October 2025

ICIT

CISO Dilemma:

Should The Enterprise Offer Personal Data Protection to the Employee as a Benefit?

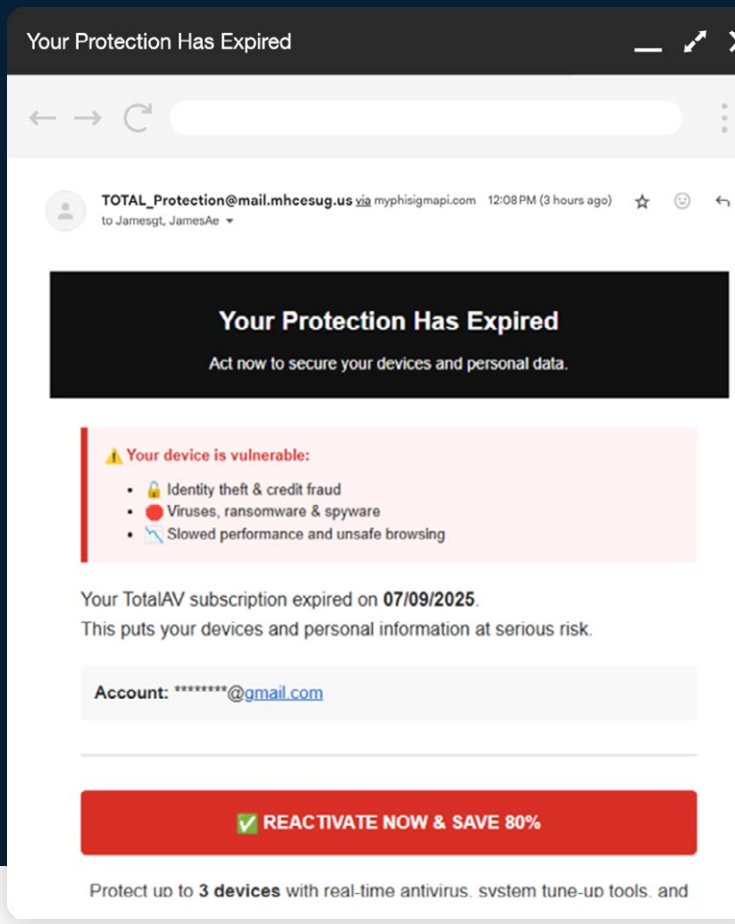
Jim Routh
Fellow, Institute for Critical Infrastructure Technology

www.icitech.org

CISO Dilemma:

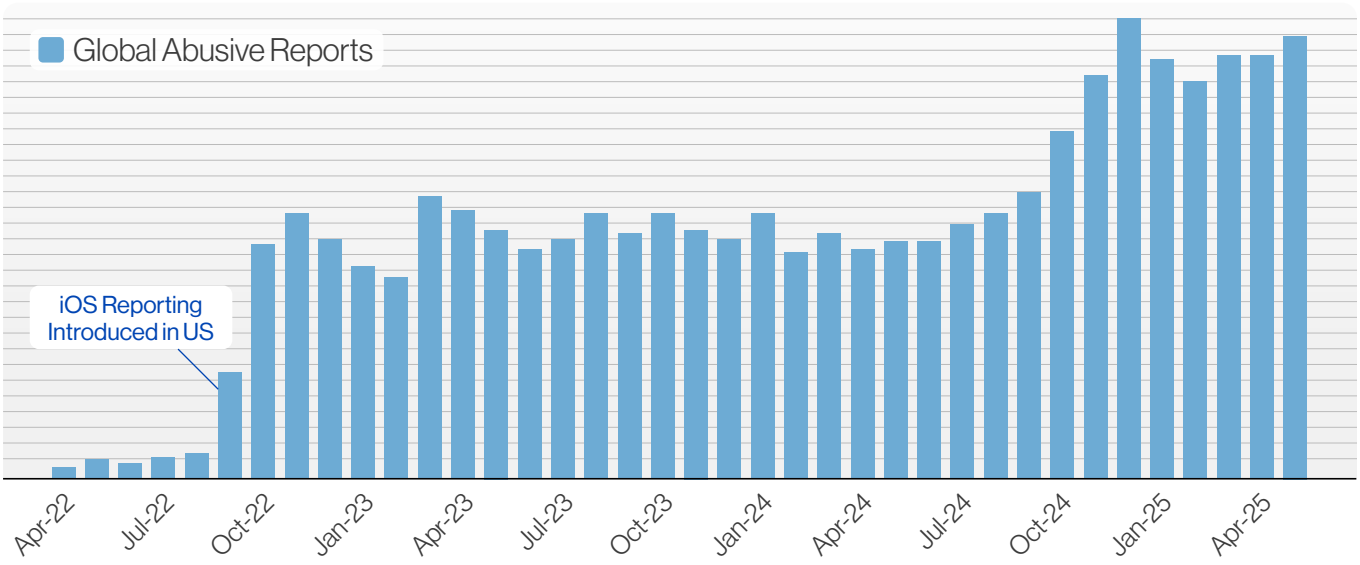
Should The Enterprise Offer Personal Data Protection to the Employee as a Benefit?

Have you recently noticed an increase in the fraudulent SMS messages you receive on your phone? I have, and I've observed that not only are the messages arriving in greater volume, but they are also better constructed with polished English and more compelling content. This led me to search for empirical data to support my hypothesis: that criminals are using Large Language Models (LLMs) to improve the quantity and quality of fraudulent SMS messages.



According to Dan Michan, who provides a newsletter on cyber trends (https://www.cybersecurity hq.com), 73% of sophisticated cyber attacks now use AI, up from 31% in Q4 2022. Furthermore, 89% of successful breaches involve social engineering enhanced by AI. Cloudmark, now part of Proofpoint, has been tracking the number of reported SMS abuse cases for the past five years in the US, and the data shows a significant increase from 2024 to 2025.

Aggregate Global Abusive Reports, since April 2022



The current situation, described by Dan Michan, is that AI has become both our most powerful defensive tool and our most dangerous vulnerability. While 78% of organizations have implemented AI for business functions, only 27% have implemented any form of AI security governance. This gap is affecting both enterprise users and digital consumers. Notably, GPT-4-powered phishing achieves a 43% click rate success, compared to just 11% without AI. One of the reasons for improved click rate success between SMS and email is people look at their phones more often today (205 times a day on average).

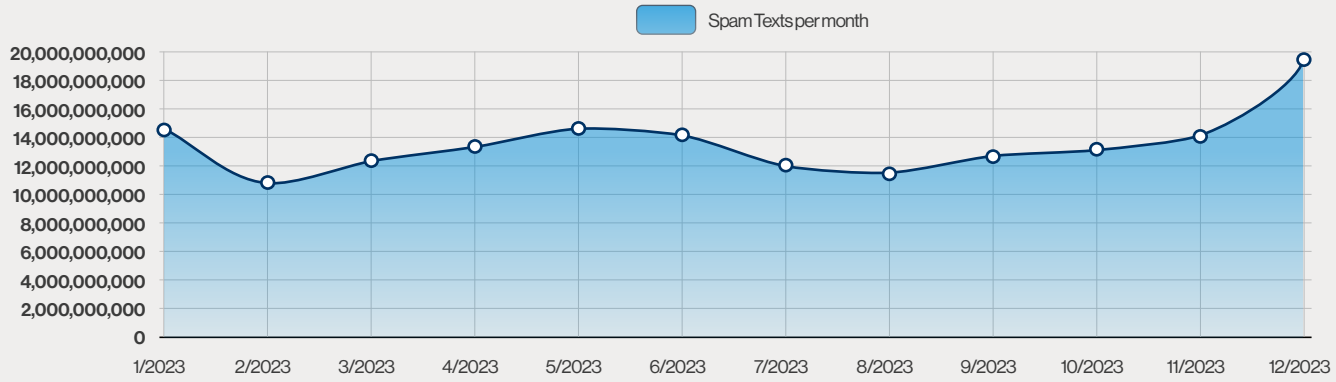
Email security has improved in recent years due to email security standards (DMARC) and products that filter SPAM and fraudulent email. Messaging platforms don't have comparable messaging security to filter out malicious messages. Messaging is more economical for criminals than email given the low cost to send messages in volume ($.01-$.05 per message). Digital consumers are more likely to open text messages before any other form of mobile communication. 90% of all text messages are read within 3 minutes of being received (2019 Mobile Usage Report). The average response time for email is about 90 minutes, compared to 90 seconds for a text message.

There are several data points indicating that deepfakes created by AI are being used to bypass both voice authentication in call centers and video authentication in video conferencing. This vulnerability is particularly concerning, as it can be exploited for financial gain. Specifically, the voice authentication breach is often linked to the transfer of electronic funds in an attempt to commit fraud. Meanwhile, the use of both video images and voice synthesis by offshore or remote workers is a common tactic to secure multiple job assignments, to farm out the work to others, and take a cut of the fees paid. Employers are finding it challenging to identify and remediate this type of fraud, which can take several months to detect. The threat actors' success rate is alarming, with a 67% success rate on voice-based social engineering. Employers are finding it challenging to identify and remediate this type of fraud, which can take several months to detect. The threat actors' success rate is alarming, with a 67% success rate on voice-based social engineering.

As more data becomes available on the use of AI in these types of fraud, the pressure on enterprises to adjust their controls and mitigate the risk of fraud impacting customers will grow. So, where should an enterprise start?

Most enterprises have already implemented protections against phishing emails targeting individual employees' work emails. They use a combination of tools to reduce the likelihood of fraudulent emails reaching enterprise users. However, as the number of remote and hybrid workers continues to grow, and with the widespread adoption of the Bring Your Device (BYOD) approach, conventional controls are often limited to work email and not extended to SMS or personal email.

How many robotexts are Americans getting?



19.2 billion spam texts in January 2025. That's nearly ***63 spam texts*** for every person in the U.S.!

The reality is that cybercriminals don't discriminate between personal and work-related communications. As long as their phishing tactics are effective, they don't care whether the target is a work email or a personal SMS message. This blind spot in conventional security controls leaves enterprise users vulnerable to attacks that can have significant consequences for both personal and business assets. According to Robokiller's Spam Text Insights, 19.2 billion spam texts were sent in January of this year, which is 63 spam texts for every person in the US.

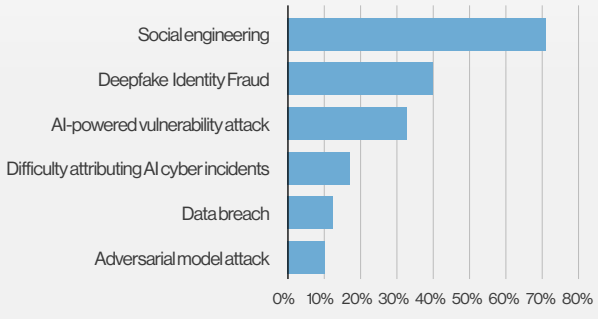
Google's threat intelligence group (Mandiant) published details about a campaign tied to a Vietnam-linked group (UNC6032) that used thousands of deceptive ads on Facebook and LinkedIn, convincing viewers into visiting lookalike sites for legitimate AI tools (Luma AI, Canva Dream Lab, and King AI). This campaign included about 2.3 million users in the EU. Once the user entered the fake site and entered text or image prompts, users received various types of malware designed to install backdoors, as well as an infostealer that could record keystrokes and steal sensitive data like passwords for digital wallets and password managers. Enterprise users who use their devices for personal use of common social networks are now exposed to sophisticated malware that steals credentials for both personal and corporate use. Is this type of attack in scope for an enterprise CISO or not?

Trend Micro predicts that scammers will double down on social engineering using AI-generated videos distributed via popular social networks. AI is being used today to generate views and clicks for payment. Threat actors will continue to innovate how to incorporate and use AI to maximize the return on investment of their campaigns. The financial sector held a recent workshop on AI threats, and survey results identify social engineering as the top cyber challenge due to AI, with identity fraud as the second.

In this context, the threat landscape has shifted, and enterprises need to reassess their security controls to account for the increased attack surface of personal devices and communications. By taking a more holistic approach to security, enterprises can better protect their users and mitigate the risks associated with phishing attacks, regardless of whether the attack vector is a work email, a personal email, or an SMS message.

Financial sector's most acute AI-related cybersecurity challenges

(participant questionnaire, May 28, 2025)



FINANCIAL INDUSTRY FORUM ON ARTIFICIAL INTELLIGENCE II:
A COLLABORATIVE APPROACH TO AI THREATS, OPPORTUNITIES, AND BEST PRACTICES
WORKSHOP 1- SECURITY AND CYBERSECURITY
JULY 2025

Historically, enterprise cybersecurity professionals have been hesitant to venture into the realm of controlling personal usage versus corporate use cases. As a cybersecurity professional in the past, I recall traveling to senior executives' homes to configure their routers for home office requirements, while deliberately avoiding any discussion of personal use of their home networks despite observing vulnerabilities. This reluctance has been a long-standing trend among Chief Information Security Officers (CISOs) over the years, even as the dependence on personal devices and networks to support remote and hybrid workers has increased.

However, the times are changing. With the growing threat landscape and the increased risk of data breaches, it may be time for CISOs to reconsider their stance on this issue. 93% of C-Suite executives have a current or former home address listed on a data broker site, according to VanishID. 94% of the C-Suite have exposed clear text credentials with an average of 4.3 exposed credentials per executive. Typical employees average 2.7 exposed credentials. One possible approach is to offer both corporate and personal protection on personal devices as an employee benefit. This could be a game-changer in the world of cybersecurity, as it would provide employees with a comprehensive security solution that protects both their personal and professional data. Today, more people in the world own a cell phone vs. a toothbrush, according to Kevin Thomsen, Head of Cybercrime/Fusion Operations at TD Bank Group.

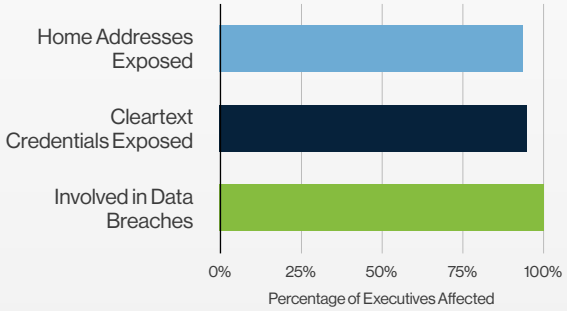
The catalyst for this shift may be the emergence of new cybersecurity products that offer protection for both corporate and personal data for employees. Several early-stage companies are developing this type of data protection, recognizing the need to protect personal data to reduce exposure to corporate data.

The question is, are CISOs ready to seize this opportunity and protect not only their enterprise data but also the personal data of their employees? Unfortunately, it's unlikely that many will be eager to take on this challenge, at least initially. However, there will likely be a few early adopters who will venture forward with effective controls for both use cases.

The opportunity here is for the enterprise to support the use of these controls while also recognizing that part of the deployment is an employee benefit for their personal computing use cases. Several enterprises have offered password managers for storing personal and corporate passwords to employees, defraying some of the cost to encourage employees to take advantage of this as a benefit.

C-Suite Digital Exposure

Based on analysis of 10,000+ executives across 65 industries



Key Insights

- **93%** of executives have their home addresses exposed on data broker sites
- **94%** of executives have exposed cleartext credentials
- **100%** of executives have been involved in at least one data breach
- On average, each executive appears in **43 data breaches**
- Executives average **11+ data broker profiles** containing their personal information

By taking this approach, CISOs can demonstrate their commitment to protecting their employees' personal data and well-being, while also enhancing the overall security posture of the organization. This approach is already showing up in the market as several products are now helping shrink the amount of digital breadcrumbs spread by senior executives to reduce their personal and professional attack surface, ultimately reducing the risk of being a target.

In the past, employees have often been resistant to the idea of additional security controls on personal devices, viewing it as intrusive and overly restrictive. However, the threat landscape has changed significantly, and employees are now facing a deluge of sophisticated attacks, often powered by AI. This has created a new dynamic, where employees may be more willing to accept additional controls on their personal devices if they see them as a means of protection rather than a restriction.

In this context, the enterprise may have a unique opportunity to step in and offer protection to its employees. Not only can this enhance the overall security posture of the organization, but it can also help mitigate the risk of data breaches and cyberattacks that could have far-reaching consequences.

There are several reasons why an enterprise may wish to avoid the liability of protecting an employee's personal data. For one, it can be a complex and costly endeavor, requiring significant resources and expertise. Additionally, there may be concerns about overstepping into employees' personal lives or compromising their privacy. However, there are also compelling reasons to offer such protection as a benefit. By doing so, the enterprise can demonstrate its commitment to the well-being and security of its employees, which can have a positive impact on morale and productivity. Moreover, offering protection to employees can be seen as a way to attract and retain top talent, particularly in industries where cybersecurity is a major concern.

Ultimately, the decision to offer protection to employees is a strategic one that requires careful consideration of the potential benefits and risks. For many organizations, the benefits of offering protection as a benefit may outweigh the costs and challenges, particularly in a world where cyber threats are becoming increasingly sophisticated and pervasive.

The adoption of generative AI for both consumers and enterprises marks a significant turning point in the evolution of computing capabilities. This technological advancement is more transformative than any previous innovation, including the rise of mobile devices and cloud computing. Today, a growing majority of software used by enterprises leverages Large Language Models (LLMs) as a fundamental component of functionality. The widespread adoption of LLMs has already begun to reshape the software development landscape, enabling developers to create more sophisticated and efficient code.

The availability of millions of open-sourced LLMs and agents has further accelerated this change. With these powerful tools at their disposal, developers can now rely on LLMs to produce code, revise code, and even improve code quality and time-to-market. This has the potential to revolutionize the software development process, making it faster, more efficient, and more effective.

The impact of LLMs on software development is already being felt, with many organizations leveraging these technologies to automate tasks, enhance productivity, and improve the quality of their software. As the use of LLMs continues to grow, we can expect to see even more significant changes in the way software is developed, deployed, and maintained.

The shift towards generative AI is not just a technical advancement; it also represents a fundamental change in how we approach software development. It requires a new mindset, new skills, and a new set of tools. Organizations that fail to adapt to this new reality risk being left behind, while those that embrace the opportunities offered by LLMs and generative AI will be well-positioned to thrive in a rapidly changing world.

As a cybersecurity professional supporting an enterprise today, it's essential to consider how AI can enhance your protection capabilities. This requires exploring various approaches that leverage AI to stay ahead of emerging threats. However, this journey also demands careful navigation of the boundaries between corporate and personal data protection.

To achieve this, it's crucial to engage in open and exploratory dialogue with your colleagues in the Legal department. This collaboration will help you understand the nuances of data protection laws and regulations, ensuring that your AI-driven security strategies remain compliant. By doing so, you'll be able to strike a balance between protecting enterprise assets and respecting the personal data of your employees.

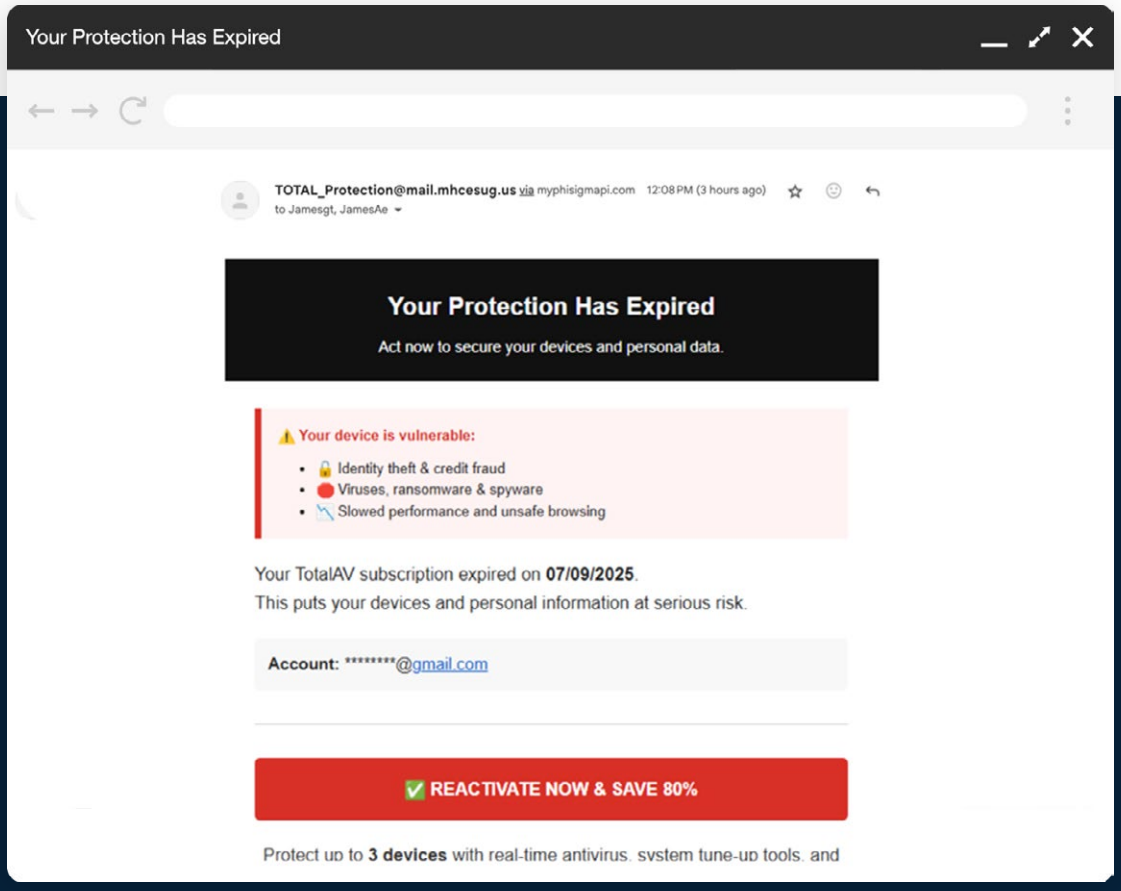
It's also essential to recognize that AI governance cannot be reduced to simply relying on conventional and established cybersecurity controls. Threat actors have adapted their tactics to exploit AI-powered vulnerabilities, and cybersecurity professionals must make similar adjustments to stay ahead. This means embracing AI-driven solutions that can help you detect, respond to, and prevent sophisticated attacks.

CISOs should be cautious not to mislead stakeholders by suggesting that AI governance is merely a matter of applying traditional cybersecurity controls. Instead, they should acknowledge that AI requires a new set of controls, frameworks, and strategies that can effectively mitigate the risks associated with AI-powered threats. The financial sector has identified the most acute AI-related cybersecurity challenges, and social engineering tops the list, followed by identity fraud.

According to Professor Tom Malone from MIT, AI alone is better at many decision-making tasks, but human+AI augmentation improves human judgment. There are tasks that AI is more effective at than humans, and tasks that humans outperform LLMs. The combination of humans with AI will improve outcomes in specific tasks involving judgment. AI governance at enterprise scale needs to both encourage the exploration of AI use cases while also providing the necessary control capabilities for the combination of AI and human judgment necessary to meet stakeholder needs. Human judgment, augmented with AI, may offer a reasonable approach to protecting both personal and corporate data in the future.

By embracing AI and collaborating with stakeholders across the organization, cybersecurity professionals can develop innovative solutions that benefit from AI usage while ensuring the protection of both corporate and personal data. This approach will enable enterprises to stay ahead of emerging threats and maintain a robust security posture in an increasingly complex and dynamic threat landscape.

Is it time for the cybersecurity leader to offer protection capabilities for employees that cover both misuse of corporate and personal data in alignment with threat actor tactics? Are you ready for this evolution? Are there legal liability implications to providing personal data protection for employees as a benefit? Absolutely! What is clear is that as threats mature in applying AI for attacks on enterprise and personal data, there will be more choices of products and capabilities to manage the risk of both. Some enterprises will move away from SMS as a second factor, some will further lock down SMS usage and some will offer alternative messaging platform (iMessage, RCS, Signal, WhatsApp, etc.) options with selected controls. It's time for the CISO to prepare for the eventual outcome of data protection capabilities for professional and personal data usage in both policy and with a set of capabilities for employees.



About

ICIT

The Institute for Critical Infrastructure Technology (ICIT) is a nonprofit, nonpartisan, 501(c)3 think tank with the mission of modernizing, securing, and making resilient critical infrastructure that provides for people's foundational needs. ICIT takes no institutional positions on policy matters. Rather than advocate, ICIT is dedicated to being a resource for the organizations and communities that share our mission. The views and opinions expressed in this essay are solely those of the author(s) and do not necessarily reflect the official policy or position of ICIT. Any assumptions made within the analysis are not reflective of the position of any entity other than the author(s). To learn more, please visit www.icitech.org

Jim Routh

Jim Routh serves on the Boards of Savvy Security, Accountable Digital Identity Association, and the Global Resiliency Federation. He is the former Board Chair for the Health Information Sharing & Analysis Center (H-ISAC) and former Board member for the Financial Services Information Sharing & Analysis Center (FS-ISAC). Jim is the Chief Trust Officer for Saviynt. Jim is a former CSO/CISO for American Express, DTCC, KPMG, Aetna, CVS, and MassMutual. Jim brings a vast business and technology background to the boards and senior executives and is considered a digital and cyber security industry expert and thought leader. Jim is an advisor for Wiz, Netskope, Armis, Transmit Security, Security Scorecard, Gurucul, Data Theorem, Panaseer, Legit Security, CodeZero, Picnic, and Rekin. He serves in an advisory capacity and is an investor for cyber-specific venture funds including Syn Ventures, CyberStarts, Security Leadership Capital, Ballistic Ventures, and Rain Capital. Jim is an ICIT Fellow and an adjunct faculty member, and he teaches cybersecurity at the NYU Tandon School of Engineering. Jim also mentors over 90 cybersecurity professionals and students.

CyberRisk Alliance

CyberRisk Alliance provides business intelligence that helps the cybersecurity ecosystem connect, share knowledge, accelerate careers, and make smarter and faster decisions. Through our trusted information brands, network of experts, and innovative events we provide cybersecurity professionals with actionable insights and act as a powerful extension of cybersecurity marketing teams. Our brands include SC Media, the OfficialCybersecurity Summits, TECHEXPO Top Secret, Security Weekly, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, Cybersecurity Collaborative, ChannelE2E, MSSP Alert, LaunchTech Communications, CyberRisk TV and Execweb. To learn more, please visit www.cyberriskalliance.com

Thank you to our Strategic Partner **CyberRisk Alliance**

ICIT

www.icitech.org