Inward Journey," focused on nurturing mental wellbeing, a vital aspect for today's leaders. In a world driven by fast-paced technological change, Sumit emphasized the importance of grounding oneself through mindfulness, enabling leaders to manage stress and maintain a sense of balance in their personal and professional lives. The participants were guided through meditation techniques aimed at fostering clarity and focus—qualities essential for navigating complex decision-making processes.

Venkatesh Mahadevan (Venki), Board Member of CaaS, delivered an insightful opening address titled "Moving the Needle" through storytelling and real-world examples of transformation.

He highlighted key examples from around the world, emphasizing the power of accessibility, collaboration, and innovation in driving change. Venki inspired the audience to identify ways in which they can "move the needle" in their respective fields, stressing that even a single idea can create significant change.

He encouraged a mindset of collective action and innovation, asking leaders to consider their roles in shaping the future, especially with innovations like AI and ChatGPT. He closed with a powerful reminder: "Do not die with the music inside your head," encouraging the audience to share their ideas and foster innovation rather than holding them back.

The address was a mix of humor, inspiration, and deep reflection, leaving the audience motivated to take action and create lasting change in their organizations.

#### Keynotes and Thought Leadership

The morning session featured a lineup of influential speakers sharing thought-provoking insights:

- Mohammed Abdul Hadi, Director of Enterprise Infrastructure Solutions at StorIT Distribution, delivered the Partner Keynote,





highlighting the future of enterprise infrastructure and the evolving role of technology in driving growth and operational efficiency.

- Aphiwe Qhama Menziwa, Founder of Tembisa Ratanga, took the stage with an inspiring talk titled “A Place of Hope,” where he shared the story of how his organization is transforming lives in disadvantaged communities, showcasing the power of technology in driving social change.
- Mayuresh Kothari, Technical Director at Secureworks, provided a keynote focusing on cybersecurity and the growing challenges of protecting digital ecosystems in an increasingly interconnected world.
- Jayakumar Mohanachandran, CRO of CaaS Research, shared his insights on “AI Foresights

and Outlook 2024-25,” offering a glimpse into how artificial intelligence will shape industries and redefine the future of business. His insights provided valuable context for CIOs as they plan for AI integration into their operations.

#### **Technology and Innovation Presentations**

The technological landscape took center stage as thought leaders shared groundbreaking insights:

- Gautam Nimmagadda, CEO of Quixy, introduced “The Power of No-Code Platforms for Seamless Applications.” His talk underscored the efficiency and agility that no-code platforms offer for businesses to rapidly develop and

deploy applications, reducing dependency on traditional development cycles.

- Rajeev Dutt, General Manager of SwissGRC, joined virtually for a session titled “GRC for Strategic Excellence and Operational Resilience,” shedding light on how governance, risk, and compliance solutions are integral to building Later in the day, Sumit Manav returned to the center stage to captivate the audience with a second session, “Your Path to Lifelong Wellbeing.” Building on his earlier meditation program, Sumit offered actionable tips for embedding mindfulness practices into daily routines,





empowering leaders to achieve sustained mental clarity and physical vitality.

The last of the morning's partner keynotes was delivered by Caryn Vos, Senior Manager of the Crypto Division at Altron, who said the company has become a trusted leader with a full stack of solutions that bring centralized security controls, policies, and compliance into heterogeneous and dynamic hybrid cloud environments.

The highlight of the afternoon was a Leadership Masterclass led by Haragopal Mangipudi, the founder of guNaka, renowned keynote speaker, and author. The session, specifically tailored for CIOs, delved deep into the complexities of modern leadership.

#### **Global CIO Forum Finale: Reflections and Future Outlook**

The event concluded with a reflective session led by Anushree Dixit, Global Head at GEC Media Group, where she recapped the highlights of the forum and discussed the future outlook for the CIO community. Her talk served as a call to action for all attendees, inspiring them to implement the knowledge gained over the course of the forum to shape the future of their organizations.

Anushree also hosted the highly anticipated Day 2 Lucky Draw, adding an element of excitement to the closing moments of the event.

With the formal proceedings concluded, attendees prepared to depart from the hotel to catch their flight to Cape Town. This marked the beginning of the next chapter of their journey as leaders, armed with insights, connections, and strategies gained over the course of the Global CIO Forum.

#### **Day three**

The final day of The World CIO 200 2024 Finale unfolded in Cape Town with a dynamic blend of excitement, exploration, and celebration, offering attendees an unforgettable experience that encapsulated the spirit of innovation, adventure, and connection.

The participants took part in the Harley Davidson Chauffeur Rides. This thrilling experience allowed guests to discover the scenic beauty of Cape Town from the seat of legendary Harley Davidson motorcycles, alongside vintage cars, which offered a nostalgic yet exhilarating touch to the journey. As the riders roared through Cape Town's picturesque routes, braving the rain, the energy was palpable, and the scenic beauty of the Cape left an indelible mark on everyone. This high-octane adventure provided a unique and memorable way to immerse in the natural splendor of the region, blending adventure with exploration.

Following the excitement of the morning rides, attendees were treated to a serene and indulgent picnic and wine tasting at the renowned Simons Restaurant located at Groot Constantia, one of South Africa's most iconic wine estates. The afternoon was marked by relaxation, where participants savored a selection of fine wines while enjoying gourmet delicacies in the peaceful ambiance of the vineyard. Surrounded by lush landscapes and centuries-old winemaking traditions, the wine tasting offered a luxurious pause in the day's activities, giving everyone a chance to unwind and relish Cape Town's culinary and viticultural excellence.

As the day progressed, attendees were given some well-deserved leisure time, allowing them



to relax, explore Cape Town further, or reflect on the week's transformative discussions and experiences. This break provided a personal moment for attendees to recharge before the evening's highly anticipated events.

The highlight of the evening was the electrifying session featuring husband and wife adventurers Chris and Julie Ramsey, who shared their experiences from their pole to pole expedition in an EV.

Their talk, titled "Charged for Change: The Electrifying Journey of Chris and Julie Ramsey," delved into their passion for adventure and sustainability, showcasing how they had overcome challenges along the 17,000 mile route.

In every way, the final day was a fitting conclusion to The World CIO 200 2024 Finale, blending adventure, relaxation, insightful discussion, and celebration. The day left participants with a profound sense of community and a shared commitment to innovation and transformation in the tech world. The finale will be remembered not only for its high-profile speakers and engaging activities but also for the inspiration and connections it fostered among the global CIO community.

# OVERLOOKING THE FUNDAMENTALS: THE HIDDEN PITFALLS IN HIGH-END CYBERSECURITY ENVIRONMENTS

The cybersecurity sector has grown steadily and quickly in the past few years. Organizations seek more complex tools and techniques such as artificial intelligence (AI), machine learning, and zero trust to keep up. Such technologies are presented as enterprise-grade with set-up security that provides dynamic protection against new threats. At the same time, by implementing such progressive instruments, an organization might miss basic levels of cybersecurity, thereby producing opportunities for possible attacks. Any high-tech security systems in place can be rendered ineffective if their simple supporting features are blown off.

## The Basics: What are They? Why Do They Matter?

At the heart of cybersecurity are fundamental principles critical for ensuring an organization's secure environment. Integers such as

**KHALED AL TENEJI,**  
Head of Cyber Security  
Operation Center,  
Ministry of Interior







routinely updating the software and setting complex passwords for the organization's employees are among the basics. For instance, ensuring that every installed software has an updated version with vulnerabilities associated with patches will go a long way to avoiding such a problem.. Strict password policies and multi-factor authentication are other measures that enhance security when attacking the system from an external source, which is almost impossible. At the same time, training employees raises awareness of the dangers associated with phishing.

Another overlooked fundamental component of cybersecurity is network segmentation, isolating a network into components to prevent the breaches from spreading. This can help mitigate damage and contain an attacker in a single network section. Data backups are also essential to protect against ransomware since information and files in a backup can be recovered without falling for a ransomware attack. All these practices may sound simple and perhaps even obvious to a layperson, but they embody the building blocks of a sound cybersecurity regime.

### Common Pitfalls: Where Organizations Go Wrong

It is common for organizations to over-rely on automated systems, thinking that the technology alone can solve it all regarding security. Even though automation helps greatly, it cannot debilitate the human element of decision-making and

supervision.. These systems lack close supervision, so critical signs of the breach will be unnoticeable, and the attackers will sustain unnoticed vulnerabilities.

There is also ignorance regarding updating or patching systems on time. Hackers always seize the best opportunity and take advantage of the vulnerability they know is open, and it is always embarrassing if an organization takes time to apply patches. One example is the WannaCry ransomware attack in 2017 that targeted thousands of organizations globally. The attack targeted a Windows system flaw that the software giant Microsoft had addressed, but many firms had not yet addressed it even though the patch was available.

Another common source of failure is the lack of proper employee training. A simple click on a link in a phishing e-mail or other similar tricks can easily defeat sophisticated security measures. Education is, therefore, critical to ensuring employees know the current threats and how they can be avoided. The final issue that deserves consideration is that people quickly get used to having sophisticated security systems in their homes or offices. It contributes to organizational complacency, which leads to reliance on advanced technologies and failure to take care of basic things. Such confidence is evident, especially given the high-profile data breaches that occurred, for example, at Target in 2013.. They did an excellent job in protecting their network from external threats and intruders, but Target did not have proper network segmentation, and hence,

attackers could breach the security measures and access the customers' data.

### Balancing the Basics with Advanced Technologies

In essence, to have a competitive and effective cybersecurity strategy, relying only on fundamental measures is impossible, but equally, it is not enough to adopt only spectacular technology solutions. Thus, the protection strategy must assume a multilayered model with both components integrated into the working process. Simple things such as audits and assessments of the current security will not allow the basics to be forgotten as new technologies are incorporated. Organizations should also define policies regarding updates for the software, training the employees, and handling the incidents to make it clear that those are pillars of their security approach. Conclusion: The Foundation of a Secure Future

Cybersecurity is a crucial practice today, but fundamental cybersecurity measures are still relevant even as newer and improved solutions are being developed. It is imperative that organizations also understand that even with all the high-tech controls that are put up, the basics of defending a network are the stepping stones to developing a protective shield for tomorrow. Therefore, by continuously revisiting and practicing these fundamental measures, organizations can achieve targeted security architecture encompassing new and old threats. ➡

# SECURE BY DESIGN

## **? Can you explain SolarWinds' "Secure by Design" initiative and how it differs from other security frameworks in the industry?**

Since January 2021, SolarWinds has been championing Secure by Design, which sets the cybersecurity gold standard by focusing on people, infrastructure, and software development, to enhance the strength of the company's security framework. What's fundamentally different with our approach is that we recognise the need for action by the industry as a whole. Consequently, with Security by Design, we are not only establishing SolarWinds as a trusted leader in enterprise software security, but by releasing components of this system as open source, we are advancing the cyber security maturity of the IT industry.

Secure by Design also stands apart in its emphasis on continual improvement through least-privilege access methodologies and regular system tests by designated red teams. This framework aims to close gaps, not only in attack detection and prevention, but also in recovery and future-proofing against breaches. In this way, the program is designed to go beyond mere compliance, driving SolarWinds and the broader industry toward a higher standard of resilience and security.

Another defining element of Secure By Design is the SolarWinds Next-Generation Build System. This leverages a unique 'parallel build' process where software is developed in multiple secure, duplicate, and ephemeral environments, by separated teams who work with the same documentation. This makes supply chain attacks more difficult to execute as it prioritizes cybersecurity throughout the entire lifecycle management process.

## **? What specific challenges or lessons from previous cyberattacks shaped the development of the Secure by Design program?**

It's no secret that SolarWinds was targeted in the SUNBURST attack through a new type of sophisticated cyberattack where malware was used to monitor company systems and automatically inject malicious code into the company's legitimate code before it was made available to customers.

This attack made us reassess and redesign our entire software development model, which has culminated in our adoption of the

A portrait of Sascha Giese, a man with a beard and glasses, wearing a blue shirt. The portrait is positioned on the left side of the page, partially overlapping the text.

**SASCHA GIESE,**  
Global Technical Evangelist,  
Observability  
SolarWinds



aforementioned Next-Generation Build System and its unique parallel build process.

A key learning from this attack, which was highlighted by independent experts, was that it's nearly impossible for any one company to stop sophisticated, motivated, and well-funded nation-state actors. This is why with Secure by Design, we have championed an approach that does not only seek to benefit SolarWinds, but the entire industry. This is best evidenced in the fact that we have been releasing components of our Next-Generation Build System as open source, building out a community approach to support cyber resiliency, and being committed to improving overall security through transparency.

**? How does the Secure by Design initiative address the evolving threat landscape, particularly in securing the software development lifecycle?**

One of the main steps we have taken to secure our software development lifecycle has been to embrace the best practice of maintaining detailed Software Bill of Materials (SBOMs). These can play a crucial role in protecting against and preventing these types of attack by providing a fine-grained list of components and interdependencies, including open-source and third-party components. Since they provide a detailed inventory of all the software components and transitive dependencies within a system, they make it easier to quickly identify unusual or unauthorized components that might indicate living-off-the-land tactics.

**? What are the top**

**cybersecurity threats businesses in the MENA region face today, and how do you recommend they prioritize their defences?**

While the scale and sophistication of attacks continues to grow, there are no standout 'big surprises'. Attackers remain true to their tried and tested techniques which are still all over the place. For example, businesses are still dealing with ransomware attacks, and this continues to prove challenging for those that fail to implement a robust backup and recovery program.

In addition, spearhead phishing has become more popular again. This is partly the fault of us as individuals, as many of us tend to share too much personal information in the public domain, and criminals use this to impersonate us or persons close to us to achieve their goals. As each employee is part of the extended security team, proper training should be provided by the IT team to create awareness to mitigate this particular risk. In fact, I would deem this mandatory for C-suite executives who in many ways hold the proverbial keys to the kingdom.

**? How has the threat landscape evolved over the past year, especially with the increased adoption of cloud technologies and remote work?**

Since the first days of cloud adoption, the black hats have used them for the very same reasons as a traditional company: high availability, theoretically unlimited resources, and a choice of locations to make an attack more difficult


to detect, as it could come from Arizona, Amsterdam, or Singapore.

As securing cloud entities is a shared responsibility, we experienced a lot of loopholes in the early days, but over the years, we got smarter. Unfortunately, the situation repeated itself at the start of the pandemic, as organizations equipped their employees to work from home with nothing more than a company-provided laptop. So, IT teams faced a new situation again, which got heavily exploited until businesses learned how to protect their resources in environments that extended well beyond their own four walls.

**? Are there any emerging cyberattack vectors that companies should be particularly aware of as we move into 2025?**

The incorporation of AI into the cybersecurity landscape is an inevitable evolution. Similar to what I just said regarding the cloud, this concept is following a similar path; first, companies started using AI-based solutions, but over time, frameworks became more affordable and accessible. One of the consequences is that, again, criminal organizations and nation-states now use AI-based systems for even more sophisticated attacks. Those systems need less time to discover networks and nodes and continue with cloud entities. They also respond significantly faster to countermeasures, than human actors. But while all of this sounds scary, it's just a continuation of the decades-old game of cat-and-mouse.

**? How important is information sharing across the cybersecurity industry, and what barriers currently exist in facilitating better collaboration?**

Back to our own experience from 2021, we shared our findings and most of our countermeasures with the software vendor community. Even if some of us compete, we shouldn't forget that we're all in the same boat, and attacks on technology providers are daily events. Communication is critical, as all attempts to sweep things under the rug fail sooner or later. As an industry, we have unfortunately seen countless such attempts, and if these have gone on to show anything, it's that they don't exactly win the trust of customers—or should I say ex-customers? 



# AI-DRIVEN DEFENSE

## **? How does Trend Micro's cybersecurity platform provide centralized visibility across clouds, networks, devices, and endpoints, and what benefits does this offer to organizations in terms of threat detection and response?**

Trend Micro's cybersecurity platform, Trend Vision One, provides centralized visibility across clouds, networks, devices, and endpoints by leveraging its Extended Detection and Response (XDR) and Attack Surface Risk Management (ASRM) capabilities. XDR aggregates security data from various sources—such as cloud environments, on-premises networks, endpoints, and mobile devices—into a single, comprehensive dashboard, giving security teams a holistic view of the entire digital infrastructure. This cross-layer integration enables real-time monitoring, detection, and response to threats across multiple vectors. ASRM complements this by continuously assessing the organization's attack surface, identifying vulnerabilities, and providing insights into potential risks. Together, XDR's advanced threat detection and ASRM's proactive risk management empower organizations to detect and respond to threats more effectively while also reducing their attack surface. By filtering out false positives and providing actionable insights, Trend Vision One helps security teams prioritize critical threats, reducing alert fatigue and enhancing the efficiency of their responses. Ultimately, the combined capabilities of XDR and ASRM strengthen the organization's security posture, streamlining both threat detection and response efforts for comprehensive protection. Another key benefit is the continuous updates to threat intelligence that Trend Vision One provides. This ensures that organizations remain equipped to handle evolving threats, enhancing their overall security and compliance efforts.

## **? With your platform protecting over 500,000 organizations worldwide, can you share how Trend Micro tailors its solutions to meet the specific needs of diverse industries?**

Trend Micro recognizes that each industry faces unique cybersecurity challenges, especially in the face of rapid digital transformation and the rise of sophisticated AI-driven threats. As organizations embrace digital

technologies, they encounter new risks such as AI-powered phishing, advanced ransomware, and vulnerabilities in cloud environments, IoT devices, and software supply chains. Additionally, threats from nation-state-sponsored attacks are becoming increasingly complex and harder to detect.

In response, Trend Micro's Trend Vision One platform is designed to be highly adaptable. Our solutions are continuously updated with the latest threat intelligence to address both emerging and existing threats. This proactive approach ensures that our clients, regardless of their industry, benefit from real-time protection tailored to their specific needs. By leveraging our deep expertise and global threat research, Trend Micro ensures that our solutions are finely tuned to meet the diverse requirements of various sectors.

## **? How do your techniques optimize security for environments like AWS, Microsoft, and Google?**

Trend Micro optimizes security for cloud environments like AWS, Microsoft Azure, and Google Cloud Platform through a comprehensive

**BILAL BAIG**  
Regional Technical  
Director, MMEA,  
Trend Micro

suite of techniques designed to enhance protection, visibility, and control. A core component of this strategy is their Cloud Security Platform, which integrates intrusion detection and prevention systems that monitor and block malicious activities in real-time, alongside anti-malware protection that continuously scans workloads to ensure that cloud instances remain secure. This real-time monitoring safeguards critical data and applications from evolving threats while ensuring workloads remain compliant and protected.

Additionally, Trend Micro leverages machine learning for behavioral analytics to detect anomalies in user and entity behavior, facilitating the identification of insider threats and enabling automated responses to security incidents. Continuous risk assessment and regulatory compliance tools further strengthen their security posture, allowing organizations to adapt quickly to evolving threats while maintaining robust data protection. This comprehensive approach ensures that organizations can effectively harness cloud services while safeguarding their critical assets.

API security is another critical area of focus, with Trend Micro monitoring and protecting APIs from unauthorized access and potential data breaches, ensuring secure interactions between cloud services. Their integration with native cloud services enhances security by working seamlessly with the built-in features of AWS, Azure, and Google Cloud, creating a unified and comprehensive security posture. Additionally, by leveraging global threat intelligence, Trend Micro delivers real-time insights into emerging threats, enabling faster, automated responses to incidents. This automation not only reduces response time but also strengthens the overall security efficacy, allowing organizations to securely harness the scalability and flexibility that cloud environments provide.

### **? Can you explain how Trend Micro's approach to earlier detection and faster response helps organizations reduce their overall risk, particularly in complex enterprise environments?**

Trend Micro's approach to earlier detection and faster response is pivotal in managing risk within complex enterprise environments. At the heart of this strategy is our AI-driven Extended Detection and Response (XDR) capabilities within Trend Vision One. By breaking down traditional security silos, our platform provides

comprehensive, real-time visibility across hybrid IT environments, enabling early detection of threats before they can inflict significant damage. Our offerings play a crucial role in this process by automating threat analysis and reducing the noise of irrelevant security events. This results in a 70% improvement in detection and response times, allowing security teams to act swiftly and decisively. Additionally, our platform reduces the volume of false positives by 55%, which helps in focusing resources on the most critical threats. By minimizing network dwell time by 65%, our solution ensures that threats are contained and mitigated rapidly, reducing the overall risk of breaches. This not only protects against immediate threats but also aids in quicker recovery and lessens the impact of attacks, making it an essential component of modern, resilient security strategies.

### **? How does Trend Micro ensure continuous innovation in its cybersecurity solutions to stay ahead of emerging threats and evolving attack vectors?**

At Trend Micro, continuous innovation in cybersecurity is driven by a multi-faceted approach that blends cutting-edge research, advanced technologies, and robust industry collaborations. Trend Micro Research is at the core of this effort, proactively identifying and analyzing emerging threats worldwide. By closely monitoring new vulnerabilities, malware, and attack patterns, our research teams enable real-time protection and the development of effective countermeasures. This proactive approach ensures our solutions evolve alongside the threat landscape, allowing us to stay ahead of cybercriminals and address potential threats before they can impact our customers. Similarly, the Zero Day Initiative (ZDI), one of the world's largest vulnerability research programs, focuses on discovering and disclosing zero-day vulnerabilities—unknown security flaws that attackers could exploit—before they are weaponized. By partnering with global security researchers, ZDI facilitates responsible disclosure and patches, reducing the risk of zero-day exploits.

In addition to research, AI and Machine Learning play a crucial role in enhancing our threat detection and response capabilities. By analyzing massive datasets from diverse sources, our AI-driven solutions improve threat prediction, automate responses, and prevent sophisticated attacks, offering deeper insights and more accurate defenses. Cross-industry

collaborations with partners, governments, and academia further fuel our innovation, enabling us to stay ahead of emerging trends and shape the future of cybersecurity. Together, these elements position Trend Micro solutions to not only respond to current threats but also anticipate and prepare for future challenges, providing comprehensive protection across a wide range of digital environments.

### **? How does Trend Micro leverage AI in its platform, and what role does it play in enhancing threat detection and response?**

Trend Micro leverages AI extensively within its platform, employing innovative tools like the Trend Vision One Companion and Deepfake Inspector to enhance threat detection and response.

The Trend Vision One Companion serves as a generative AI security assistant, specifically designed to bolster the effectiveness of cybersecurity teams. Its capabilities include generating actionable insights from alerts, crafting precise search queries tailored to specific threats, and interpreting complex attacker scripts. By simplifying intricate tasks and bridging the expertise gap, this AI tool significantly boosts the competency and efficiency of security teams, allowing them to respond to incidents more effectively.

On the other hand, the Deepfake Inspector addresses the rising threat of AI-driven deepfakes, which can lead to identity theft and financial fraud. This tool employs advanced behavioral analysis techniques that surpass traditional detection methods, enabling it to identify deepfakes more reliably. By providing real-time alerts, the Deepfake Inspector ensures that organizations can proactively address this evolving threat, safeguarding their assets and maintaining trust with customers and stakeholders.

Together, these AI-driven innovations make Trend Micro's platform agile and capable of tackling both current and emerging cyber risks. By enhancing the accuracy of threat detection and streamlining response processes, Trend Micro not only fortifies the overall security of organizations but also empowers security teams to operate more efficiently. This comprehensive integration of AI solutions positions Trend Micro as a leader in adaptive cybersecurity, providing robust protection across various digital environments and enabling organizations to stay ahead of an increasingly sophisticated threat landscape. ➡



# EMPOWERING GROWTH

## **? What is Amiviz's approach to identifying and capitalizing on emerging IT trends?**

AmiViz's approach to identifying and capitalizing on emerging IT trends is centered on continuous market analysis, strategic partnerships, and a commitment to innovation. We closely monitor global technology developments and industry shifts, allowing us to anticipate and respond to the latest trends. By maintaining strong relationships with leading technology vendors and engaging in collaborative discussions, we gain early insights into groundbreaking solutions and advancements. Additionally, we actively participate in industry events, forums, and think tanks to stay informed about new trends and

technologies. This proactive approach enables us to quickly integrate emerging solutions into our portfolio, ensuring that our customers and partners have access to the most advanced and effective Cybersecurity tools. Our focus on training and skill development for our partners also ensures that they are equipped to leverage these new technologies, allowing us to capitalize on market opportunities and drive growth in a rapidly evolving IT landscape.

## **? What innovative cybersecurity solutions will AmiViz showcase at GITEX 2024, and how do they address emerging threats in the Middle East and Africa region?**

At GITEX 2024, AmiViz will showcase a range of innovative cybersecurity solutions designed to tackle the emerging threats specific to the Middle East and Africa region. These solutions include advanced AI-powered threat detection systems, zero-trust security frameworks, and next-generation endpoint protection technologies.



**ILYAS MOHAMMAD**  
COO  
AmiViz



Our offerings are tailored to address the region's unique cybersecurity challenges, such as increasing ransomware attacks, sophisticated phishing schemes, and growing vulnerabilities in cloud environments. By integrating these cutting-edge technologies, AmiViz empowers businesses in the region to enhance their security posture, protect critical assets, and respond swiftly to evolving cyber threats, ensuring resilience in an increasingly complex digital landscape.

**? How does AmiViz support vendors and resellers in localizing cybersecurity solutions to meet the unique regulatory and market needs across the Middle East and Africa region?**

AmiViz supports vendors and resellers in localizing cybersecurity solutions by providing deep regional expertise and tailored strategies that align with the unique regulatory and market needs of the Middle East and Africa.

We collaborate closely with vendors to adapt their technologies to comply with local data protection laws and industry standards.

Additionally, we offer specialized training and support to resellers, enabling them to effectively address the specific cybersecurity challenges faced by businesses in the region. Through our strong local presence and knowledge, we ensure that solutions are both relevant and compliant, driving successful adoption across diverse markets.

**? With the AI-powered platform, how does AmiViz enable channel partners to identify and capitalize on up-sell and cross-sell opportunities to maximize revenue?**

AmiViz's AI-powered platform equips channel partners with advanced analytics and insights to identify up-sell and cross-sell opportunities. The platform analyzes customer data and usage patterns to highlight potential needs for additional or complementary solutions.

Partners can tailor their offerings to align with customer requirements and preferences. This targeted approach not only enhances the effectiveness of sales strategies but also maximizes revenue by uncovering

opportunities for expanding existing accounts and introducing new solutions, ensuring that partners can optimize their sales performance and drive growth.

**? What investment areas are you focusing on to drive future growth and innovation?**

AmiViz is focusing on several key investment areas to drive future growth and innovation. We are heavily investing in advanced cybersecurity solutions, AI technologies, and cloud computing to stay ahead of industry trends and meet evolving customer needs. Additionally, we are enhancing our partner training programs. Investments in cutting-edge technology and strategic partnerships are central to our strategy, ensuring that we continue to deliver innovative solutions and maintain our leadership position as focus Cybersecurity distributor.

AmiViz is heavily investing in resources across the region to support our partners and customers with innovative technologies. Our major investment is focused on Saudi Arabia, where we are expanding our team to better serve the growing demand for cutting-edge IT solutions and support.

**? How does AmiViz plan to expand its partner network and enhance its AI-driven platform capabilities for cybersecurity at GITEX 2024, particularly in addressing the needs of government and large enterprises?**

At GITEX 2024, AmiViz plans to expand its partner network by actively engaging with new and existing partners, particularly targeting government agencies and large enterprises. We will showcase our advanced AI solutions that address complex cybersecurity needs, such as threat detection, incident response, and compliance management. By demonstrating our platform's ability to provide tailored, scalable solutions, we aim to attract partners interested in leveraging these capabilities to serve high-profile clients.

Our goal is to build strong partnerships, enhance our platform's functionalities, and provide comprehensive solutions that meet the rigorous demands of these critical sectors. Please visit us at Gitex in Cybervalley, Hall 24, stand A45. [🔗](#)



# NEXT-GEN OBSERVABILITY

**Go beyond traditional  
IT monitoring.**

Actionable, AI-powered insights  
across any environment.

 Observability

 Network

 Systems

 Database

 ITSM

 Application

 IT Security



# FUTURE-PROOFING CYBERSECURITY

**? What emerging cybersecurity threats do you believe pose the greatest risk to organizations globally in the coming years?**

Looking ahead, the most concerning cybersecurity threats will stem from increasingly sophisticated cybercriminal activities, particularly ransomware and supply chain attacks. Ransomware has evolved beyond simply locking down data—it now threatens companies with extortion schemes that involve data leaks. Having led cybersecurity efforts at Makita Gulf FZE since 2009, I've seen how these

threats shift tactics, targeting vulnerabilities in critical infrastructure and financial systems. State-sponsored cyber activities are also of growing concern, with attacks becoming more disruptive as geopolitical tensions rise. Additionally, AI-powered cyber-attacks present an alarming future risk, where machine learning is leveraged to develop adaptive and elusive malware. As the cybersecurity landscape continues to evolve, organizations must remain vigilant, constantly

**MOHAMMED NABEEL ZUBAIR**

Senior Cyber Security & Risk  
Compliance Engineer,  
Makita Gulf FZE



updating their defenses to address these sophisticated threats.

**? How should organizations prepare for the growing challenges of securing the Internet of Things (IoT) and other connected devices?**

Securing IoT devices requires a multi-faceted approach that incorporates endpoint security and network segmentation. At Makita, we quickly recognized the importance of securing our IoT environment through robust monitoring systems, regular firmware updates, and strict access controls. Organizations must implement a layered defense model that includes device authentication, encryption, and real-time traffic monitoring. Secure design principles should be embedded in IoT devices from the development stage. Furthermore, selecting vendors that adhere to rigorous security standards and continually assessing the security posture

of connected devices are critical steps to mitigate IoT-related risks.

**? What role do you see artificial intelligence and machine learning playing in both enhancing and compromising cybersecurity efforts?**

AI and machine learning are transforming cybersecurity. In my role at Makita, we've integrated AI-driven solutions into our SOC, enabling us to automate threat detection and response, and significantly reduce reaction times. On the flip side, malicious actors are leveraging AI to enhance phishing attacks, create sophisticated malware, and automate attacks. One particular area of concern is the use of AI-generated deepfakes in social engineering attacks, which can trick employees into revealing sensitive information. To balance the benefits and risks of AI, it's crucial to stay ahead of AI-driven threats while leveraging the

technology to strengthen our defenses.

**? How can companies ensure effective collaboration between the public and private sectors to tackle large-scale cyber threats?**

Collaboration between the public and private sectors is crucial to combating large-scale cyber threats. Open communication and intelligence sharing have proven to be essential in strengthening defenses. Makita has participated in several public-private partnerships, which have significantly improved our incident response strategies. Formalized channels for threat intelligence sharing and collaboration on cybersecurity frameworks can bolster both private organizations and government agencies. Regular engagement between the sectors fosters trust, leading to stronger collective resilience against cyber threats.

**? What are the key**





### **considerations for organizations when it comes to protecting sensitive data in a multi-cloud environment?**

In a multi-cloud environment, organizations must implement comprehensive data protection strategies across all cloud platforms. At Makita, we focus on ensuring strong governance, encryption, and data visibility. Clear data ownership, encryption at rest and in transit, and consistent identity and access management controls across platforms are critical. Automated monitoring tools that provide real-time visibility into cloud activities are essential to detect and mitigate security breaches. Regular audits and compliance checks further ensure data protection across multi-cloud environments.

### **? How do you foresee the role of the CISO evolving as cybersecurity becomes more integral to business strategy?**

The role of the CISO is shifting from a purely operational function to a strategic

leadership position that aligns with business objectives. At Makita, cybersecurity has become a core component of our business strategy. As digital transformation accelerates, the CISO must act as a key advisor to the executive team, ensuring that cybersecurity risks are managed in alignment with business goals. The future CISO will need to develop a broader business acumen, balancing security with innovation while fostering a company-wide culture of security awareness.

### **? What steps can organizations take to mitigate the risks associated with supply chain cybersecurity vulnerabilities?**

Supply chain vulnerabilities pose significant risks, particularly when relying on third-party services. At Makita, we have implemented rigorous vendor management processes, including security audits and enforcing cybersecurity standards. Organizations must ensure that security requirements are enforced throughout the supply chain, from onboarding suppliers to

conducting regular assessments. Network segmentation is another effective measure, limiting third-party access to critical systems and data. Collaborating with suppliers to share threat intelligence and best practices will further enhance supply chain resilience.

### **? In your opinion, what are the most critical skills and competencies future CISOs will need to succeed in an increasingly complex threat landscape?**

The future CISO will need to be a multi-disciplinary leader, combining technical expertise with strategic management skills. They must stay abreast of emerging technologies such as AI, cloud security, and blockchain while maintaining strong leadership and communication skills to manage teams and advocate for cybersecurity at the executive level. Cultivating a security-first culture and proactive risk management will be essential. Additionally, continuous learning and adaptation to the evolving threat landscape will be vital for future CISOs to successfully lead their organizations through cybersecurity challenges. ➡



# THE SHIFTING SANDS OF CYBERSECURITY

## ? What emerging cybersecurity threats do you believe pose the greatest risk to organizations globally in the coming years?

Cybersecurity is a strategic priority that can no longer be isolated from the IT department and other departments. Gartner has predicted that by 2026, 70 percent of boards will include at least one member with expertise in the field. This enables organizations to move beyond reactive defense, meaning that they can act on new business opportunities that come with being ready.

So Cyber threats are expected to continue to evolve and advance in the coming years as technology advances, and security experts point to the possibility of new challenges and threats emerging in the future.

Perhaps I will focus on the most important attacks from my point of view :

### • AI and Machine Learning Threats

These technologies automate attacks, create more convincing phishing emails, and even identify vulnerabilities in target systems. Which increases the level of risk and the need for advanced technologies to detect it.

### • Regulatory and Compliance Challenges

The evolving digital threat landscape has prompted governments and regulatory bodies to introduce new cybersecurity regulations and standards. Organizations now face greater pressure to comply with these requirements, but achieving and maintaining compliance can be challenging, given the dynamic nature of digital threats.

### • Third-Party Exposure

Many third parties tend to be much less secure than the major companies they work with & this prompts attackers to exploit less secure environments to achieve their goals.

### • Social Engineering

Social engineering remains one of the most risk hacking techniques employed by cybercriminals, largely because it relies on human error rather than technical vulnerabilities. This makes these attacks all the more dangerous because it's a lot easier to trick a human than it is to breach a security system.

## ? How should organizations prepare for the growing challenges of securing the Internet of Things (IoT) and other connected devices?

The proliferation of IoT devices has led to unprecedented levels of connectivity and data collection. From smart home devices like thermostats and security cameras to industrial sensors and autonomous vehicles, IoT technology has permeated every aspect of our lives and businesses.

**MOHAMMED ALSHAMRANI,**  
Cyber Security Lead  
Cyberani

While IoT offers immense benefits such as improved efficiency, real-time monitoring, and enhanced customer experiences, its rapid growth also presents significant security challenges. For example: different security Vulnerabilities, unencrypted traffic, secure firmware updates, Data Privacy and Integrity, lack of Standardization and so on.

Addressing the challenges posed by IoT security requires a multi-faceted approach, integrating technology, policy, and collaboration among stakeholders. Here are some innovative solutions to enhance IoT security:

#### • Secure-by-Design Principles

Implementing secure-by-design principles involves integrating security features into IoT devices from the design phase. This includes hardware-based security modules, cryptographic protocols, and secure boot mechanisms to prevent unauthorized access and tampering.

#### • Blockchain for IoT Security

Blockchain technology offers a decentralized and tamper-resistant platform for securing IoT data and transactions. By leveraging blockchain's immutability and consensus mechanisms, IoT networks can enhance data integrity, authentication, and access control.

#### • AI-Powered Threat Detection

AI and machine learning algorithms can analyze vast amounts of IoT data in real time to detect anomalies and potential security threats. By employing AI-driven threat detection systems, organizations can proactively identify and mitigate security risks before they escalate.

#### • Collaborative Security Frameworks

Collaboration among industry stakeholders, including device manufacturers, software developers, regulators, and cybersecurity experts, is essential for developing comprehensive IoT security frameworks.

All IoT Initiatives promote knowledge sharing, best practices, and standards development to address evolving IoT security challenges.

### ? What role do you see artificial intelligence and machine learning playing in both enhancing and compromising cybersecurity efforts?

Traditional security measures are no longer sufficient in combating sophisticated cyber-attacks. This is where Artificial Intelligence (AI) steps in, from its ability to analyze vast amounts of data and identify patterns that may indicate malicious activity. With the ever-increasing volume and complexity of cyber threats, human analysts alone cannot keep up with the speed

and accuracy needed to detect and respond effectively.

AI-powered systems can continuously monitor networks, endpoints, and user behavior, quickly spotting anomalies or suspicious activities that would have otherwise gone unnoticed. By leveraging machine learning algorithms, these systems can adapt and evolve over time to stay one step ahead of hackers.

Furthermore, AI enhances threat detection by automating tedious tasks such as log analysis and vulnerability scanning. It frees up valuable time for security professionals to focus on more critical aspects of incident response rather than getting overwhelmed with manual processes. In addition to improved threat detection capabilities, AI also enables real-time response mechanisms. When an attack occurs, AI algorithms can rapidly assess the situation based on predefined rules or through self-learning capabilities derived from historical data sets. These automated responses can include isolating affected devices or users from the network, blocking suspicious IP addresses automatically, or even initiating countermeasures against attackers in real time without human intervention.

Utilizing AI technologies in cybersecurity practices brings several advantages to organizations:

#### • Enhanced Speed

AI-powered systems work at lightning-fast speeds compared to humans when processing large volumes of data.

#### • Improved Accuracy

The machine learning models used by AI platforms continually learn from past incidents which results in better identification of potential threats.

#### • 24/7 Monitoring

Unlike humans who require rest breaks or sleep at night hours — machines are always alert making them ideal for continuous monitoring.

#### • Scalability

As the volume of data grows, AI can scale effortlessly to handle the increasing workload.

### ? How can companies ensure effective collaboration between the public and private sectors to tackle large-scale cyber threats?

Public-private collaboration is important beyond just responding to the cyber threat of the day. They can also help promote the institutional framework that we collectively use to fight this ever-growing threat, and more cyber threats

inevitably challenge our overall cyber resilience, we'll need more collaborations

The public sector also plays a key role in regulating the structure and setting the rules to be followed in collaboration development. and new regulations and developing coordinated procedures would increase stakeholders' understanding and enable them to deal with cyber threats more effectively.

In Additional, the private sector can recognize the industry a need and works on a collaborative method to set up the partnership.

The issues and success factors of effective collaboration must be considered. In addition, both the private and public sectors need incentives and motivation to share information and address the cyber threats.

### ? What are the key considerations for organizations when it comes to protecting sensitive data in a multi-cloud environment?

In today's digital world, many organizations use multiple cloud services to store and manage their data. This approach, known as a multi-cloud environment, offers numerous benefits but also has different challenges, particularly concerning data privacy, as data is stored off-site and accessed over the internet, it becomes vulnerable to cyber threats, unauthorized access, and potential breaches. Ensuring the confidentiality, integrity, and availability of sensitive information in the cloud is a critical challenge that requires robust security measures and vigilant oversight. Therefore, when using this approach, some security measures be taken into consideration related to:

**Data Encryption** : encryption ensures that data is unreadable to unauthorized users, both at rest and in transit and when selecting a cloud service provider, it is essential to verify that they offer comprehensive encryption options.

**Access Control and Identity Management:** Proper access control mechanisms are important to ensure that only authorized personnel can access sensitive data.

Through a combination of advanced authentication methods, stringent access control policies, and regular reviews, organizations can Enhance their defenses against unauthorized access and safeguard their sensitive information and data privacy in the cloud environment.

#### **Data Governance and Compliance :**

Understanding where your data is stored and processed is vital for compliance with data protection regulations and different jurisdictions have varying requirements for data privacy, and



it is essential to ensure that your cloud service provider complies with relevant regulations. And data governance policies can help in maintaining control over the geographic location of your data.

#### **Vendor Management and Security**

**Policies:** Cloud service providers and third-party vendors play a crucial role in your overall security posture. Ensuring that vendors adhere to strict security policies and regularly reviewing their security practices is essential for maintaining data privacy.

### **? How do you foresee the role of the CISO evolving as cybersecurity becomes more integral to business strategy?**

The CISO Role Changing!

Although the role of the CISO now can vary widely across organizations depending on their size and nature, however, with the evolution of the cybersecurity landscape, this role has transformed from a purely technical role to a leadership role, tends to lean much further into executive leadership and risk management, with a prime responsibility to keep C-Level in touch with security risks relating to organizational objectives, strategy and business outcomes. To smoothly transition from a technical to a leadership role, CISOs also need to have good business decision-making and communication skills. They should no longer wait for a security incident to occur, rather, they should adopt a proactive approach to identify and mitigate risks. Moreover, it is also the need of the hour for the CISOs to align and integrate all of their strategies with enterprise risk management to make more accurate decisions.

### **? What steps can organizations take to mitigate the risks associated with supply chain cybersecurity vulnerabilities?**

The day-to-day operations of a supply chain are complex and require the accurate delivery of products and services at the right time. Organizations may have to deal with serious operational, financial, or reputational issues if something interferes with these processes. The large scale of a modern supply chain increases the potential for security vulnerabilities to emerge at some stage of it, resulting in attack vectors across a large attack surface. Cyber Security is more important than ever, given that a single security incident affecting a third-party vendor can have catastrophic consequences for other organizations further down the supply

chain.

Here some controls to Mitigate Supply Chain Security Threats :

#### **• Mitigating Vulnerabilities and Penetration Testing**

Vulnerability scans enable early detection of low-level vulnerabilities and a penetration testing team can help identify more advanced threats within the supply chain and improve the overall security system.

#### **• Identifying and Encrypting Data**

A data discovery tool can help identify and classify files containing sensitive data, and customer data. With a comprehensive view of all the company's data, hence, to secure valuable assets with advanced encryption.

With more businesses relying on online platforms and transactions, advanced controls such as digital signatures and MFA can enhance supply chain security.

#### **• Planning for Incident Response**

It is important to prepare for breaches, attacks, or incidents by establishing an effective incident response plan. A well-tested, practical, easy-to-implement response plan and deployable remediation actions help minimize losses, reputational damage, and customer churn rates.

#### **• Managing Third-Party Risk**

Understanding third-party risk allows organizations to identify the potential impact on their operations due to inadequate monitoring and failure to comply with data security regulations.

Getting approval from C-Level is critical to be sure third-party risk is top of mind and being taken seriously.

### **? In your opinion, what are the most critical skills and competencies future CISOs will need to succeed in an increasingly complex threat landscape?**

At its core, the CISO leads defending an organization security and threats, ensures that all parts of the organization understand the value of Cyber security, and aligns security policies with overall business objectives.

Therefore, it is important to have some skills and competencies that help him achieve that and here some modern critical skills CISOs Need to success.

#### **• Passion for Learning**

The new advance technologies, from generative AI, IoT to quantum computing, offers both opportunities and risks in cybersecurity. Therefore, it is vital that security leaders stay up to date in their knowledge of the technology

landscape and the threats that may be evolving alongside these developments, in addition to stay abreast of the latest concepts in cybersecurity.

#### **• Team Management**

Amid the cyber skills gap and growing pressures on security teams, issues like stress and burnout have become prevalent, including among CISOs. This in turn has led to a high rate of turnover in cybersecurity roles, with many professionals considering leaving the sector altogether.

And retention is an increasing challenge for CISOs. That's why it's important to provide personalized training and development opportunities is vital for keeping employees motivated and happy in their current teams.

#### **• Business Knowledge and Understanding**

As well as understanding the technical components of cybersecurity, it is vital that CISOs have an in-depth understanding of the business they work in. There are a variety of ways CISOs can garner such an understanding. One is taking formal business education and courses.

#### **• Networking and Relationship Building**

It is important that security leaders take the time to speak to people throughout the organization to understand their role. This will help them develop appropriate security controls that are effective.

Security leaders will also need to coordinate closely with other departments in the event of a cybersecurity incident, such as HR and legal. Regular exercises should be conducted to practice how responses are coordinated.

#### **• Communication**

Usually CISO obtaining the largest possible budget from the business and must be able to communicate clearly how that budget is to be allocated and if an increase is required.

CISOs must be able to explain cyber risks, and the work of the security team, to the board and C-level. This means having a clear message that can be communicated to a non-technical audience.

They must understand fundamental business concepts and be able to communicate in a language that executives will understand and pay attention to. For example, how cyber-attacks can impact business bottom lines, such as market share and loss of reputation.

This information should be presented in a manner business leaders are used to – concise points that highlight important statistics. If the boardroom properly understands how cyber incidents can damage business goals, and the important work of the security team in preventing this, they will be much more likely to provide more support to the CISO, financially and otherwise. 🔗

# IMPLEMENTING STRONG CYBERSECURITY

## **? What emerging cybersecurity threats do you believe pose the greatest risk to organizations globally in the coming years?**

The world of cybersecurity is always evolving, with cybercriminals constantly finding new and more persistent ways to exploit vulnerabilities. One significant evolution is seen in ransomware attacks, which have moved beyond simply encrypting data and demanding a ransom. Modern ransomware involves data exfiltration and threats of public disclosure, disrupting business operations and damaging reputations. The major threats faced by the organizations include:

- 1.) Operational disruption
- 2.) Cyber espionage
- 3.) Phishing attacks
- 4.) Unauthorized third-party access
- 5.) Insider threats
- 6.) Ransomware
- 7.) Cloud based attacks due to insecure Cloud connections..

## **? How should organizations prepare for the growing challenges of securing the Internet of Things (IoT) and other connected devices?**

Organizations face significant challenges in securing the Internet of Things (IoT) and other connected devices

due to the increasing complexity and scale of these systems. To effectively prepare for these challenges, organizations should adopt a comprehensive strategy that encompasses various security measures, best practices, and regulatory considerations.

**NAMAN TALDAR,**  
Regional Lead (OT Cyber  
Security) - META,  
Rockwell Automation







### Key Challenges in IoT Security

Device Vulnerabilities.

Lack of Standardization

Data Privacy Risks

Integration Challenges

Physical Security Threats

Best Practices for Securing IoT Devices

Implement Strong Authentication:

Organizations should enforce robust authentication mechanisms, including multi-factor authentication and regular password updates, to protect against unauthorized access.

Regular Software Updates: Keeping firmware and software up to date is crucial in mitigating vulnerabilities. Organizations should establish a patch management process to ensure timely updates are applied.

Data Encryption: Encrypting data both at rest and in transit helps protect sensitive information from interception and unauthorized access.

Network Segmentation: Segmenting IoT devices from core business networks can limit the potential impact of a security breach. This approach helps isolate vulnerabilities and reduces the attack surface.

Continuous Monitoring: Implementing tools for real-time monitoring and threat detection can help organizations identify potential breaches before they escalate into serious incidents.

Utilize Advanced Security Solutions:

Employing advanced technologies such as

digital twins and public key infrastructure can enhance the overall security posture by providing integrity, authentication, and encryption across IoT ecosystems.

### **? What role do you see artificial intelligence and machine learning playing in both enhancing and compromising cybersecurity efforts?**

While artificial intelligence (AI) has enabled cybercriminals to expand their capabilities, it has also emerged as a powerful tool in the fight against cyber threats. AI's capabilities in threat detection and response have revolutionized cybersecurity practices.

Machine learning algorithms analyse vast amounts of data to identify patterns and anomalies that may indicate a cyberattack. There are multiple solutions that leverage AI capabilities to detect unusual patterns of behavior within networks, identifying anomalies that may indicate potential cyber threats. Advanced AI-driven systems assist security analysts in investigating and responding to these threats with greater efficiency. Additionally, AI solutions analyze user behavior to identify and mitigate insider threats, using machine learning algorithms to detect deviations from typical activity patterns, thereby enhancing overall security posture.

Organizations face significant challenges in protecting sensitive client data from

increasingly sophisticated cyber threats.

By implementing an AI-powered threat detection system, they can identify and neutralize threats in real time, enhancing their security posture and improving client trust.

### **? How can companies ensure effective collaboration between the public and private sectors to tackle large-scale cyber threats?**

To effectively tackle large-scale cyber threats, companies can implement several strategies to ensure collaboration between the public and private sectors.

Here are key approaches:

1. Establish Public-Private Partnerships (PPPs)

Public-private partnerships are essential for leveraging the strengths of both sectors. Governments can provide regulatory frameworks and incentives, while the private sector contributes technical expertise and innovation. These partnerships facilitate the exchange of resources, information, and best practices, creating a collaborative environment to address cyber threats more effectively.

2. Enhance Information Sharing

A critical component of effective collaboration is robust information sharing about cyber threats, vulnerabilities, and attack techniques. Establishing trusted

platforms for this exchange allows organizations to enhance their situational awareness and respond proactively to emerging threats.

### 3. Foster Collaborative Research and Development

Joint research initiatives can drive innovation in cybersecurity technologies and methodologies. By pooling resources and expertise from academia, industry, and government, stakeholders can develop advanced tools to combat evolving cyber threats. This collaboration ensures that cybersecurity professionals are equipped with the necessary skills to address future challenges.

### 4. Conduct Training and Simulation Exercises

Regular training exercises that involve both sectors can improve preparedness for cyber incidents. These exercises should go beyond theoretical discussions to include practical scenarios that test response capabilities.

**5. Promote International Cooperation** Cyber threats often cross national borders; therefore, international collaboration is essential. Governments should work with global organizations to establish common frameworks for information sharing and joint incident response efforts. This cooperation can enhance global cybersecurity resilience against transnational cybercrime.

By implementing these strategies, companies can foster a more effective collaborative environment with public sector entities, significantly enhancing their ability to combat large-scale cyber threats.

## ? What are the key considerations for organizations when it comes to protecting sensitive data in a multi-cloud environment?

When it comes to safeguarding sensitive data across multiple cloud platforms, organizations must address several critical considerations:

#### Data Security

- Encrypt data both in transit and at rest using industry-standard protocols like AES 256-bit encryption
- Ensure encryption keys are securely managed and accessible only to authorized personnel
- Implement robust access controls and authentication measures like multi-factor



authentication to prevent unauthorized access

#### Data Governance

- Establish a centralized data governance framework to consistently manage data across clouds
- Classify data based on sensitivity and apply appropriate security controls
- Maintain visibility over data location and access permissions in each cloud environment

#### Compliance

- Understand and adhere to relevant data protection regulations like GDPR, HIPAA, and CCPA in each cloud environment
  - Ensure data residency requirements are met, especially in regions with strict data sovereignty laws
  - Maintain evidence of compliance through centralized monitoring and reporting
- #### Shared Responsibility
- Clearly define security responsibilities between the organization and cloud providers based on the shared responsibility model
  - Ensure security controls are consistently applied across all cloud services, including IaaS, PaaS, and SaaS
- #### Monitoring and Incident Response
- Implement centralized monitoring and logging to detect and respond to security incidents across multiple clouds
  - Establish clear incident response procedures and communication channels with cloud providers

By addressing these key considerations, organizations can develop a robust multi-cloud data protection strategy that safeguards sensitive information, ensures compliance, and enables secure collaboration across cloud platforms.

## ? What steps can organizations take to mitigate the risks associated with supply chain cybersecurity vulnerabilities?

Organizations can take several proactive steps to mitigate the risks associated with supply chain cybersecurity vulnerabilities. Here are key strategies based on best practices:

1. Conduct Regular Security Audits
2. Implement Multi-Factor Authentication (MFA)
3. Keep Software Updated
4. Educate Employees
5. Control Access Through the Principle of Least Privilege
6. Conduct Vendor Risk Assessments
7. Implement a Zero Trust Model
8. Develop an Incident Response Plan
9. Foster Collaboration Across the Supply Chain

By implementing these strategies, organizations can significantly reduce their vulnerability to supply chain cyberattacks and enhance their overall cybersecurity posture. ➡



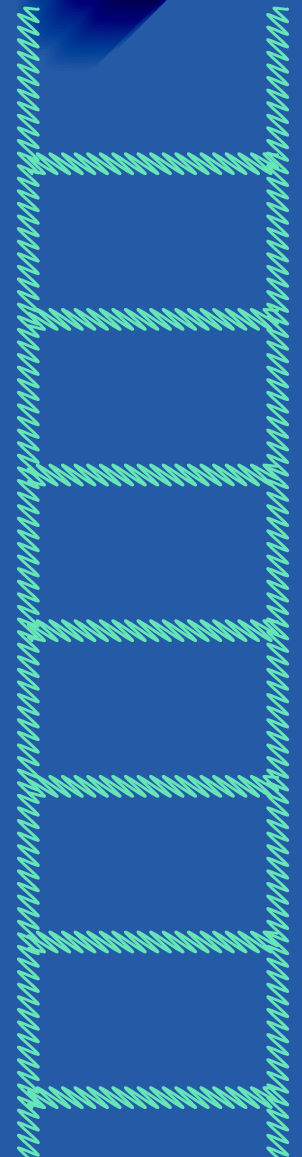
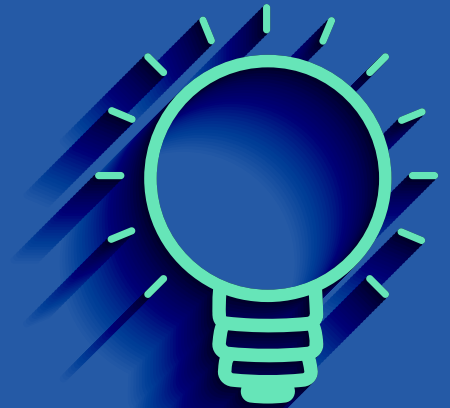
05 NOVEMBER 2024  
UAE

12 NOVEMBER 2024  
KSA

# CPCA

CHANNEL PARTNER CONCLAVE & AWARDS 2024

## POSSIBILITIES THROUGH OPPORTUNITIES



IN ASSOCIATION WITH



BROUGHT TO YOU BY



#CPCAWORLD



CPCAWORLD.COM

Info@gecmidiagroup.com



+ 971 4564 8684

# STRATEGIC LEADERSHIP FOR SUCCESS

## ? What do you consider the most critical priority for a CISO today?

In today's rapidly evolving technological landscape, the role of the CISO has become more crucial than ever. The CISO is not only a custodian of the organization's IT infrastructure but also a strategic leader responsible for driving innovation, ensuring cybersecurity, and fostering a digital-first culture. Among these multifaceted responsibilities, one can argue that the most critical priority for a CISO today is leading digital transformation.

In conclusion, the most critical priority for a CISO today is leading digital transformation. This involves not only adopting new technologies but also transforming business models, processes, and organizational culture. By articulating a clear digital vision, fostering a culture of innovation, managing change effectively, and ensuring robust cybersecurity measures, the CISO can drive digital transformation efforts that position the organization for long-term success. While there are challenges to be overcome, the potential benefits of digital transformation make it a strategic imperative for any organization seeking to remain competitive in today's digital world.

## ? What key factors contribute to the success of a CISO, in your opinion?

The role of a CISO is multifaceted and demanding, requiring a blend of strategic vision, technical expertise, and leadership

acumen. By embodying these key factors, a CISO can effectively navigate the complexities of the digital age, driving transformation

**MOHAMMED FEROZ KHAN,**  
Head of IT Security  
Compliance and Projects  
TOTAL





efforts that position the organization for sustained success. The ability to balance innovation with operational stability, manage organizational change, and prioritize cybersecurity are essential for any CISO aiming to lead their organization through the challenges and opportunities of today's digital landscape.

### **? How do you foster and support collaboration across different departments?**

Fostering and supporting collaboration across different departments is essential for organizational success. By creating a collaborative culture, implementing effective communication channels, leveraging collaborative tools, encouraging cross-functional teams, building trust, and promoting continuous improvement, organizations can enhance teamwork and achieve their goals. The strategies outlined in this document provide a roadmap for building a cohesive and collaborative workplace, ensuring that all departments work together seamlessly toward common objectives.

### **? How do you keep up with the latest innovations and trends in technology?**

In today's rapidly evolving digital landscape,

keeping up with the latest innovations and trends in technology is crucial for both personal and professional growth. The pace at which technology advances can be overwhelming, but with the right strategies and tools, you can stay informed and ahead of the curve. This document outlines effective methods to stay updated with technological advancements and leverage them for success. Finally, maintaining a curious and open-minded attitude is key to staying updated with technology trends. Embrace the unknown, be willing to explore new ideas, and remain adaptable. The tech industry is constantly evolving, and a mindset of continuous curiosity will help you stay engaged and informed.

By implementing these strategies, you can effectively keep up with the latest innovations and trends in technology. Staying informed will not only enhance your knowledge and skills but also position you to take advantage of new opportunities and drive success in your personal and professional endeavors.

### **? How do you strike the balance between operation and innovation?**

In today's rapidly evolving business landscape, organizations are constantly challenged to balance operational efficiency with innovation. While operations ensure the smooth functioning of day-to-day

activities, innovation drives growth and competitive advantage. Striking the right balance between these two aspects is crucial for long-term success. Here are some strategies to achieve this equilibrium: Cultivating a growth mindset within the organization is vital for balancing operation and innovation. Encourage employees to view challenges as opportunities for learning and growth. By fostering resilience and adaptability, you can create an environment where both operational excellence and innovative thinking thrive.

In conclusion, balancing operation and innovation is a dynamic and ongoing process that requires deliberate effort and strategic planning. By fostering a culture of continuous improvement, leveraging technology, encouraging cross-functional collaboration, and maintaining a growth mindset, organizations can achieve a harmonious equilibrium that drives both efficiency and innovation. This balance will not only ensure the smooth functioning of day-to-day activities but also position the organization for long-term success and competitiveness in the ever-changing business landscape.

### **? What are the biggest challenges currently facing CISO, and how would you address them?**

CISO play a critical role in today's rapidly evolving technological landscape. However, they face a myriad of challenges that require strategic thinking and innovative solutions. Here are some of the most pressing issues CISO are grappling with and strategies to address them.

- Cybersecurity Threats
- Data Management and Analytics
- Digital Transformation
- Talent Acquisition and Retention
- Budget Constraints
- Regulatory Compliance

In conclusion, while CISO face numerous challenges in today's dynamic business environment, addressing these challenges with strategic and proactive measures can lead to significant advancements and successes. By focusing on cybersecurity, data management, digital transformation, talent acquisition, budget management, and regulatory compliance, CISO can navigate the complexities of their role and drive their organizations towards sustained growth and innovation. ➡



# PRIORITIZING DATA SECURITY IN THE AGE OF GENERATIVE AI

The rapid advancement of GenAI technologies like ChatGPT and Copilot continue to revolutionize how organizations approach problem-solving, content creation task automation and so much more. These powerful tools not only offer remarkable potential to enhance productivity and drive innovation but also inspire a new wave of possibilities. However, as businesses integrate these technologies into their operations, the need to prioritize data security everywhere becomes essential to mitigate the associated risks.

## Understanding the Cybersecurity Risks and Building a Culture of Cybersecurity Awareness

While GenAI presents numerous opportunities, it also poses

**SAMER DIYA,**  
Vice President  
Forcepoint META





significant cybersecurity challenges that can inadvertently expose sensitive information through user interactions. For example, sharing proprietary data with AI tools can lead to unintentional leaks, similar to risks seen with file-sharing platforms. Additionally, the ability of GenAI to produce compelling fake content, such as deepfakes, can facilitate sophisticated phishing attacks, making it easier for cybercriminals to trick users into revealing confidential information.

To effectively address these challenges, organizations must first foster a culture of cybersecurity awareness among employees. This involves educating staff on the safe use of GenAI tools and clarifying the types of information appropriate to share. By empowering employees to recognize potential risks, organizations can take the first step in strengthening their defenses against AI-driven data breaches and foster a proactive approach to security.

#### Adopting Comprehensive Security Frameworks

Beyond employee education, implementing

robust security frameworks that prioritize data security everywhere is critical to properly safeguard against potential threats. For digital first organizations, implementing a unified solution that leverages the proactive power of Data Security Posture Management (DSPM) with the reactive capabilities of Data Loss Prevention (DLP) solutions can allow security teams to understand how data is stored, used and moved across an organization – while monitoring access to it.

Effective DLP solutions can prevent sensitive information from being shared with generative AI applications, whereas AI-powered DSPM solutions can facilitate the visibility that is repeatedly missing from unstructured AI use. Secure Web Gateway (SWG) and Cloud Access Security Broker (CASB) solutions provide further defenses for users adopting GenAI technologies, ensuring that users only access trusted web applications and avoid sharing data with unknown ones.

All of this can be a lot to take in, which is why Forcepoint recently launched Forcepoint GenAI Security to merge the

information protection capabilities in Forcepoint DSPM and Forcepoint DLP alongside the cloud-based capabilities in Forcepoint ONE Security Service Edge (SSE) that encompasses solutions like CASB and SWG. The solution even integrates with OpenAI to secure data in ChatGPT Enterprise – truly securing data wherever it resides in the AI era.

#### Embracing Innovation with Confidence

As organizations explore the exciting possibilities offered by GenAI, prioritizing data security is paramount. By fostering employee awareness, implementing comprehensive security frameworks and leveraging advanced technological solutions, businesses can harness the benefits of these transformative tools while safeguarding their sensitive information. Maintaining a holistic approach to data security not only equips organizations with the necessary strategies to navigate the future of generative AI confidently but also ensures that innovation and security coexist harmoniously, providing a sense of reassurance and confidence. 🔑

# FROM STRATEGIC THINKING TO CRISIS MANAGEMENT

## ? What emerging cybersecurity threats do you believe pose the greatest risk to organizations globally in the coming years?

Emerging Cybersecurity Threats:

- Ransomware & RaaS: Rising attacks with accessible tools for cybercriminals.
- Supply Chain Attacks: Compromising vendors leads to widespread harm.
- AI-Driven Attacks: Sophisticated, scalable threats using AI.
- IoT Vulnerabilities: Weak security in connected devices, exposing critical systems.
- Cloud Security & Insider Threats: Increased risks from misconfigurations, insider actions.
- Quantum Computing & Deep fakes: Future decryption risks and advanced disinformation tools.

## ? How should organizations prepare for the growing challenges of securing the Internet of Things (IoT) and other connected devices?

To address the growing challenges of securing IoT and

connected devices, organizations should:

- **Develop a Comprehensive IoT Security Strategy:** Assess and define security requirements for all IoT devices.
- **Implement Strong Authentication and Access Controls:** Use multi-factor authentication and network segmentation to

### ABDElMAJED SAEED

CyberTech, Cyber Security Advisor  
– CEO - Business Partner,  
Confidential





restrict device access.

- **Use Encryption and Secure Protocols:** Encrypt data and use secure communication protocols like TLS.
- **Regularly Update Firmware and Software:** Ensure devices are patched and updated automatically when possible.
- **Monitor and Manage IoT Devices:** Use real-time monitoring and centralized device management.
- **Ensure Endpoint Security:** Utilize secure boot mechanisms and Endpoint Detection and Response (EDR).
- **Adopt Zero Trust Architecture:** Assume potential compromise and verify all device access attempts.
- **Prepare Incident Response Plans:** Develop specific plans for IoT security breaches.
- **Educate Employees:** Provide IoT security training and promote security awareness.
- **Collaborate with Manufacturers and Vendors:** Ensure vendors follow industry security standards.
- **Adopt IoT Security Standards:** Align with recognized frameworks like NIST and ISO/IEC 27001.
- **Ensure Legal Compliance:** Stay updated on evolving regulations like GDPR and CCPA.

By adopting these strategies, organizations can protect IoT ecosystems and mitigate potential cyber threats.

## ? What role do you see artificial intelligence and machine learning playing in both enhancing and compromising cybersecurity efforts?

AI and ML play a dual role in cybersecurity, offering both enhanced defences and new vulnerabilities.

### Enhancing Cybersecurity:

- **Threat Detection and Response:** AI/ML analyse large data sets to identify anomalies and improve detection over time.
- **Automation:** AI automates repetitive tasks, freeing security teams for complex challenges.
- **Predictive Analysis:** AI predicts vulnerabilities, enabling proactive defence.
- **Threat Hunting:** AI uncovers hidden threats faster.
- **Endpoint Security:** AI detects malicious behaviour, improving malware prevention.

### Compromising Cybersecurity:

- **AI-Powered Attacks:** AI helps criminals

create more sophisticated and adaptive attacks.

- **Adversarial ML:** Attackers manipulate data to deceive AI systems.
- **Deep fakes:** AI-generated content is used for social engineering.
- **Evasion:** AI adapts attacks to avoid detection.
- **Data Poisoning:** False data weakens AI defences.

In summary, AI and ML enhance cybersecurity but also present new risks that must be managed.

## ? How can companies ensure effective collaboration between the public and private sectors to tackle large-scale cyber threats?

To effectively tackle large-scale cyber threats through public-private collaboration, companies can adopt several strategies:

- **Information-Sharing Protocols:** Establish real-time threat intelligence sharing and standardized communication channels.
- **Public-Private Partnerships:** Create joint task forces, conduct collaborative workshops, and simulations.
- **Legal and Regulatory Framework:** Develop guidelines for information sharing, provide compliance requirements, and offer regulatory incentives.
- **Advanced Technologies and Tools:** Utilize AI and big data for unified cyber defence and develop shared cybersecurity infrastructure.
- **Workforce Training:** Implement joint training programs and cross-sector secondments to enhance skills.
- **Coordinated Incident Response:** Develop a unified response framework with continuous monitoring and feedback loops.
- **Culture of Collaboration:** Foster trust through transparency and regular stakeholder engagement.

## ? What are the key considerations for organizations when it comes to protecting sensitive data in a multi-cloud environment?

To protect sensitive data in a multi-cloud environment, organizations should focus on:

- **Data Classification and Governance:**

Classify data based on sensitivity and establish governance policies for storage and access.

- **Access Control and Identity Management:** Implement unified IAM systems, adopt least privilege access, and enforce multi-factor authentication (MFA).
- **Data Encryption:** Encrypt data in transit and at rest using strong standards and manage encryption keys securely.
- **Security and Compliance Monitoring:** Use continuous monitoring tools, ensure compliance with regulations, and conduct regular audits.
- **Data Loss Prevention (DLP):** Deploy DLP solutions and enforce policies to prevent unauthorized data transfers.
- **Interoperability and Integration:** Ensure security tools are interoperable across cloud providers and integrate with existing systems.
- **Backup and Disaster Recovery:** Perform regular backups, encrypt backup data, and have a tested disaster recovery plan.
- **Vendor Management and SLA Compliance:** Evaluate cloud providers' security measures and ensure SLAs cover data security and breach notification.
- **Risk Management and Threat Intelligence:** Conduct risk assessments and use threat intelligence to adapt security measures.
- **Employee Training and Awareness:** Provide security and incident response training to staff.

## ? How do you foresee the role of the CISO evolving as cybersecurity becomes more integral to business strategy?

The role of the Chief Information Security Officer (CISO) is shifting from a technical focus to a more strategic and business-oriented role. Key changes include:

- **Strategic Leadership:** CISOs are moving beyond technical duties to align cybersecurity with business goals, participating in board-level discussions, and demonstrating how cybersecurity supports business growth.
- **Cross-Functional Collaboration:** They need to coordinate with various departments and foster a culture of security awareness throughout the organization.
- **Business Enabler:** CISOs are balancing cybersecurity risks with business opportunities, ensuring that security

supports digital transformation and emerging technologies.

- **Adaptation to New Threat**

**Landscapes:** They will focus on proactive threat intelligence, incident response, and navigating complex regulatory environments.

- **External Engagement:** CISOs will handle communications with external stakeholders and manage reputational aspects in the event of a breach.

- **Innovation and Continuous Learning:** Staying updated on innovative solutions and continuously developing skills in emerging areas will be crucial.

Overall, CISOs are becoming key strategic leaders who integrate cybersecurity with broader business strategies.

## **? What steps can organizations take to mitigate the risks associated with supply chain cybersecurity vulnerabilities?**

Organizations can take several steps to mitigate risks associated with supply chain cybersecurity vulnerabilities. These steps include:

- **Conducting Comprehensive Risk Assessments**

- Perform regular risk assessments to identify vulnerabilities within the supply chain.

- Assess the cybersecurity posture of suppliers and partners to understand potential risks.

- Develop a risk management plan that includes strategies for mitigating identified risks.

- **Implementing Robust Cybersecurity Policies and Controls**

- Establish and enforce strong cybersecurity policies and standards for both the organization and its suppliers.

- Implement multi-factor authentication (MFA), encryption, and secure access controls to protect sensitive information.

- Use network segmentation to limit the spread of potential breaches.

- **Conducting Supplier Due Diligence and Continuous Monitoring**

- Perform thorough due diligence on all suppliers and third parties before engaging in business.

- Regularly monitor suppliers for compliance with cybersecurity policies and detect any changes in their risk posture.

- Implement continuous monitoring tools to detect and respond to threats in real-time.

- **Enhancing Incident Response and Recovery Plans**

- Develop and maintain an incident response plan that includes supply chain-related incidents.

- Regularly test and update the incident response plan to ensure readiness.

- Collaborate with suppliers to ensure they have robust incident response and recovery plans in place.

- **Increasing Awareness and Training**

- Conduct regular cybersecurity awareness training for employees, suppliers, and partners.

- Educate stakeholders about supply chain risks and best practices for mitigating them.

- Provide specific training on recognizing phishing attempts and other social engineering attacks.

- **Implementing Cybersecurity Frameworks and Standards**

- Adopt industry-recognized cybersecurity frameworks, such as NIST Cybersecurity Framework or ISO/IEC 27001, to establish a structured approach to managing supply chain risks.

- Ensure that suppliers also adhere to these frameworks and standards.

- **Improving Supply Chain Visibility and Collaboration**

- Foster greater transparency and communication with suppliers regarding cybersecurity practices and expectations.

- Use technology solutions, like blockchain and real-time monitoring tools, to increase supply chain visibility.

- Collaborate with suppliers to share threat intelligence and cybersecurity best practices.

- **Regularly Reviewing and Updating Contracts**

- Include cybersecurity requirements and clauses in contracts with suppliers and third parties.

- Require suppliers to provide proof of compliance with cybersecurity standards.

- Regularly review and update contracts to address evolving cybersecurity threats and regulations.

- **Utilizing Advanced Technologies and Solutions**

- Implement advanced cybersecurity solutions, such as AI and machine learning, to detect and respond to threats more effectively.

- Use tools like Security Information and Event Management (SIEM) and Endpoint

Detection and Response (EDR) systems for enhanced monitoring and threat detection.

- **Establishing Strong Governance and Oversight**

- Develop a governance framework that includes supply chain cybersecurity as a core component.

- Designate a dedicated team or individual responsible for overseeing supply chain cybersecurity efforts.

- Ensure senior leadership is involved in cybersecurity governance and decision-making processes.

By taking these steps, organizations can better protect their supply chains from cybersecurity threats and minimize the potential impact of a cyber incident.

## **? In your opinion, what are the most critical skills and competencies future CISOs will need to succeed in an increasingly complex threat landscape?**

Future Chief Information Security Officers (CISOs) will need a blend of diverse skills to tackle the complex cybersecurity landscape. Key competencies include:

- **Technical Expertise:** Deep knowledge of cybersecurity, emerging technologies, and risk management.

- **Strategic Thinking:** Ability to align security with business goals and manage financial implications.

- **Leadership and Communication:** Strong skills in leading teams and communicating complex issues to non-technical stakeholders.

- **Adaptability:** Agility in adapting to evolving threats and a commitment to continuous learning.

- **Legal and Regulatory Knowledge:** Understanding of global laws and privacy regulations to ensure compliance.

- **Incident Response:** Skills in managing crises, developing response plans, and ensuring business continuity.

- **Collaboration:** Ability to build partnerships internally and externally for enhanced security.

- **Analytical Skills:** Proficiency in analysing threats and making informed decisions.

- **Ethical Awareness:** Upholding high ethical standards and understanding cultural sensitivities.

These competencies will help CISOs effectively protect their organizations against dynamic threats. ➡

# NAVIGATING COMPLEX THREATS WITH DIVERSE SKILLS

## **? What emerging cybersecurity threats do you believe pose the greatest risk to organizations globally in the coming years?**

As the digital landscape evolves, organizations face increasingly complex cybersecurity threats. Key emerging risks include sophisticated ransomware that employs double extortion tactics, targeting not only for data decryption but also to prevent the public release of stolen information.

Supply chain vulnerabilities are on the rise as attackers target third-party vendors, highlighting the need for robust supply chain

security.

Cloud security gaps, resulting from rapid adoption and misconfigurations, expose sensitive data to cybercriminals.

AI-driven attacks are becoming more sophisticated, with malicious actors using AI for advanced phishing, automated vulnerability scanning, and malware.

The proliferation of IoT devices with minimal security measures presents a broad attack surface, especially for critical infrastructure.

The rise of deepfake technology poses new threats by creating convincing but fabricated media to deceive or manipulate.

Advanced Persistent Threats (APTs) involve state-sponsored attacks focusing on long-term infiltration and data exfiltration, targeting critical infrastructure and sensitive industries.

Insider threats are growing more sophisticated, causing significant harm where monitoring and controls are inadequate. To counter these emerging threats, organizations should adopt a Zero Trust framework, enhance threat intelligence, and invest in AI-driven defense mechanisms.

## **? How should organizations prepare for the growing challenges of securing the Internet of Things (IoT) and other connected devices?**

Securing the Internet of Things (IoT) and other connected devices is increasingly critical as their use grows across various sectors.

Organizations should adopt a multi-faceted approach to address these challenges effectively. Embracing a Zero Trust model ensures that no device is implicitly trusted, requiring continuous verification of all devices. Strengthening device authentication and access controls with multi-factor authentication (MFA) and strict access policies helps limit interactions to authorized personnel. Implementing network or micro-segmentation



**KANESAN PANDI**  
Head of Information  
Security,  
Galadari Group



isolates IoT devices to minimize breach impact and protect critical assets. Regularly updating firmware and software addresses vulnerabilities, while strong data encryption protects information in transit and at rest. Conducting comprehensive risk assessments identifies and mitigates vulnerabilities, and advanced threat detection tools using machine learning and behavioral analytics enhance real-time threat identification. A robust device lifecycle management process ensures secure onboarding, monitoring, and decommissioning of devices. Collaborating with IoT vendors to ensure integrated security and promoting security awareness and training among employees further strengthens the organization's security posture.

### **? What measures do you have in place to protect sensitive data stored in the cloud?**

We use a combination of best practices to evaluate a CSP before onboarding them in line with the highlighted risks above. Over and above, we use a combination of tools to monitor and protect our cloud solutions such as MFA, CASB, DLP, IAM, Attack Surface, and Data Encryption while as practices to name a few, we make sure that we perform

Regular Access and Configuration Reviews, Third-Party Risk Audits and Vulnerability Assessments. These measures provide us with significant assurance and satisfaction in reducing risks.

### **? What role do you see artificial intelligence and machine learning playing in both enhancing and compromising cybersecurity efforts?**

AI and machine learning (ML) play a crucial role in both enhancing and compromising cybersecurity. On the positive side, AI and ML advance threat detection by swiftly analyzing patterns and anomalies, automate incident response for quicker reactions, and use behavioral analytics to identify unusual activities and potential insider threats. They also enable predictive analysis to forecast threats and enhance threat intelligence by aggregating and analyzing emerging threat data.

However, these technologies also pose risks; AI can be used to create sophisticated malware that adapts to evade detection, generate convincing phishing attempts, and produce deepfakes for misinformation. AI's evasion techniques can bypass traditional security measures, and resource-draining

attacks can target AI systems.

To balance these advantages and risks, it's essential to combine AI with human oversight, regularly update models to stay current with evolving threats, secure AI systems against compromise, and ensure ethical use to prevent contributing to cyber threats.

### **? How can companies ensure effective collaboration between the public and private sectors to tackle large-scale cyber threats?**

In the UAE, where cybersecurity is a national imperative, fostering strong collaboration between the public and private sectors is essential for addressing large-scale cyber threats. Companies can achieve this by engaging in national cybersecurity initiatives, actively participating in government-led threat intelligence sharing, and aligning their security practices with national frameworks. Building robust communication channels with regulatory authorities, co-investing in joint cybersecurity training, and contributing to the creation of industry standards will further enhance cooperation. Such collaboration ensures a unified and more resilient approach to combating evolving





cyber threats across the nation.

**? What are the key considerations for organizations when it comes to protecting sensitive data in a multi-cloud environment?**

Protecting sensitive data in a multi-cloud environment requires a strategic approach that includes data classification and encryption, consistent security policies, and robust visibility and monitoring across all platforms. Organizations must ensure strict access management by utilizing identity and access management (IAM) solutions and regularly assess the security practices of each cloud provider. Compliance with data residency policy is crucial, as is ensuring interoperability of security tools across different cloud environments. Additionally, a well-defined incident response and recovery plan is essential to effectively address potential breaches and maintain data integrity.

**? How do you foresee the role of the CISO evolving as cybersecurity becomes more integral to business strategy?**

As cybersecurity increasingly becomes a core component of business strategy, the role of the CISO is undergoing significant transformation. The CISO is shifting from a primarily technical position to a strategic

leadership role, where they collaborate closely with the C-suite and board to integrate cybersecurity with business objectives and risk management. This evolution includes balancing security needs with business innovation and agility, fostering cross-departmental collaboration with IT, legal, finance, and HR, and focusing on building a resilient security posture. The CISO's responsibilities are expanding to ensure comprehensive data privacy, oversee the adoption of emerging technologies like AI and Zero Trust, and manage enterprise-wide risk. Ultimately, the CISO is evolving from a technical expert into a pivotal business leader, crucial for shaping and driving the organization's overall strategy and success.

**? What steps can organizations take to mitigate the risks associated with supply chain cybersecurity vulnerabilities?**

To mitigate risks associated with supply chain cybersecurity vulnerabilities, organizations should adopt a multi-faceted approach. This includes conducting thorough assessments of vendor security practices, implementing robust contractual agreements with strict cybersecurity requirements, and enforcing access controls (PAM) and Zero Trust to limit and monitor supplier access. Continuous monitoring and real-time threat detection are crucial for identifying suspicious activities, while well-developed incident response plans

ensure readiness for supply chain-related security incidents. Enhancing collaboration with suppliers and industry partners to share threat intelligence, educating employees about supply chain risks, and regularly updating security policies are also essential steps in strengthening overall supply chain security.

**? In your opinion, what are the most critical skills and competencies future CISOs will need to succeed in an increasingly complex threat landscape?**

To navigate the increasingly complex threat landscape, future CISOs will need a diverse set of skills and competencies. Key skills include strategic thinking and leadership to align cybersecurity initiatives with business goals and manage risks effectively. Technical expertise in emerging technologies like AI and Zero Trust is essential for enhancing security measures and staying ahead of threats. Strong risk management abilities are crucial for identifying and mitigating cyber risks across the organization. Competency in fostering cross-functional collaboration ensures effective integration of cybersecurity practices with other departments. Additionally, a focus on continuous learning is important to keep pace with evolving threats and regulatory requirements. These skills collectively equip future CISOs to drive comprehensive and resilient cybersecurity strategies in a dynamic environment. ➡



GLOBAL CIO EXPERTISE,  
DRIVING INNOVATION  
FOR PEOPLE AND PLANET

CONSULTING | RESEARCH | ON DEMAND

[www.iamcaas.com](http://www.iamcaas.com)



- RESEARCH
- INSIGHT & BENCHMARKING
- EMERGING TECHNOLOGIES
- GOVERNANCE
- RISK & COMPLIANCE
- CYBER SECURITY
- DIGITAL TRANSFORMATION
- DEOPS & DIGITAL INFRASTRUCTURE
- ERP & CRM





**GEC  
AWARDS**  
2024

**HONORING  
THE  
BEST**

