ITPV

Connecting with Solution Provider in
EMERGING MARKET

Vol IX | Issue 1 | May 2024 | Pages 36

▪ Northern ▪ Eastern ▪ Maharashtra ▪ Gujarat ▪ MP & Chattisgarh ▪ North East ▪ Southern ▪ UP & Uttarakhand ▪ Bihar & Jharkhand

Cybersecurity Chronicles: CISO Priorities Unveiled

Bhavesh Kumar
SK Finance

Dr. Fene Osakwe
Springboard

Justin Ong
Panasonic

Jenny Tan
ISACA Singapore Chapter

Abhijit Chakravarty
HDFC Bank

TECHPLUS MEDIA™

VERTIV

Looking for a compact, efficient and robust UPS? Look no further!

Presenting

Liebert ITA2 30kVA

A fully digital, highly reliable, double-conversion UPS solution.

Its cutting-edge design enables seamless integration into your current system, or various other ecosystems. And it's tailored for global deployment in a low carbon, compact footprint. The ITA2 is the ultimate level of engineering and dynamics from Vertiv. So, you can deploy this innovative, next-gen and extract great performance at low costs. Adding up to peace of mind. If you're looking to power your infrastructure, or upgrade your already protected systems, the ITA2 is a great addition to your support backup.

Talk to us today!

Explore solutions at Vertiv.com/en-in
Call Tollfree : 1-800-2096070
E-mail : marketing.india@vertiv.com

Corporate Office : Plot C-20, Rd No.19, Wagle Ind Estate, Thane (W), 400604. India

SCAN CODE
TO KNOW MORE

SEAGATE

TESTED.

160+ Quality Tests
Ensures long-term durability

Rescue DATA RECOVERY SERVICES
3 YEARS INCLUDED*
*Not valid on 1TB drives

OPTIMIZED.

ImagePerfect™ Firmware
Zero dropped frames
Non-stop vigilance

SkyHawk Health Management
Real-time prevention, intervention & recovery

Up to 550TB Workload Rate**
Always on long-term recording

Up to 2.5 Million Hours
Mean Time Between Failure

SUPPORTS UP TO 64 HD CAMERAS

Up to 5 Years Warranty

PROVEN.

40+ YEARS OF EXPERIENCE

VARINDIA Star Nite AWARDS 2023
BEST HARD DRIVE AWARD 2023

NCN MOST Innovative PRODUCT OF THE YEAR 2022
MOST INNOVATIVE PRODUCT OF THE YEAR 2022

15 dt AWARDS 2023
BEST HARD DRIVE BRAND 2023

**Skyhawk video drives are designed for always-on workloads of 180TB/year, 550TB/year for Skyhawk AI.

www.seagate.com

SCAN TO LEARN MORE

For enquiries, contact: Rahul Seth, Regional Head | **Mobile -** 9819020604 | **Email:** Rahul.Seth@seagate.com
For marketing support, contact: Talwinder Singh | **Mobile -** 9650164235 | **Email:** talwinder.singh@seagate.com

CONTENT

COVER STORY

IN CONVERSATION

BHAVESH KUMAR,
CISO and DPO, SK Finance

DR. FENE OSAKWE, Council Member, Forbes Technology & Cyber Security Mentor, Springboard

JUSTIN ONG, CISO & DPO, Panasonic

JENNY TAN, President, ISACA Singapore Chapter

ABHIJIT CHAKRAVARTY, Senior VP of Core Network & Security Operations, HDFC Bank

Canon

Delighting You Always

COMPACT AND POWERFUL DOCUMENT SCANNERS

FOR EVERY DIGITIZATION NEED

DR-C225II

DR-C240

P208-II

DR-F120

CHECK OUT OUR HIGH SPEED DOCUMENT SCANNER RANGE:

Personal Scanners

P-208II

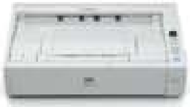
Workgroup Scanner

DR-C240

Network Scanner

Scan Front 400

Departmental Scanners



DR-M1060

Production Scanners

DR-G2140

Business Can Be Simple

FOR SALES ENQUIRIES : West Bengal - Suvrendu Mitra : 98316 62162, Inderjit Yadav : 99030 25352, Saptarshi Bhandari - 98308 56977; Bihar - Virvijay Singh : 95235 96990; Jharkhand - Lokesh Nath : 70860 14183; Odisha - Bharat Kumar Singh : 91675 32045

Cybersecurity Chronicles: CISO Priorities Unveiled

As guardians of digital assets and stewards of organizational resilience, CISOs must navigate a complex web of priorities, ranging from enhancing risk posture to embracing emerging technologies. Based on the CISO Priorities Survey 2024, this cover story provides invaluable insights into this shifting paradigm, with over 560 security decision-makers sharing their perspectives. The story delves into the top priorities, challenges, and strategies shaping the cybersecurity landscape, offering valuable insights into the evolving role of CISOs in navigating these turbulent waters

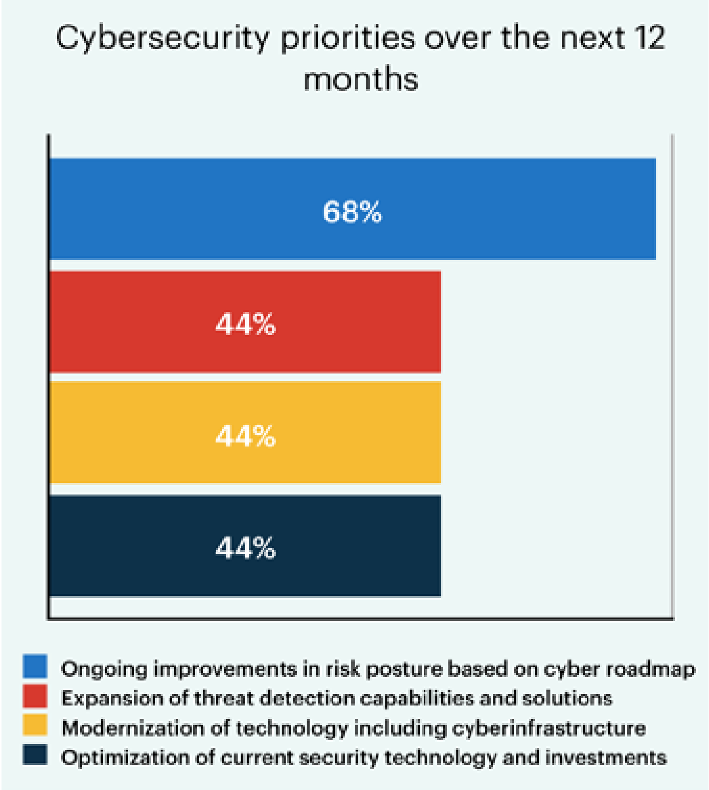
Emerging from over three years of the COVID-19 pandemic, the landscape in which Chief Information Security Officers (CISOs) operate has irrevocably changed. Cybersecurity has transcended its traditional IT roots to become a distinct functional area of the business, essential for delivering broader business outcomes. Organizations increasingly recognize the pivotal role cybersecurity plays in enabling success across all facets of the business, from safeguarding sensitive data to fostering customer trust and driving innovation. As a result, the future role of the CISO has never been more vital.

The CISO Priorities Survey 2024 offers a comprehensive insight into the evolving cybersecurity landscape, providing a nuanced understanding of the shifting priorities, challenges, and investment strategies of CISOs. With responses from over 560 security decision-makers across various industries, the survey delves into key areas such as budget allocations, outsourcing trends, board engagements, talent management, and the adoption of emerging technologies.

In this cover story, we embark on a detailed analysis of the CISO survey findings, shedding light on the strategic imperatives shaping the cybersecurity landscape. From navigating budgetary constraints to harnessing the power of Artificial Intelligence (AI) for cyber defense, CISOs are at the forefront of driving organizational resilience in the face of evolving cyber threats. Through proactive strategies and a holistic approach to cybersecurity, organizations can align their security initiatives with broader business objectives, ensuring sustainable success in an increasingly digital world.

At the heart of CISO priorities lies the ongoing quest to enhance risk posture based on a robust cyber roadmap. Over two-third (68%) of surveyed CISOs prioritize ongoing enhancements to their risk posture based on a cyber roadmap, signaling a strategic commitment to adaptability and resilience in the face of evolving threats. Additionally,

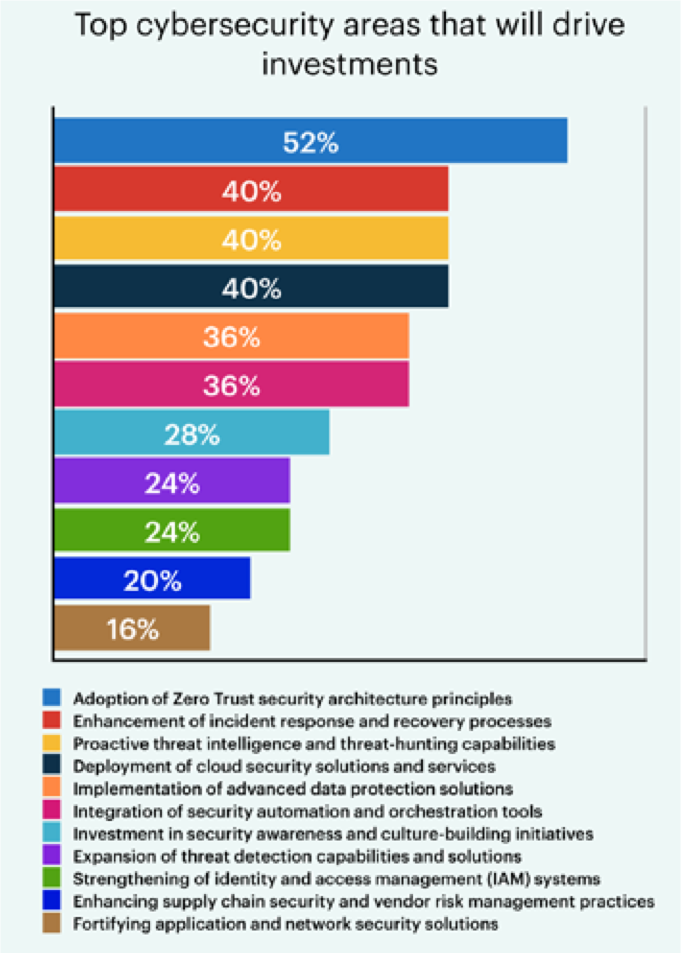
Enhancements to Risk Posture based on Cyber Roadmap is the Top CISO Priority



Top cybersecurity priorities over the next 12 months

1. Ongoing improvements in risk posture based on cyber roadmap
2. Modernization of technology including cyberinfrastructure
3. Optimization of current security technology and investments
4. Expansion of threat detection capabilities and solutions

Zero Trust Principles Dominate CISOs' Cybersecurity Investments



Top cybersecurity areas to drive investments

1. Adoption of zero-trust security principles
2. Enhancement of incident response and recovery processes
3. Proactive threat intelligence and threat-hunting capabilities
4. Deployment of cloud security solutions and services
5. Implementation of advanced data protection solutions
6. Integration of security automation and orchestration tools

50% emphasize the modernization of technology, including cyber infrastructure, recognizing the importance of staying ahead with updated tools and systems. Furthermore, 45% focus on optimizing current security investments, while 44% emphasize expanding threat detection capabilities and solutions.

The findings reveal a multi-faceted approach to addressing cybersecurity challenges, with a clear emphasis on enhancing risk posture through ongoing improvements based on a cyber roadmap. This priority underscores a strategic focus on continuous evaluation and refinement of security strategies to adapt to evolving threats effectively. Simultaneously, the prioritization of modernizing technology, optimizing current security investments, and expanding threat detection capabilities reflects a comprehensive strategy aimed at bolstering the organization's overall cybersecurity resilience. Such priorities signify a recognition of the dynamic nature of cyber threats and the need for agile, proactive measures to safeguard digital assets and maintain operational continuity in an increasingly complex threat landscape.

52% of surveyed CISOs prioritize the 'Adoption of Zero Trust security principles' as their foremost cybersecurity investment focus. Additionally, 40% of CISOs each prioritize 'Enhancing incident response and recovery processes,' 'Proactive threat intelligence and threat-hunting capabilities,' and 'Deploying cloud security solutions and services.' Moreover, 36% of CISOs each prioritize 'Implementing advanced data protection solutions' and 'Integrating security automation and orchestration tools' as their primary investment areas.

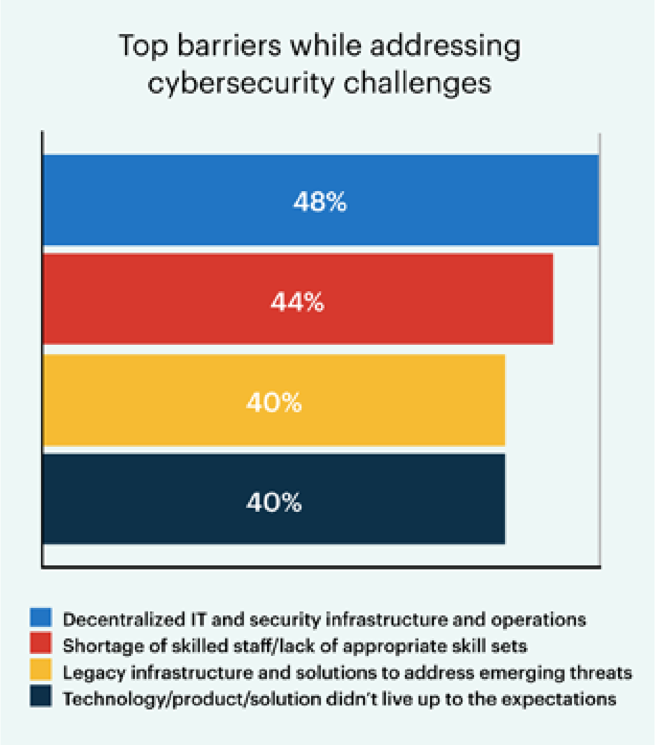
The survey findings highlight a nuanced approach to cybersecurity investment, reflecting a diverse set of priorities aimed at fortifying organizational defenses. The emphasis on adopting zero-trust

security principles by a majority of CISOs underscores a paradigm shift towards a more proactive and granular security model. Additionally, the widespread focus on enhancing incident response, threat intelligence capabilities, and cloud security solutions reflects a recognition of the evolving threat landscape and the need for robust defenses across multiple fronts. Moreover, the prioritization of advanced data protection and security automation tools signifies a concerted effort to safeguard sensitive data and streamline security operations in an increasingly complex digital environment.

Nearly half (48%) of surveyed CISOs identified decentralized IT and security infrastructure and operations as their primary barrier to addressing cybersecurity challenges in the past 12 months. Following closely, 44% cited a shortage of skilled staff or lack of appropriate skill sets as the second-largest challenge. Additionally, 40% of respondents each cited challenges related to legacy infrastructure and solutions, as well as instances where technology, products, or solutions fell short of expectations.

The findings shed light on the primary challenges faced in addressing cybersecurity concerns over the past year. The prevalent issue of decentralized IT and security infrastructure underscores the complexity of modern organizational landscapes, where disparate systems and operations pose significant hurdles to cohesive security management. Additionally, the shortage of skilled staff reflects a persistent industry-wide struggle to recruit and retain talent capable of navigating evolving cyber threats effectively. The significant concerns surrounding legacy infrastructure and unmet technology expectations highlight the need for agile, adaptive solutions that can adequately address emerging cybersecurity challenges while aligning with organizational needs and expectations.

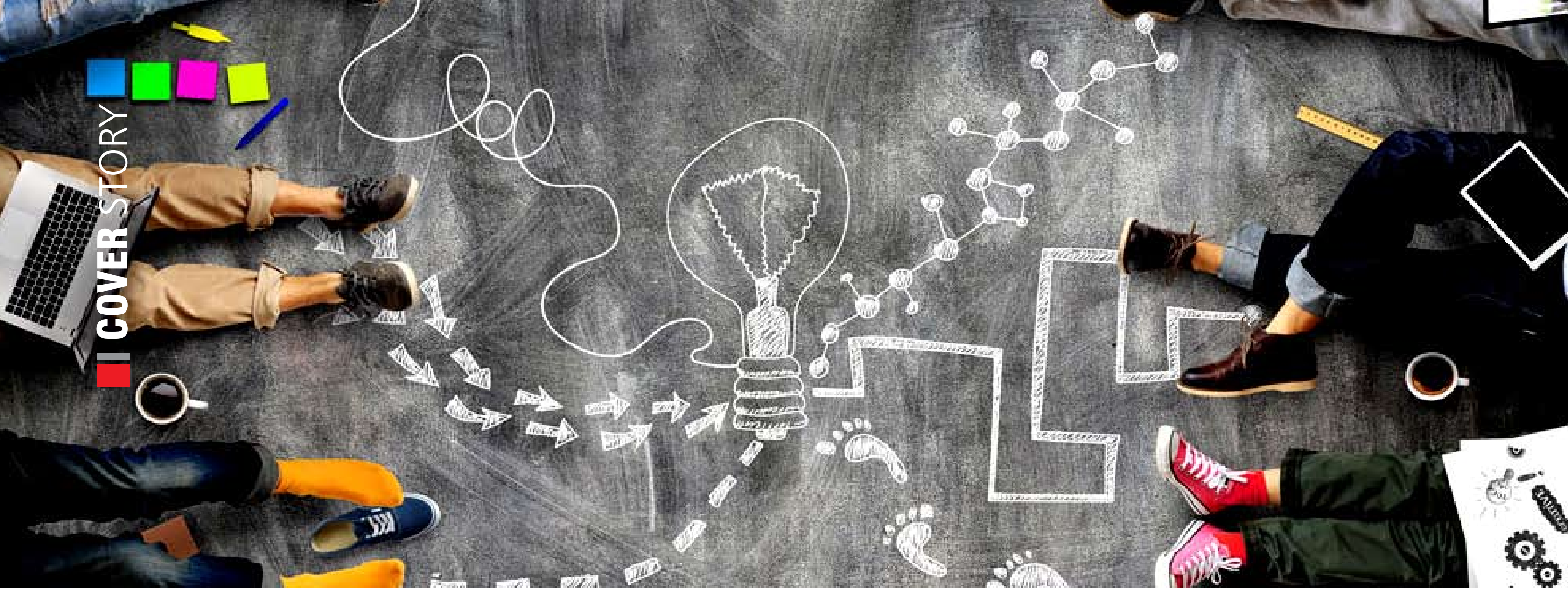
Decentralized Infrastructure and Talent Shortages are Key CISOs' Concerns



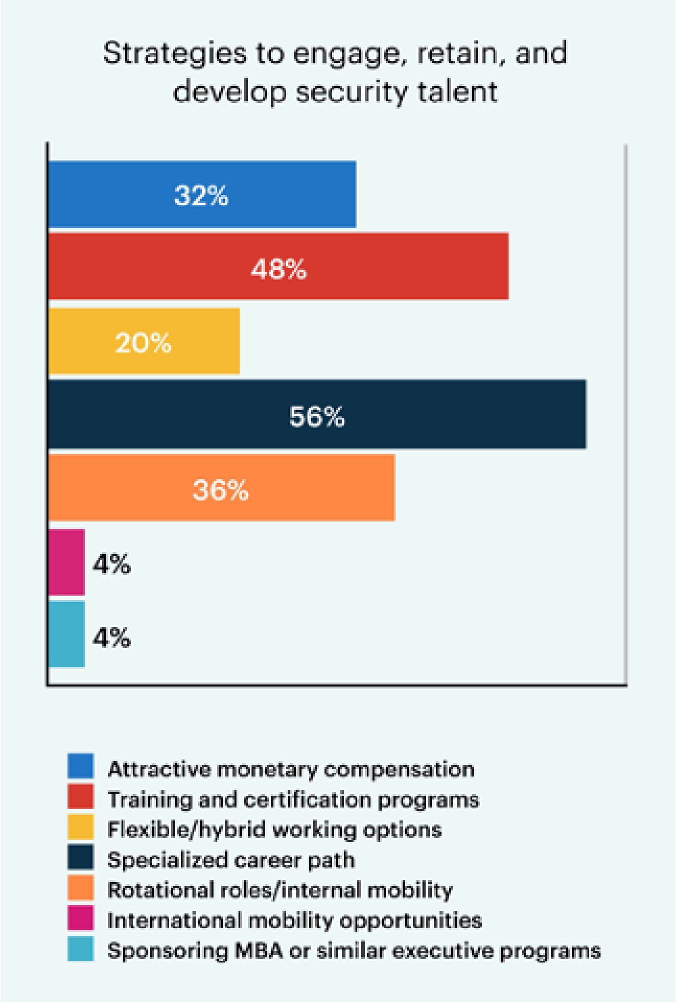
Top barriers while addressing cybersecurity challenges

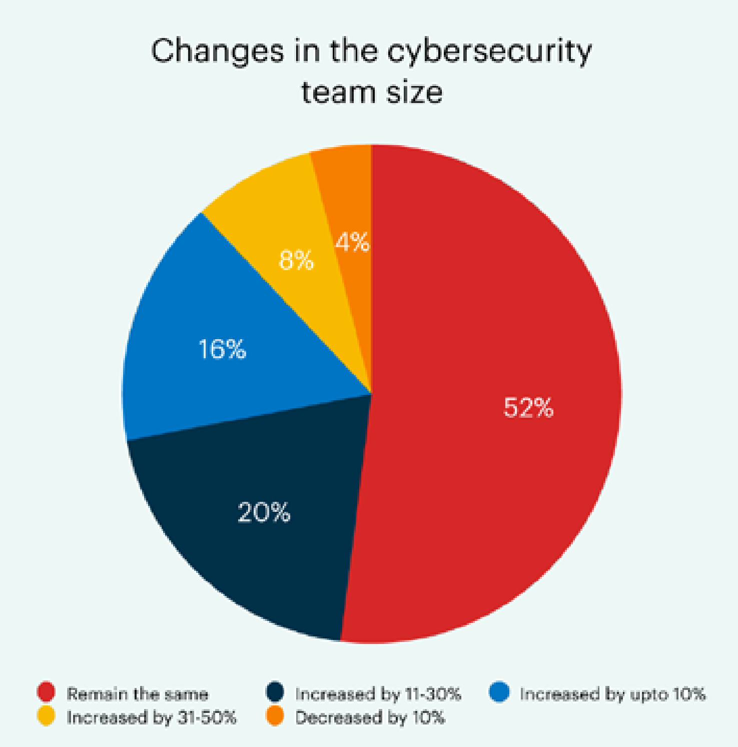
1. Decentralized IT and security infrastructure and operations
2. Shortage of skilled staff/lack of appropriate skill sets
3. Legacy infrastructure and solutions to address emerging threats
4. Technology/product/solution didn't live up to the expectations

"We must critically evaluate the practicality and relevance of cybersecurity courses in universities to ensure graduates are adequately prepared for the evolving cyber landscape," says Dr Fene Osakwe, Council Member, Forbes Technology & Cyber Security Mentor, Springboard.



Cyber Career Pathways Take Center Stage in CISO Priorities





Top strategies to engage, retain, and develop security talent

1. Specialized career path
2. Training and certification programs
3. Rotational roles/internal mobility
4. Attractive monetary compensation
5. Flexible/hybrid working options

The findings reveal diverse strategies to engage, retain, and develop security talent, with a clear emphasis on specialized career paths as the top priority for 56% of respondents. This highlights a growing recognition of the importance of providing clear progression opportunities and skill development pathways within the security field.

Additionally, training and certification programs are valued by 48% of CISOs, indicating the significance of ongoing learning and professional development in retaining talent. Rotational roles and internal mobility, favored

by 36%, offer employees diverse experiences and opportunities for growth. While monetary compensation and flexible working options also hold appeal, the emphasis on career advancement and skill enhancement underscores the critical role of professional development in talent retention within the cybersecurity domain.

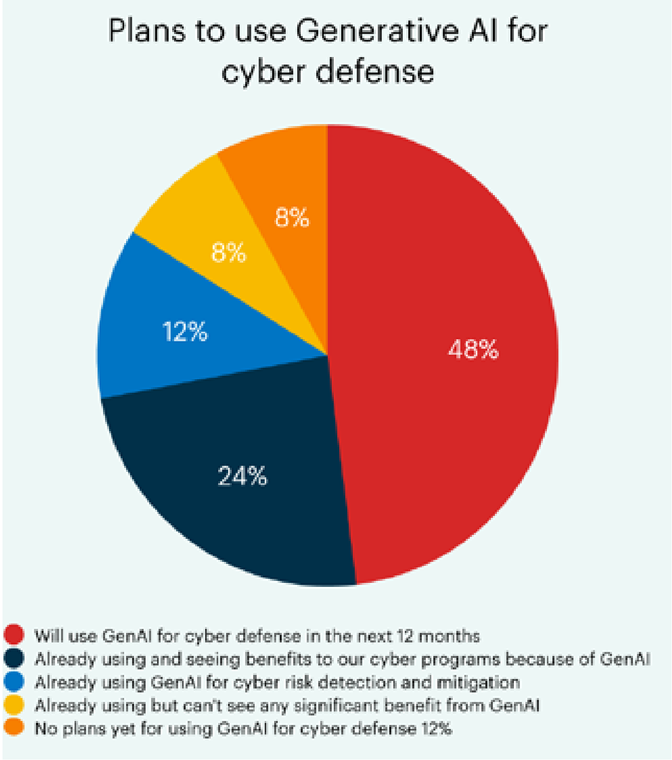
Further, the findings reveal a mixed picture regarding changes in security team size within organizations. While almost 45% report an increase in team size by 10% or more, with a notable 20% experiencing growth of 11-30%, a majority of CISOs (52%) indicate that their team size has remained unchanged.

This variation in team size adjustments may reflect differing organizational responses to evolving cybersecurity threats and priorities. Factors such as increased awareness of cyber risks, regulatory requirements, and the growing complexity of IT environments could drive organizations to invest in expanding their security teams. Conversely, other organizations may prioritize optimizing existing resources or leveraging technology solutions to enhance security capabilities without significant changes in team size.

Nearly half (48%) of surveyed CISOs plan to implement GenAI for cyber defense within the next 12 months. Additionally, a substantial 44% are already utilizing GenAI for cyber risk detection and mitigation. Among these users, 24% report experiencing tangible benefits to their cyber programs. However, 8% express dissatisfaction, citing a lack of significant benefits despite already implementing GenAI.

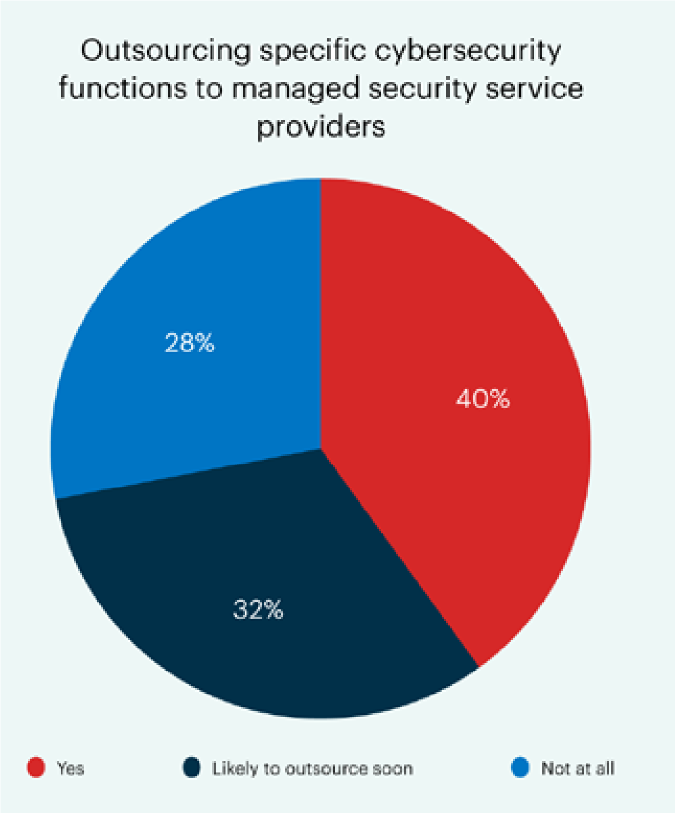
The findings underscore a growing reliance on GenAI technology for cyber defense. This indicates a widespread recognition of the potential of AI-driven solutions to enhance cybersecurity measures. The significant portion already using GenAI for risk detection and mitigation, along with a subset experiencing tangible benefits, highlights the efficacy of these tools in bolstering cyber programs. However, the minority reporting no significant benefits suggests that while the technology holds promise, successful implementation may require fine-tuning or more tailored integration to fully realize its potential across diverse cybersecurity environments.

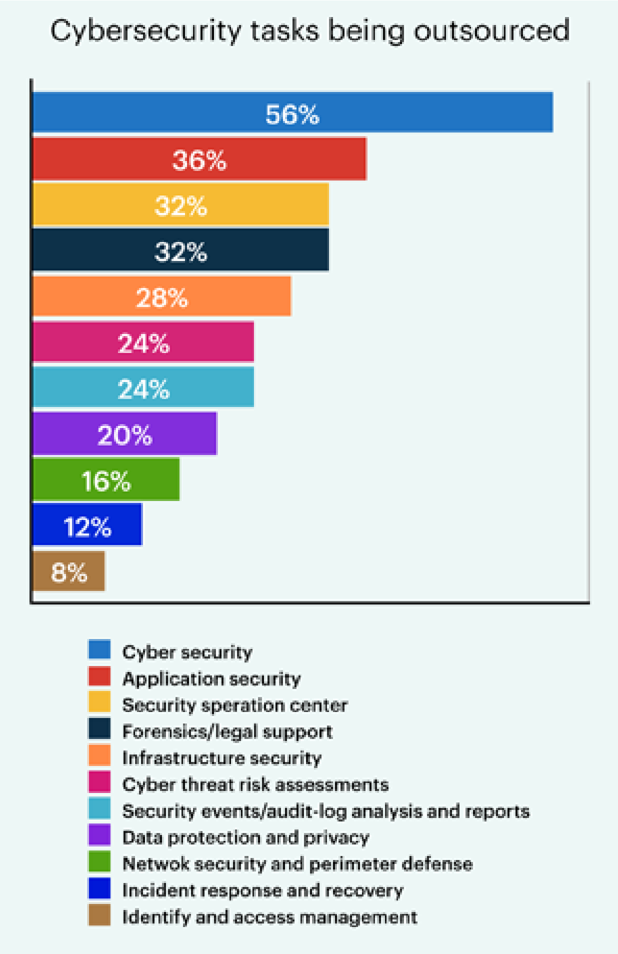
CISOs are Embracing GenAI for Cyber Risk Management



While GenAI offers exciting possibilities for innovation and efficiency, it also presents new vulnerabilities and security risks. CISOs must carefully assess the implications of integrating GenAI into their systems to safeguard sensitive data and mitigate potential threats. By adopting a cautious approach, CISOs can proactively tackle security concerns

Cloud Security & Application Security Top Outsourcing Priorities





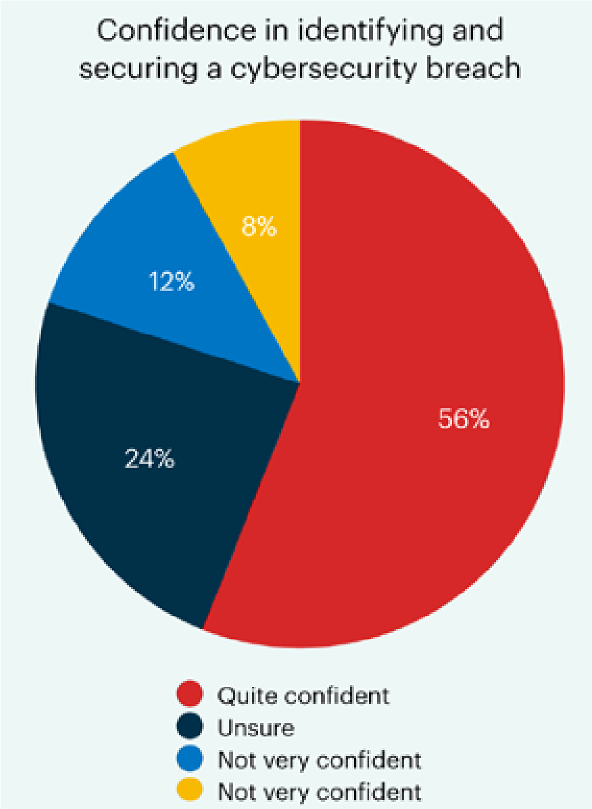
and develop strategies to protect their organizations. It's crucial for CISOs to stay informed about AI technology advancements and collaborate with their teams to implement robust security measures aligned with their organization's needs.

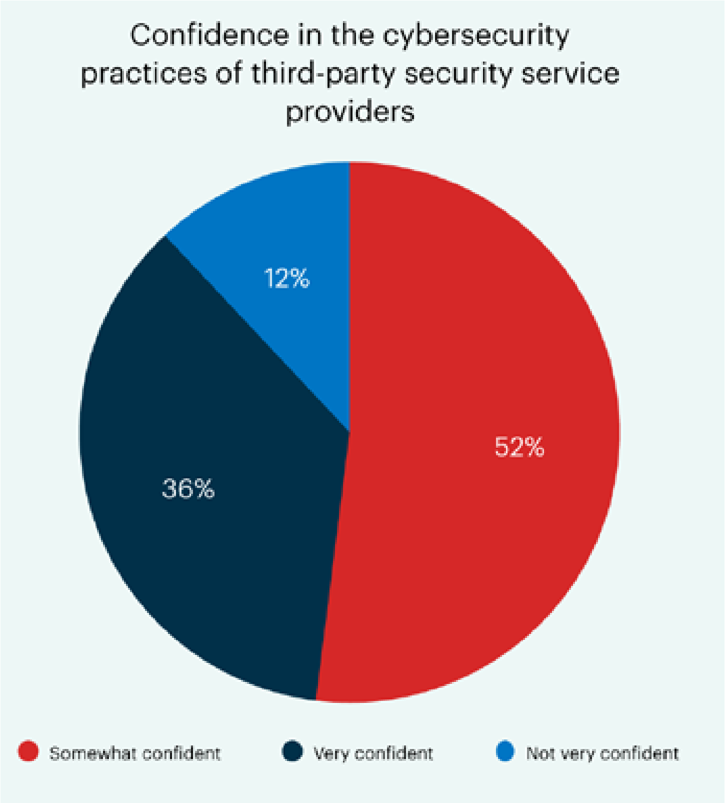
The rapid evolution of artificial intelligence brings forth various security challenges. From data breaches to ethical dilemmas in AI decision-making, the landscape is complex. A key concern is the potential manipulation or bias in AI systems, leading to discriminatory outcomes. Ensuring fairness and transparency in AI algorithms is essential. Additionally, interconnected AI systems raise

Top cybersecurity tasks CISOs are outsourcing

1. Cloud Security
2. Application security
3. Security operations center
4. Forensics/legal support
5. Infrastructure security
6. Cyber threat risk assessments
7. Security events/audit-log analysis and reports

Divergent Confidence Levels in Cybersecurity Breach Response



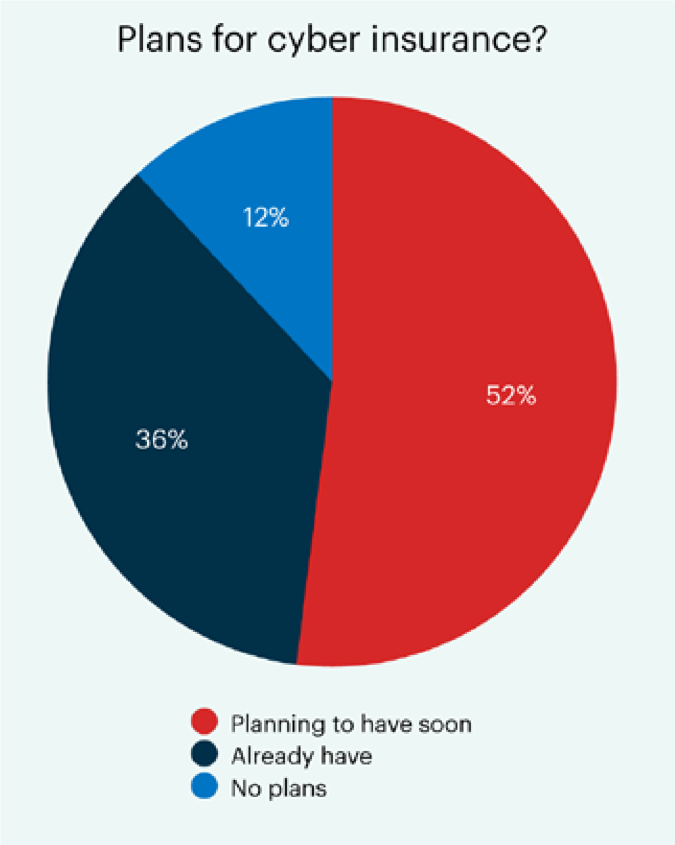


fears of large-scale cyber attacks and threats to critical infrastructure. Protecting against such risks demands robust cybersecurity measures and constant vigilance. Moreover, managing vast amounts of data processed by AI systems poses challenges in data privacy and protection.

CISOs can tackle these challenges by deploying AI-powered security solutions to detect and respond to breaches effectively. Fostering a cybersecurity-aware culture among employees through training and communication is vital. Collaboration with AI experts and staying updated on AI developments are also crucial for devising defense strategies against potential cyber threats. By understanding how AI technologies can be exploited by cyber attackers, CISOs can proactively devise robust defense strategies. In summary, addressing security challenges in GenAI requires a multifaceted approach involving advanced security solutions, awareness campaigns, and staying informed about AI advancements.

The findings underscore a notable trend towards outsourcing cybersecurity functions to managed security

Cyber Insurance Gains Major Traction as CISOs Look to Mitigate Risk



service providers (MSSPs), with a significant 40% already leveraging external expertise in this realm. Additionally, the prospect of outsourcing is appealing to 32% of CISOs who are considering such a move shortly.

This growing inclination towards outsourcing can be attributed to several factors, including the increasing complexity of cyber threats, the shortage of skilled cybersecurity professionals, and the need for specialized expertise and round-the-clock monitoring. By outsourcing certain functions to MSSPs, organizations can access advanced capabilities, enhance their cybersecurity posture, and alleviate the burden on internal resources, allowing them to focus on core business objectives. However, the 28% of CISOs who opt not to outsource may prioritize maintaining control over sensitive data or prefer in-house expertise tailored to their specific needs and requirements.

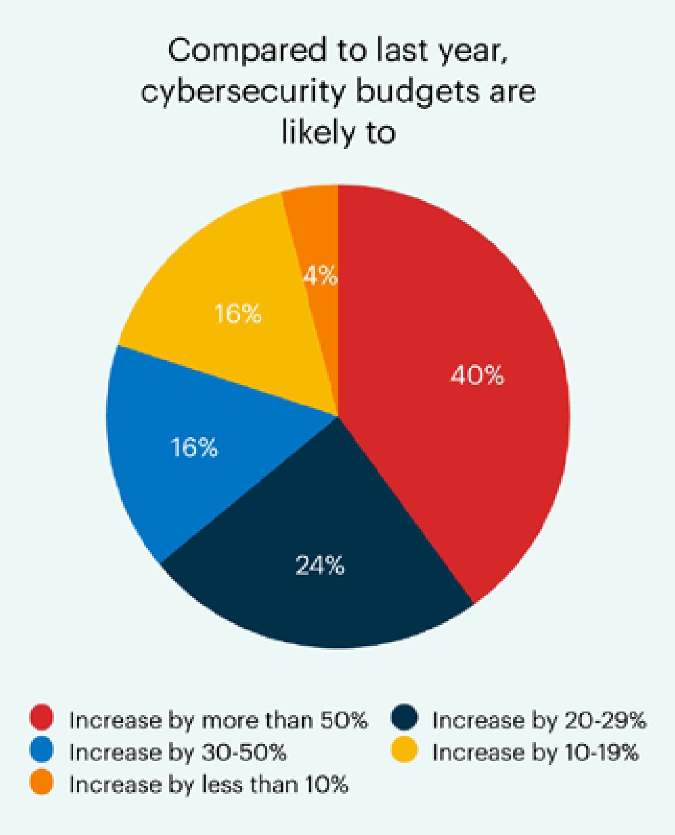
The results paint a clear picture of the cybersecurity tasks most commonly outsourced or likely to be outsourced to managed security service providers (MSSPs). Cloud security emerges as the top priority, with a majority of 56% of CISOs opting for outsourcing in this area. This trend is unsurprising given the complexity and specialized nature of cloud security requirements, coupled with the rapid adoption of cloud technologies.

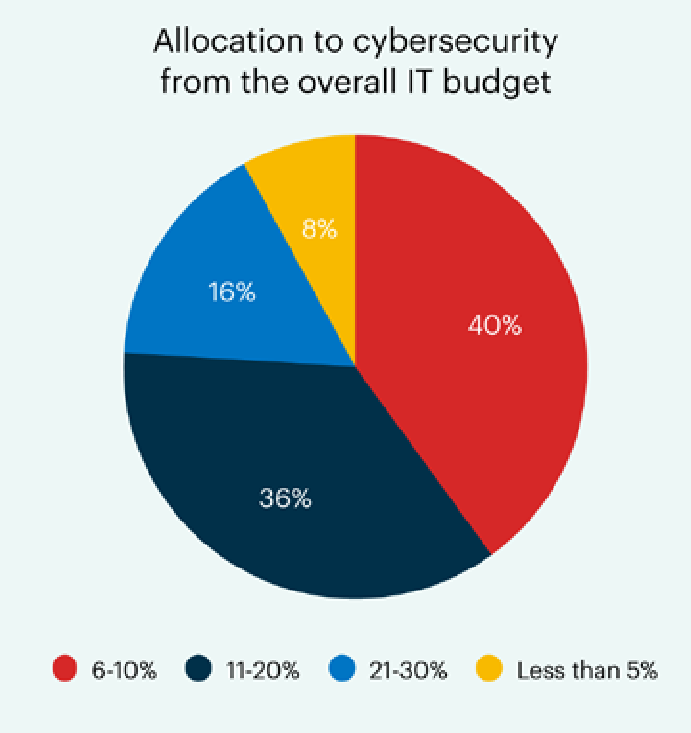
Additionally, the significant outsourcing of application security by 36% of CISOs reflects the need for expert oversight in safeguarding critical software assets. Tasks such as security operations center management and forensics/legal support follow closely, indicating a recognition of the benefits of outsourcing these specialized functions to external partners. This strategic allocation of responsibilities allows organizations to tap into specialized expertise, enhance operational efficiency, and bolster their overall cybersecurity posture.

The findings highlight a notable discrepancy in confidence levels regarding the ability to quickly identify and secure cybersecurity breaches within organizations. While a majority, constituting 56% of respondents, express confidence in this capability, a significant 32% admit to being either unsure or not very confident. Moreover, only 12% of CISOs report feeling very confident in their organization’s readiness to handle cybersecurity breaches promptly.

This variance in confidence underscores the multifaceted nature of cybersecurity preparedness, which is influenced by factors such as the complexity of cyber threats, the efficacy of detection and response

Over 56% of CISOs Anticipate Cybersecurity Budget Increases



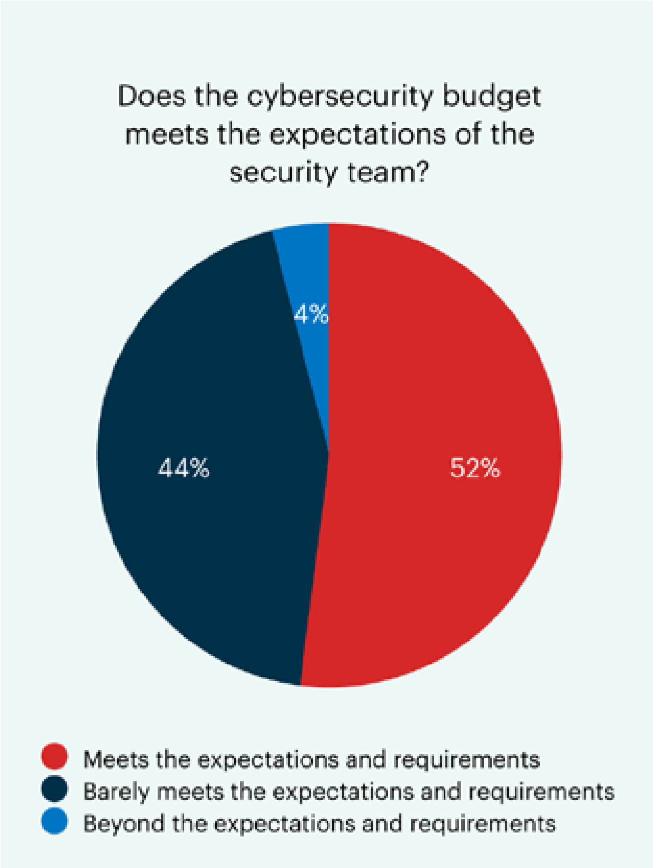


mechanisms, and the level of investment in cybersecurity resources and training. Addressing this disparity requires a holistic approach, encompassing continuous improvement of detection and response capabilities, robust incident response planning, and ongoing cybersecurity awareness and training initiatives across the organization.

Further, the results reveal a nuanced perspective on the confidence levels in the cybersecurity practices of third-party security service providers. While a majority, comprising 52% of respondents, express some level of confidence, a notable 12% admit to feeling not very confident in these practices. Interestingly, only 36% of CISOs report being very confident in the cybersecurity practices of their third-party providers.

This variation in confidence levels underscores the importance of diligent vetting and ongoing monitoring of third-party vendors' security protocols. Concerns are stemming from factors such as the lack of transparency or visibility into vendor security measures, instances of data breaches or security incidents involving vendors, and evolving regulatory requirements governing vendor risk

CISOs Split on Satisfaction with Cybersecurity Budgets



management. To address these concerns and build greater confidence, CISOs should prioritize robust vendor risk management frameworks, regular assessments, and clear communication channels with third-party providers.

The outcomes unveil a growing recognition of the importance of cyber insurance as a crucial component of organizational risk management strategies. While 36% of respondents already have cyber insurance in place, a significant majority of 52% are actively considering purchasing cyber insurance for their organizations.

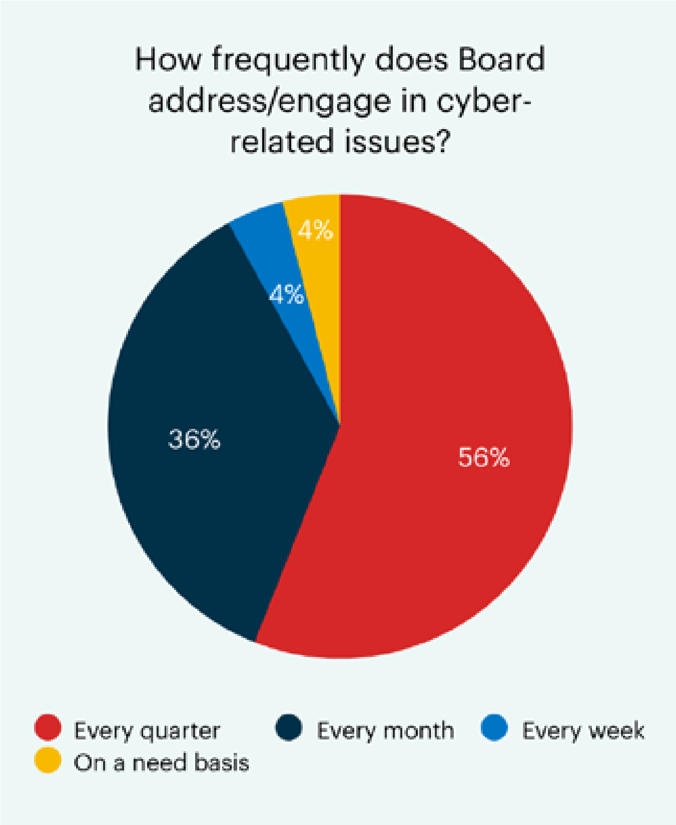
This trend reflects a heightened awareness of the evolving cyber threat landscape and the potential financial ramifications of cyber incidents. Cyber insurance offers a safety net against the increasing frequency and sophistication of cyberattacks, providing financial protection for costs related to data breaches, business interruptions, and regulatory fines. The relatively low percentage of 12% of CISOs without cyber insurance underscores the need for greater education and awareness about the benefits of this coverage, particularly as cyber risks continue to escalate in complexity and severity.

The outcomes reveal an upward trajectory in cybersecurity budgets underscoring a heightened awareness of the escalating cyber threats facing organizations. Over 56% of respondents anticipate an increase in cybersecurity budgets by more than 10%; of this, 16% expect substantial growth of 30% to 50%. With cyberattacks growing in sophistication and frequency, allocating substantial resources to bolster cybersecurity defenses has become imperative.

On the other hand, 40% of CISOs foresee budgets remaining stagnant. This variance in expectations reflects the diverse challenges and priorities facing organizations in allocating resources for cybersecurity initiatives. Factors such as the proliferation of remote work, the expansion of digital footprints, and stringent regulatory requirements further amplify the need for robust security measures. However, competing budgetary priorities, resource constraints, and uncertainties surrounding economic conditions are contributing to the sizable proportion of CISOs expecting budgetary stagnation. Balancing the need for robust cybersecurity measures with fiscal prudence remains a key challenge for organizations in the coming year.

Further, the findings highlight that a notable 52% of CISOs report dedicating 11% or more of their overall

Cybersecurity Occupies Major Mindshare among Board Members



IT budget to cybersecurity, with a significant 16% allocating a substantial 21-30% specifically for security initiatives. This allocation reflects a recognition of the critical importance of cybersecurity in modern business operations and the escalating cyber threats faced by organizations.

However, a sizable portion, comprising 40% of respondents, allocate a more moderate 6-10%, while 8% allocate a comparatively lower 5% or less to the security budget. This variance in allocation underscores differing organizational priorities, risk appetites, and budget constraints, highlighting the need for a balanced approach in resource allocation to effectively address cybersecurity challenges while optimizing overall IT expenditure.

"While the allocation for security budgets is increasing due to the recognized importance by the board, customer experience and digitalization also receive significant attention," says Abhijit Chakravarty, Senior Vice President of Core Network & Security Operations, HDFC Bank.

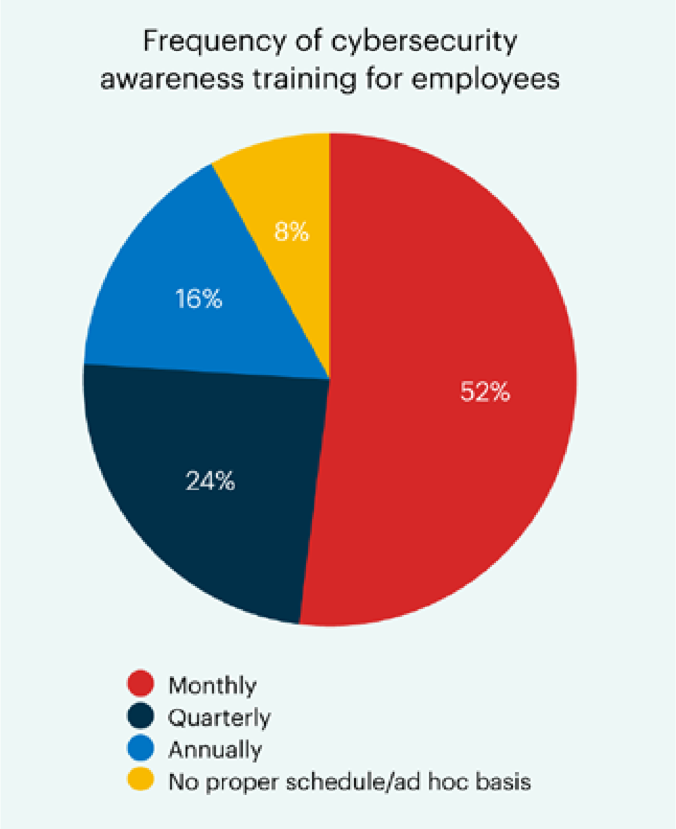
The outcomes reveal a significant divergence in perceptions regarding cybersecurity budget allocations within organizations. While a majority, comprising 52%, express satisfaction with the security budget allocation, a notable 44% of CISOs feel that the budgets only barely meet expectations and requirements. This disparity in satisfaction levels underscores the challenges faced by organizations in effectively allocating resources to address cybersecurity needs adequately.

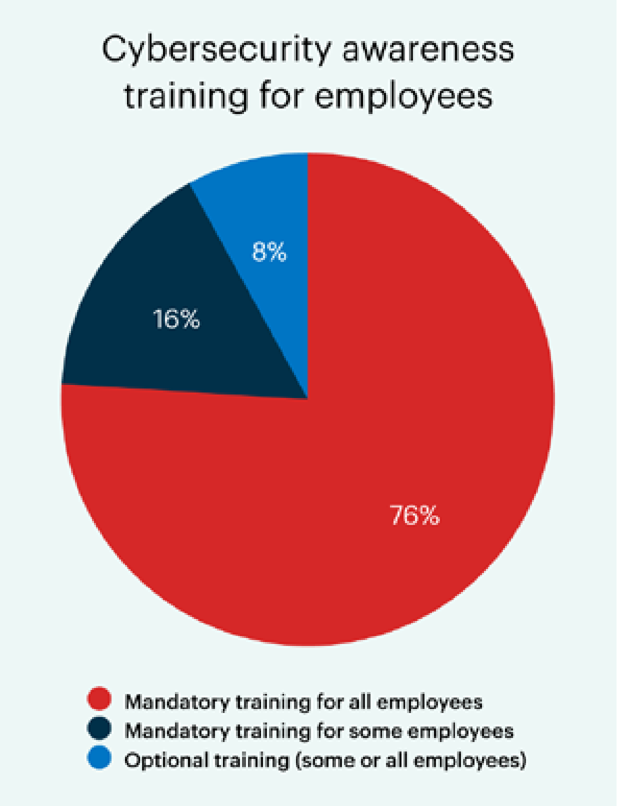
Factors such as evolving cyber threats, increasing regulatory requirements, and the need for investment in advanced security technologies contribute to the heightened expectations among security teams. However, competing budgetary priorities, resource constraints, and the difficulty in quantifying the return on investment in cybersecurity initiatives result in perceived inadequacies in budget allocations. Striking a balance between budgetary constraints and the imperative to strengthen cybersecurity posture remains a key challenge for organizations.

The findings shed light on the frequency with which cybersecurity issues are addressed by organizational boards. A significant 36% report that cybersecurity occupies a monthly slot on the board agenda, indicating a proactive stance towards addressing cyber-related concerns at the highest levels of governance. However, a majority of 56% reveal that their boards address cybersecurity matters quarterly, suggesting a more periodic approach to addressing these issues.

Giving Shape to Ideas

CISOs Prioritize Monthly Cybersecurity Awareness Training for Employees





This variation in frequency may reflect differing organizational priorities, risk appetites, and board compositions. Factors such as the evolving cyber threat landscape, regulatory requirements, and recent high-profile cyber incidents likely influence the frequency of board engagements on cybersecurity matters. Ultimately, ensuring regular board engagement on cyber-related issues is crucial for fostering a robust cybersecurity posture and aligning organizational strategies with evolving cyber risks.

A significant majority, comprising 52% of respondents, indicate that their organizations conduct these trainings every month. This frequent cadence reflects a proactive approach to ensuring that employees remain vigilant and well-equipped to recognize and respond to evolving cyber threats. Additionally, 24% of organizations opt for quarterly training schedules, while 16% conduct training annually.

However, 8% of organizations without any scheduled training regimen may be missing out on opportunities to cultivate a strong security culture and mitigate the risk of human error-related cyber incidents. Continuous and regular cybersecurity awareness training is essential in

fostering a resilient security posture, enhancing employee awareness, and safeguarding against potential cyber threats.

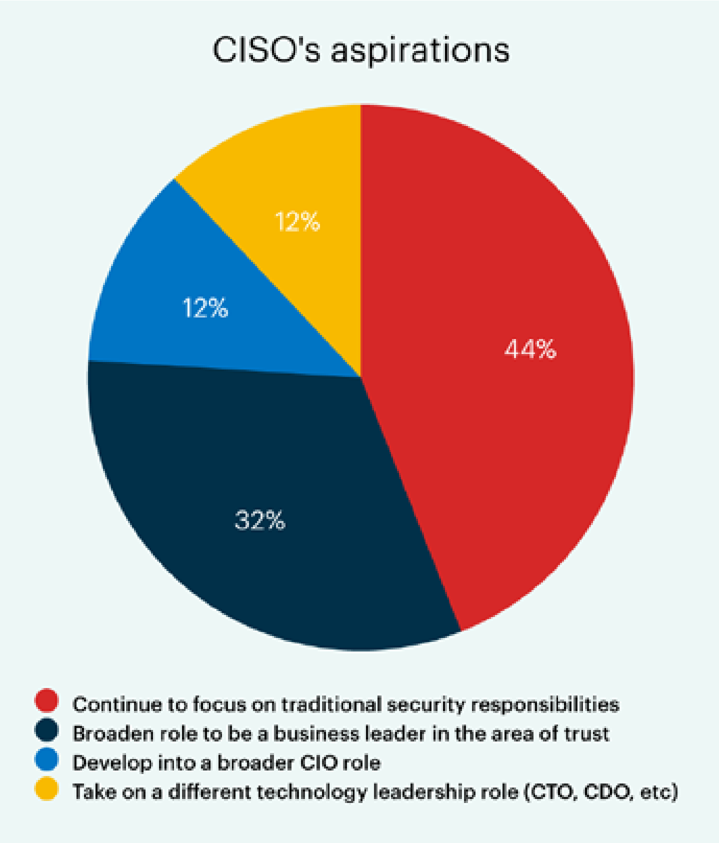
"Over 80% of cybersecurity breaches stem from user actions, underlining the need for organizations to prioritize user readiness and awareness," says Jenny Tan, President, ISACA Singapore Chapter.

Further, the outcomes underscore a strong commitment to cybersecurity awareness training within organizations, with a significant majority of 76% reporting that such training is mandatory for all employees. This reflects a recognition of the critical role that employees play in maintaining a robust cybersecurity posture and mitigating the risk of cyber threats. By making cybersecurity awareness training mandatory for all employees, organizations are ensuring that every individual understands their role in safeguarding sensitive information and detecting potential security incidents.

Moreover, the 16% of organizations mandating training for some employees may reflect a targeted approach based on job roles or access levels requiring heightened security awareness. However, the 8% of organizations offering optional training are missing out on the opportunity to cultivate a comprehensive security culture across the entire workforce, potentially leaving gaps in overall cybersecurity readiness.

The findings shed light on a significant shift in CISOs' career aspirations and the evolving nature of their roles within organizations. A majority, comprising 56% of respondents, express a desire to move on from their current positions or broaden their responsibilities to encompass more business-oriented roles. This trend reflects a growing recognition among CISOs of the need to align security initiatives with broader business objectives and priorities.

CISOs Eye Broader Business Roles in Career Evolution



Interestingly, 32% of CISOs are willing to broaden their roles to become business leaders in the area of trust, encompassing security, risk, and compliance—a testament to the expanding scope of responsibilities within the cybersecurity domain. Additionally, 12% aspire to transition into a CIO role or take on other technology leadership positions, indicating a desire for career advancement and greater influence in shaping organizational strategy and technology initiatives. This trend underscores the evolving role of the CISO from a purely technical function to a strategic business enabler, highlighting the importance of integrating security considerations into overall business decision-making processes.

Cutting-edge Technologies Drive SK Finance's Cybersecurity Strategy

BHAVESH KUMAR
Chief Information Security Officer and DPO, SK Finance

In a dynamic financial landscape increasingly shaped by digital innovation and cybersecurity challenges, Bhavesh Kumar, Chief Information Security Officer and DPO at SK Finance, offers invaluable insights into the organization's proactive approach to safeguarding online loan transactions, protecting customer data, and ensuring regulatory compliance. Kumar sheds light on the critical factors driving SK Finance's technology investments and its commitment to delivering secure and customer-centric financial services in an ever-evolving digital environment

Could you share an impactful milestone or success story from your journey in cybersecurity?

Bhavesh Kumar: Certainly, over my two-decade career, I've had the opportunity to work across various industry verticals, including IT, Pharma, Telecom, and Consulting, before transitioning to my current leadership role in BFSI. One significant milestone was when I joined a previous NBFC company. Recognizing the immense challenge of building cybersecurity frameworks from scratch due to regulatory and cyber threat pressures, I successfully created a comprehensive framework within my first decade as a CISO. This success continued as I moved to SK Finance, where I've spent the last six years preventing numerous cyber attacks and mitigating potential threats.

How do you perceive the current cybersecurity trends in the financial services sector, and what key measures are being implemented to address the evolving threat landscape?

Bhavesh Kumar: The BFSI sector plays a crucial role in the country's capital creation, despite facing numerous disruptions and cyber threats. With close to 30% of the financial landscape being covered by NBFCs, it's evident that cybersecurity is of paramount importance. Regulatory bodies like the RBI are pushing for enhanced controls and preventive measures to protect business, customer, and investor interests. Key measures include prioritizing cybersecurity assessments, strengthening remote access controls, building in-house cybersecurity capabilities, and conducting awareness programs to address the human factor in cybersecurity.

How does SK Finance ensure customer data protection and compliance with data privacy regulations, and what strategies are proving effective in this regard?

Bhavesh Kumar: SK Finance operates across diverse customer segments, including rural, semi-urban, and urban areas, each with unique data protection needs. Our data-centric approach prioritizes customer data protection through robust privacy policies tailored to different business segments. We adhere to regulatory guidelines, including RBI mandates, to ensure transparency, policy adherence, and customer trust. Additionally, leveraging technology solutions like encryption, access controls, and fraud detection systems helps safeguard customer data and ensure compliance with data privacy regulations.

How is digital innovation transforming loan processes, and what benefits and challenges are associated with integrating technology in lending operations?

Digital transformation, accelerated by the pandemic, has revolutionized loan processes, enabling faster and more efficient delivery of financial services. This digitization enhances customer experience, accessibility, and transparency. However, it also presents challenges such as cybersecurity threats, data privacy concerns, and the need for seamless integration across multiple platforms and networks. SK Finance invests in robust technology infrastructure, AI-driven risk assessments, and stringent fraud prevention measures to mitigate these challenges while maximizing the benefits of digital innovation.

What security measures does SK Finance implement to secure online loan transactions in the digital lending landscape?

Securing online loan transactions is critical for maintaining customer trust and preventing cyber fraud. SK Finance employs multi-factor authentication, data encryption, and access controls to secure loan transactions end-to-end. Additionally, we conduct thorough customer verification processes, integrate fraud detection systems, and provide customer awareness programs to prevent phishing and social engineering attacks. Our dedicated fraud control unit and partnerships with data bureaus further enhance our ability to identify and prevent fraudulent activities in online loan transactions.

> “We leverage advanced technologies like AI for security monitoring and automation, ensuring proactive threat detection and response.”

What technologies does SK Finance use to ensure customer data protection, fraud prevention, and overall cybersecurity?

SK Finance leverages advanced technologies like AI for security monitoring and automation, ensuring proactive threat detection and response. We implement robust access control mechanisms, including role-based access and privileged access management, to safeguard customer data. Additionally, we utilize endpoint detection and response (EDR) solutions, security operation centers (SOCs), and continuous security monitoring to detect and mitigate cyber threats in real-time. Our investment in AI-driven risk assessments, secure API integration, and fraud detection systems further strengthens our cybersecurity posture and ensures customer data protection.

How does SK Finance manage data flow and collaboration while ensuring compliance with regulations in the highly regulated NBFC sector?

Data flow and collaboration are essential for business operations, but they must be managed securely and compliantly, especially in the highly regulated NBFC sector. SK Finance adopts a containerized approach to API integration, ensuring secure data flow across platforms while adhering to regulatory requirements. We implement network segmentation, data encryption, and access controls to protect sensitive data and prevent unauthorized access. Regular audits, risk assessments, and compliance checks ensure that our data management practices align with regulatory standards and industry best practices.

Could you share the top three critical factors driving SK Finance’s technology investments and business expectations?

Certainly. At SK Finance, our technology investments are driven by three critical factors: first, the need for AI-driven security solutions to enhance threat detection and response capabilities; second, the importance of innovative access management solutions to balance security and user convenience; and third, the focus on proactive threat simulation and testing to identify and mitigate cybersecurity risks proactively. These factors align with our business expectations of delivering secure, seamless, and customer-centric financial services in an evolving digital landscape.

IN CONVERSATION

Structurally, CISOs should Report Directly to CEOs

DR. FENE OSAKWE
Council Member, Forbes Technology &
Cyber Security Mentor, Springboard

In a recent interview with Dr. Fene Osakwe, Council Member at Forbes Technology & Cyber Security Mentor, Springboard, we explored the evolving landscape of cybersecurity. Drawing from his expertise, Dr. Osakwe shed light on emerging threats, proactive defense strategies, and the critical role of cybersecurity in today's digital age

What are some of the emerging cybersecurity threats that organizations should be aware of, and how are these threats evolving in sophistication and impact?

Well, I recently published an article on Forbes titled "Top Cybersecurity Trends for 2024," where I discussed about nine trends. Let's focus on a few. One significant trend is nation-state-sponsored attacks. With increasing global tensions, countries are paying hackers to compromise other nations' security, steal data, and disrupt critical infrastructure. Another emerging trend is the automation of cyber attacks, pitting machines against humans. The ease of automating attacks makes them more sophisticated and challenging to combat. Lastly, there's the issue of burnout among security professionals. The overwhelming responsibilities, compliance requirements, and constant cyber threats contribute to mental health issues within the cybersecurity workforce.

Being a Chief Information Security Officer (CISO) requires multitasking and vigilance. How can organizations effectively address these evolving cyber methodologies?

Cybersecurity training is crucial, but it's no longer sufficient to rely solely on awareness. We need comprehensive training that equips employees with practical skills to identify and respond to threats effectively. Additionally, organizations must leverage machine learning and artificial intelligence in their security architecture to combat sophisticated attacks. Security by design should be integrated into every aspect of product development and processes. Lastly, the board needs to take more responsibility for cybersecurity to ensure adequate resources and attention are allocated to this critical area.

As the shift to remote work continues, what cybersecurity challenges arise, and how can organizations secure remote endpoints effectively?

Remote work introduces new vulnerabilities, requiring a proactive approach to security. Beyond awareness training, organizations should implement multi-factor authentication and behavioral analytics to detect unusual activities. Continuous monitoring and agile response mechanisms are essential to mitigate risks associated with remote work. For instance, isolating compromised devices immediately can prevent further damage.

Ransomware attacks and data breaches remain prevalent. How can organizations enhance their resilience to such threats and protect sensitive data?

A holistic approach to cybersecurity resilience is vital. Organizations should establish governance frameworks, implement data classification, and deploy robust security controls. Compliance with regulations such as GDPR, PCI, and ISO standards provides a foundation for cybersecurity practices. Additionally, organizations must invest in detection and response capabilities, leveraging tools like Security Information and Event Management (SIEM) solutions for real-time threat detection and orchestration for efficient incident response.

Zero trust security is gaining popularity. What key principles should organizations consider when implementing a zero-trust strategy?

Zero trust emphasizes never trusting, assuming breach, continuous validation, and least privilege access. Organizations should authenticate users and devices, validate access continuously, and limit access to the bare minimum required for tasks. This approach enhances security by minimizing the attack surface and mitigating the risk of unauthorized access.

Zero trust may impact productivity. How can organizations balance security and productivity?

Data classification is essential in determining the level of security required for different assets. Organizations should apply stringent security measures to critical systems while adopting a more flexible approach for less sensitive areas. By prioritizing security based on the criticality of assets, organizations can minimize disruptions to productivity.

Who should CISOs report to, and how is this reporting structure evolving?

Structurally, CISOs should report directly to CEOs, positioning cybersecurity as a business risk rather than a technology issue. While this alignment varies globally, regulations and industry standards increasingly emphasize the importance of cybersecurity oversight at the highest levels. Establishing this reporting structure ensures cybersecurity receives the attention it deserves and aligns with other business functions like finance and marketing.

> “Structurally, CISOs should report directly to CEOs, positioning cybersecurity as a business risk rather than a technology issue. Establishing this reporting structure ensures cybersecurity receives the attention it deserves and aligns with other business functions like finance and marketing.”

Compliance with regulations is crucial. How can organizations effectively navigate compliance requirements while maintaining robust cybersecurity practices?

A holistic compliance program is key, focusing on aligning cybersecurity measures with regulatory mandates. Rather than chasing individual laws, organizations should adopt a comprehensive approach that addresses common cybersecurity principles across regulations. This entails robust governance, data protection, and proactive monitoring. By implementing a unified compliance framework, organizations can streamline compliance efforts while fortifying their cybersecurity posture.

What are your top tech and business priorities for the next two to three years?

My priorities center on leveraging technology for social impact, particularly in education. I aim to scale initiatives that support underprivileged students' access to quality education. Additionally, I'm working on my second book to further disseminate cybersecurity knowledge. Bridging the gap between technical and non-technical stakeholders remains a priority, as cybersecurity increasingly influences business decisions. Ultimately, my focus is on driving positive change and innovation in both technology and business spheres.

Integrating OT and IoT Devices Presents Unique Cybersecurity Challenges

JUSTIN ONG
CISO & DPO,
Panasonic

In an era marked by unprecedented digital transformation, cybersecurity has emerged as a paramount concern for organizations across industries. Justin Ong, Chief Information Security Officer & DPO at Panasonic, offers invaluable insights into navigating the evolving cybersecurity landscape. As industries embrace IoT integration and leverage AI-driven technologies, ensuring robust cybersecurity measures becomes imperative. Join us as Hong shares Panasonic's proactive approach to cybersecurity, shedding light on emerging threats, AI's role in threat mitigation, and strategies for future-proofing security

How do you perceive the current cybersecurity landscape, and what key trends or emerging threats are you observing?

In the wake of the pandemic, we've witnessed a rapid acceleration in digital transformation efforts across industries. The shift towards remote work and reliance on digital technologies has underscored the critical importance of cybersecurity. However, alongside this transformation, we're also seeing emerging threats and uncertainties. Geopolitical tensions, economic instability, and rising inflation rates add layers of complexity to the cybersecurity landscape. Organizations are now tasked with navigating these challenges while continuing to innovate and leverage technology effectively. As we move forward, it's imperative to not only embrace technological advancements but also to fortify our cybersecurity measures to mitigate potential risks.

Can you elaborate on the specific challenges organizations face

in integrating operational technology (OT) and Internet of Things (IoT) devices while maintaining robust cybersecurity measures?

Integrating OT and IoT devices presents unique cybersecurity challenges due to their inherent differences from traditional IT systems. Unlike PCs and smartphones, which typically have advanced security features, OT devices often operate on primitive systems with limited resources. This disparity in sophistication poses challenges in terms of vulnerability management and threat detection. Additionally, the interconnected nature of these devices amplifies the potential impact of cyberattacks, particularly on critical operational systems. Therefore, organizations must adopt a comprehensive approach to cybersecurity that encompasses both IT and OT environments. This involves implementing stringent access controls, conducting regular security audits, and leveraging advanced technologies such as artificial intelligence (AI) to detect and respond to threats effectively.

■ How does Panasonic approach the integration of IoT devices while ensuring robust cybersecurity measures?

At Panasonic, we prioritize security from the inception of projects, following principles such as Privacy by Design and Security by Design. This proactive approach ensures that security considerations are woven into the fabric of our IoT deployments from the outset. We employ a risk-based approach to security, tailoring our measures to the specific requirements of each project. This includes implementing robust access controls, conducting thorough vulnerability assessments, and regularly auditing our systems for potential security gaps. Additionally, we leverage cutting-edge technologies, such as AI-powered threat detection and response capabilities, to enhance our cybersecurity posture further. By taking a comprehensive and proactive approach to cybersecurity, we aim to safeguard our IoT deployments against emerging threats effectively.

■ Can you discuss the role of AI in cybersecurity and how it contributes to mitigating internal threats and enhancing response capabilities?

AI plays a pivotal role in cybersecurity by augmenting human capabilities and enabling organizations to detect and respond to threats more effectively. One area where AI shines is in threat detection, where it can analyze vast amounts of data in real-time to identify suspicious activities or anomalies. This proactive approach allows organizations to detect and mitigate potential threats before they escalate into full-blown incidents. Moreover, AI-powered tools can assist in responding to security incidents by automating response actions and orchestrating incident response workflows. This not only accelerates response times but also ensures consistency and efficiency in the face of evolving threats. Additionally, AI can help organizations address insider threats by analyzing user behavior patterns and flagging any anomalous or suspicious activities. By harnessing the power of AI, organizations can bolster their cybersecurity defenses and effectively mitigate internal and external threats alike.

> “AI plays a pivotal role in cybersecurity by augmenting human capabilities and enabling organizations to detect and respond to threats more effectively. One area where AI shines is in threat detection, where it can analyze vast amounts of data in real-time to identify suspicious activities or anomalies.”

■ As cybersecurity continues to evolve, how do you recommend organizations future-proof their security strategies to adapt to emerging threats and technologies?

Future-proofing cybersecurity strategies requires a multi-faceted approach that encompasses technological innovation, organizational resilience, and proactive risk management. Firstly, organizations must stay abreast of emerging threats and technological advancements in the cybersecurity landscape. This entails investing in research and development initiatives, fostering collaboration with industry partners, and participating in information-sharing forums. Additionally, organizations must cultivate a culture of cybersecurity awareness and accountability across all levels of the organization. This involves providing regular training and education to employees, establishing clear policies and procedures for handling sensitive data, and fostering a sense of ownership and responsibility for cybersecurity best practices. Furthermore, organizations should embrace emerging technologies such as AI, machine learning, and automation to enhance their cybersecurity capabilities. These technologies can help organizations detect and respond to threats more effectively, streamline security operations, and adapt to the ever-changing threat landscape. By adopting a proactive and holistic approach to cybersecurity, organizations can future-proof their security strategies and effectively mitigate emerging threats and technologies.

Training and Awareness are Paramount in Mitigating Cyber Threats

JENNY TAN
President, ISACA Singapore Chapter

In an era where digital transformation and evolving cyber threats shape the modern business landscape, cybersecurity expertise is more critical than ever. Jenny Tan, President, ISACA Singapore Chapter and a seasoned cybersecurity professional, offers invaluable insights into navigating this dynamic field. From her journey in the industry to strategies for talent development and risk management, Jenny shares her expertise on emerging trends and best practices. Join us as we delve into the complexities of cybersecurity with Jenny Tan

Could you please share about your journey and expertise in the field of cybersecurity?

My journey in cybersecurity began around 20 years ago when I started my career as a software engineer. Back then, I specialized in artificial intelligence, although cybersecurity wasn't as prominent as it is today. About a decade ago, there was a notable shift towards a tech risk perspective, which led me to transition into roles focusing on tech risk and audit, where cybersecurity played a significant role.

How have you observed the cybersecurity landscape evolve in recent years, and what notable trends or changes have impacted organizations?

The cybersecurity landscape has undergone significant changes in recent years. Initially, cybersecurity was primarily concerned with basic network security. However, it has evolved to encompass various digital aspects. Nowadays, it's not just about enterprise technology; organizations must consider the digital apps on mobile devices, operational technology, and IoT concepts. This complexity has made enforcing cybersecurity measures more challenging for organizations.

What emerging threats should organizations be vigilant about, and what measures can they take to enhance their cybersecurity posture?

Organizations need to be vigilant about emerging threats, and one of the critical measures they can take is to exercise caution when adopting new technologies. It's essential to recognize that over 80% of cybersecurity breaches stem from user actions. Therefore, continuous training and awareness programs are vital. Additionally, organizations should implement Tech Risk 101 sessions before adopting new tools to ensure awareness of associated risks.

Bridging the cybersecurity talent gap is crucial. How can organizations and educational institutes collaborate to nurture the next generation of professionals?

Addressing the cybersecurity talent shortage requires a multi-level approach. Firstly, organizations should invest in training existing staff to appreciate and manage risks effectively. Additionally, providing attachment and internship programs can attract new talent to the field. Collaboration with technology associations can also help convert non-tech individuals into tech roles, complementing efforts to groom technical specialists.

Compliance with data protection regulations is a priority. How can businesses navigate data privacy complexities and ensure compliance with evolving regulations?

Navigating data privacy complexities requires a structured approach. Organizations must inventory their data landscape and assess risks based on regulatory requirements. Risk-based security measures should then be implemented, considering crown jewels and regulatory mandates. Continuous training and deploying auditors for check and balance are essential to ensure compliance.

Change management can be challenging, especially concerning cybersecurity awareness for non-technical employees. What are some best practices for organizations in this regard?

Conducting scenario-based workshops can help non-technical employees understand their role in cybersecurity. Experiential learning enables them to grasp the importance of risk management. Organizations should emphasize that cybersecurity is everyone's responsibility, linked to their employment duties and company interests.

> “It's essential to recognize that over 80% of cybersecurity breaches stem from user actions. Therefore, continuous training and awareness programs are vital. Additionally, organizations should implement Tech Risk 101 sessions before adopting new tools to ensure awareness of associated risks.”

How do you see emerging technologies like AI and blockchain impacting cybersecurity strategies, and what opportunities and challenges do they bring?

While emerging technologies offer solutions, deploying them without understanding the associated risks can be perilous. I advocate for a right-fit approach, addressing real risks with appropriate tools. Technology can support but not solely solve cybersecurity challenges. Simple solutions may suffice, avoiding unnecessary complexity.

As the President of the ISACA Singapore Chapter, what initiatives have you led, and how do they contribute to business resilience and risk management?

We've introduced conversion programs to train non-tech individuals for roles in cybersecurity and tech risk. Through webinars and events, we promote knowledge sharing on emerging technologies and standards adoption. Our crisis simulation workshops aid industry professionals in enhancing crisis management capabilities.

Balancing various roles can be demanding. How do you manage your responsibilities effectively?

Time management is crucial, along with a genuine interest in what I do. Leveraging interconnected tasks and finding commonalities among roles help optimize efforts. Aligning objectives across roles enables multitasking and achieves multiple objectives simultaneously.

Zero Trust Gives much more Granular Control and Visibility on Access and Identity

ABHIJIT CHAKRAVARTY
Senior VP of Core Network & Security Operations at HDFC Bank

In an era of rapid technological advancement and evolving cyber threats, the banking industry stands at a crossroads. To delve into the currents shaping this landscape, we sat down with Abhijit Chakravarty, Senior Vice President of Core Network & Security Operations at HDFC Bank. With a wealth of experience in network infrastructure, cybersecurity, and emerging technologies, Chakravarty shares insights into the current trends driving the banking sector's transformation and HDFC Bank's strategies for staying ahead in this dynamic environment

■ Please provide insights into the current trends shaping the banking industry, particularly in terms of technology adoption and cybersecurity?

In the banking sector, three key trends dominate: payments, lending, and digitization. However, these endeavors are futile without robust cybersecurity measures. API integrations are at the forefront of technology adoption, facilitating seamless connectivity between applications. Security remains paramount, with a particular focus on API security, given the interconnected nature of modern banking systems. Moreover, application modernization, API integrations, blockchain, and confidential computing are crucial for enhancing security and efficiency.

■ How are banking organizations adapting their network infrastructure to meet the growing demands for speed, security, and seamless customer experience?

Banking networks are undergoing a transformation, moving away from traditional setups to software-defined networks (SDN) and Network as a Service models. The integration of SD-WAN and security blurs the lines between network and security, ensuring a holistic approach to infrastructure management. Additionally, application modernization and cloud-native architectures are pivotal for enhancing agility and scalability.

■ What strategies are banks employing to stay ahead of emerging cyber threats, considering the evolving nature of cyber risks?

Banks employ a two-pronged approach: defense and prediction. While defense mechanisms safeguard against known threats, predictive analytics and threat intelligence help anticipate and mitigate zero-day attacks. Technologies such as DDoS mitigation, email filtering, and identity and access management play a crucial role in bolstering security posture.

■ Are there any particular technologies you would like to highlight in this regard?

DDoS mitigation, email phishing prevention, identity and access management, threat intelligence integration, and zero-trust network access are vital technologies in the fight against cyber threats. Additionally, robust SIEM and SOAR solutions streamline incident detection and response, ensuring timely remediation.

■ How do you handle situations where systems are compromised or data breaches occur?

In the event of a system compromise or data breach, swift action is imperative. Isolating affected systems, conducting forensic analysis, and engaging cybercrime authorities are crucial steps. Additionally, having robust data backup mechanisms with air-gapped storage ensures data resilience and facilitates recovery in the aftermath of a breach.

■ Do you believe zero-trust architecture is effective in combating the challenges posed by emerging technologies like AI?

Zero trust gives you much more granular control and visibility on access and identity. If we look at traditional VPNs, they served their purpose in the past when people needed to log into the network to work. VPNs provided a certain level of security, and later, some security was added with VDI. However, the challenge with VPNs and VDI is that when you log into a network, you essentially have lateral access to everything on that network if you compromise one identity. Zero trust addresses this issue by providing visibility and control at every stage. It challenges you at every step of access. To simplify, VPN is like locking the front door of your house; once inside, you have access to everything. Zero trust, on the other hand, challenges you at every point, like allowing access to specific rooms in your house. It's about controlling access to different resources based on the user's identity and posture.

> “VPNs provided a certain level of security, and later, some security was added with VDI. However, the challenge with VPNs and VDI is that when you log into a network, you essentially have lateral access to everything on that network if you compromise one identity. Zero trust addresses this issue by providing visibility and control at every stage.”

■ How does zero trust handle BYOD scenarios?

With zero trust, when someone logs in from their device or a third-party device, it allows you to check the device posture. You can verify if the device is clean, if the antivirus is updated, if it's running the latest patches, and even if the software versions are up to date. For example, if someone wants to upload or download a PDF file, and the Adobe version they're using is outdated, zero trust can restrict that action. It gives you the capability to enforce security measures based on device posture.

■ What is the significance of identity and access management (IAM) in today's security landscape?

IAM is foundational in security. It's where security starts. Beyond IAM, organizations need mechanisms to log data from various systems. Simply logging data isn't enough; you need to be able to correlate and analyze it effectively. This is where AI comes into play. AI helps in correlating and analyzing data to identify anomalies or suspicious activities. However, it's crucial to fine-tune the algorithms continuously to minimize false positives and ensure accurate threat detection.

What are the standard operating procedures in case of a system hack or a network breach?

If a system is hacked and the network is compromised, the first step is to isolate the affected systems from any access. Then, the focus shifts to understanding what happened, how it happened, and where it originated from. Forensic analysis and incident response are critical at this stage. However, incident response should not just be a theoretical plan; it needs to be tested through simulations or surprise drills to ensure its efficacy. Red teaming exercises, where simulated attacks are launched to test incident response, are increasingly common in organizations.

What advice do you have for handling data breaches?

In case of a data breach, it's essential to act swiftly. Forensic analysis can help determine the extent of the breach and the whereabouts of the compromised data. Reporting the breach to cybercrime detection authorities, like the cybercrime cell, is crucial. They have made significant progress in handling such incidents. Additionally, organizations need robust data backup strategies, including air-gapped backups, to mitigate the impact of ransomware attacks. Hackers now target backup sets directly, so having secure backup mechanisms is crucial.

How are banks navigating the regulatory landscape while fostering innovation in financial services?

Banks need to classify and categorize data according to regulatory requirements, such as those outlined in the DPDP Act. Compliance audits, particularly for handling personal data (PCI DSS audits), are essential. Banks must ensure compliance with industry standards and regulatory requirements while partnering or collaborating with third parties. Security posture, risk assessment, and compliance auditing play a significant role in navigating the complex regulatory landscape.

> “AI helps in correlating and analyzing data to identify anomalies or suspicious activities. However, it's crucial to fine-tune the algorithms continuously to minimize false positives and ensure accurate threat detection.”

How do banks balance customer-centric initiatives with maintaining high standards of data protection and privacy?

Balancing customer experience with security is crucial. Too much convenience may compromise security, while excessive security measures may inconvenience customers. Technologies like SASE, API integrations, and digital journeys are essential for delivering a seamless customer experience while ensuring security. Organizations must focus on delivering SST (Simplicity, Speed, Trust) to customers to drive adoption of digital products and services.

What are your top tech and security priorities for the next one or two years?

Visibility and observability remain top priorities, along with threat assessment and risk management. Enhancing customer experience through omni-channel integration and leveraging AI for personalization are also key priorities. Additionally, application and infrastructure modernization, coupled with robust security measures, are essential for staying ahead in the evolving landscape.

How have budgets for IT landscapes changed, given the increased emphasis on security and digital transformation?

Budgets for security have increased as organizations recognize the importance of robust security measures. Similarly, investments in customer experience and digital transformation have also grown. However, it's essential to align budgets with strategic priorities and focus on executing initiatives effectively to achieve desired outcomes.

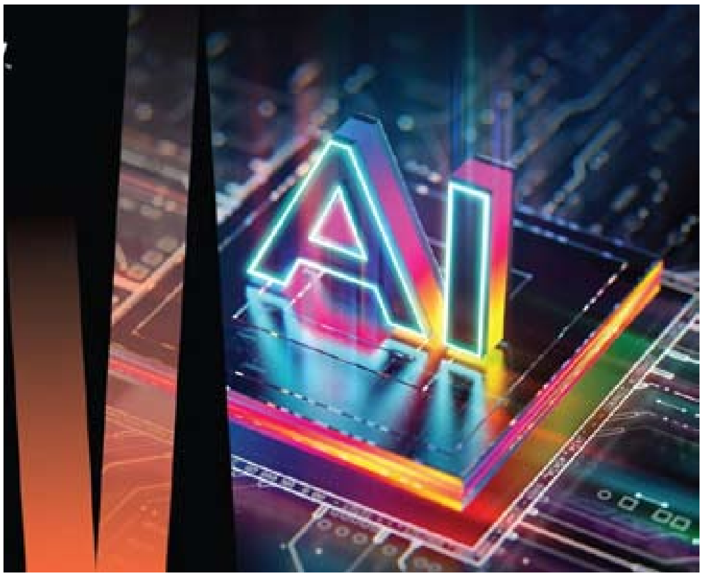
What do you see as the most impactful trend shaping the future of the banking industry, and how is HDFC Bank positioning itself to embrace these trends?

Open banking, payments innovation, and digitization are driving the future of the banking industry. HDFC Bank is positioning itself to embrace these trends by focusing on customer-centric initiatives, enhancing security measures, and leveraging AI and digital technologies to deliver personalized and seamless banking experiences.

What advice would you give to aspiring leaders in the ICT domain?

Aspiring leaders should focus on aligning vision, strategy, and execution. Execution is paramount for success; having a great vision or strategy is not enough if you cannot execute effectively. Additionally, prioritize customer experience and business transformation, and always strive for simplicity, speed, and trust in technology implementations. Finally, remember that execution is an ongoing journey, and continuous learning and adaptation are key to staying ahead in the rapidly evolving ICT landscape.

Vertiv Unveils AI Hub with First AI Reference Design Portfolio for Critical Infrastructure



As AI applications rapidly expand, data centers face a shortage of expert guidance. Vertiv (NYSE: VRT), a global leader in critical digital infrastructure, addresses this gap with the launch of their AI Hub. This platform offers partners, customers, and visitors access to expert information, reference designs, and resources to develop AI-ready infrastructure.

The Vertiv AI Hub provides white papers, industry research, tools, and power and cooling portfolios suitable for both retrofit and new applications. The reference design library includes scalable liquid cooling and power infrastructure supporting GPU chipsets from 10-140kW per rack.

Reflecting the evolving AI tech landscape, the AI Hub will be continuously updated with new content, including an AI Infrastructure certification program for Vertiv partners.

"Vertiv has a history of pioneering technology and insights for the data center industry," said Vertiv CEO Giordano (Gio) Albertazzi. "We are dedicated to providing the knowledge, portfolio, and guidance needed for our customers to deploy energy-efficient AI infrastructure. Our partnerships with leading chipmakers and innovative data center operators uniquely position us to assist on their AI journey."

Sean Graham, research director at IDC, added, "Every industry is seeking to leverage AI for business value, but there are many uncertainties about infrastructure deployment. Vertiv's expertise is crucial for businesses developing AI strategies and seeking comprehensive information sources."

Fujitsu Expands Automation with UiPath to Achieve Digital Transformation Goals

Fujitsu, a leading Japanese ICT company, is scaling its enterprise-wide use of the UiPath AI-powered Business Automation Platform. This initiative, part of the FujiTra project, aims to boost workforce efficiency by 40%.

Fujitsu launched the FujiTra (Fujitsu Transformation) project in October 2020 to overhaul its business processes, organizations, and corporate culture. Recognizing the potential of AI-powered automation, Fujitsu selected UiPath as its solution partner. Fujitsu has been utilizing UiPath's solutions across more than 140 departments globally since 2017, achieving substantial time savings.

The expanded collaboration will see UiPath assist Fujitsu in optimizing existing business processes and designing new, automation-led processes. This is expected to streamline operations and enhance workforce efficiency, preparing Fujitsu for future workforce changes. The goal is to maintain short-term productivity and achieve a 40% increase in workforce efficiency long-term.

Yuzuru Fukuda, Fujitsu's Corporate Executive Officer, emphasized the strategic importance of automation in accelerating business transformation and expressed confidence in UiPath as a trusted partner in this journey. Rob Enslin, CEO of UiPath, highlighted how Fujitsu exemplifies the successful integration of AI and automation for enterprise-wide transformation.

As part of the partnership, UiPath will also help Fujitsu train its workforce in automation skills through UiPath Academy courses and the open badge system, alongside hands-on and technical consultations.

Channel Point

Navigating the India Cyber Security Market Through a Channel Partner's Lens

Dear Readers,

As we delve into the intricate landscape of India's cyber security market, it's essential to recognize the pivotal role that channel partners play in shaping this dynamic sector. With cyber threats evolving at an unprecedented pace, the demand for robust security solutions has never been more critical.

Channel partners are uniquely positioned to bridge the gap between cutting-edge security technologies and the end-users who need them. By leveraging their deep understanding of local market nuances and customer needs, they can offer tailored solutions that address specific vulnerabilities and compliance requirements.

One significant trend we've observed is the growing collaboration between channel partners and cyber security vendors. This synergy is not just about pushing products but about co-creating value-driven security strategies. Channel partners are moving beyond traditional reseller roles to become trusted advisors, helping businesses navigate complex security landscapes with holistic approaches.

Moreover, the rise of managed security services is reshaping the market. Channel partners are increasingly adopting managed services models, providing continuous monitoring, threat detection, and response capabilities. This shift not only ensures enhanced security for clients but also opens up new revenue streams and business opportunities for partners.

However, challenges remain. The rapid pace of technological advancements, coupled with the increasing sophistication of cyber threats, demands continuous upskilling and investment in new technologies. Channel partners must stay ahead of the curve, ensuring they are equipped with the latest knowledge and tools to combat emerging threats.

In this issue, we explore the various facets of India's cyber security market from a channel partner's perspective. Through expert insights, case studies, and in-depth analysis, we aim to provide you with a comprehensive understanding of the current landscape and future opportunities.

As always, we welcome your feedback and look forward to your continued engagement.

Stay secure

K. Singhal

KALPANA SINGHAL, Editor
(E-mail: kalpana@techplusmedia.co.in)

TECHPLUS MEDIA™

EDITOR: KALPANA SINGHAL
CONTENT HEAD: Amit Singh
ASSISTANT EDITOR: Rajneesh De
CORRESPONDENT: Aaratrika Talukdar
CORRESPONDENT: Atreyee Chakraborty

INTEGRATED MARKETING COMMUNICATION:
Aakash Vahal
Saugata Mukherjee, Mamta Dhiman,
Nishit Saxena

ASSOCIATE ANALYST
Shaithra S

SALES:
Harpreet Singh | Pratap Jana

PRODUCTION HEAD:
Aji Kumar

WEBSITE:
Sheetal Varshney/Ramesh Kr

PROMOTION:
Vikas Yadav /Amit Pandey

CIRCULATION:
Pratap

FINANCE:
Inder Pal

HEAD OFFICE:
370A, Sant Nagar, East of Kailash, New Delhi
Tel: 41625763, 26237405, 41620042
Email - kalpana@techplusmedia.co.in

MARKETING OFFICE:
10 UF, West Wing, Raheja Tower,
MG Road, Shanthala Nagar, Ashok Nagar,
Bengaluru, Karnataka-560001

Delhi: 9711841991 | **Mumbai:** 9711841992
Kolkata / Guwahati: 9331072026
Bangalore: 9354347953

OWNED, PRINTED & PUBLISHED BY ANUJ SINGHAL Printed at Modest Graphics Pvt. Ltd., C 52-53, DDA Shed, Okhla Industrial Area, Phase - I, New Delhi-20, Place of Publication: 370A, 2nd Floor, Sant Nagar, East of Kailash, New Delhi-110065, Editor- Anuj Singhal

Note: While every possible care is taken prior to accepting advertising material, it is not possible to verify its contents. ITPV will not be held responsible for such contents, or for any loss or damages incurred as a result of transactions advertising/advertorial in this publication. We recommend that the readers make necessary inquiries and verification before remitting money or entering into any agreement with advertisers, or otherwise acting on advertisement in any manner whatsoever.

PANTUM
प्रिंटिंग के लिए नया युग

Pantum India Product Line

Business is Complicated, Printing Should be Simple

Vibrant 18 Series

Elite Series

PT-L280 Series

PT-L380 Series

PT-B680 Series

Simple&Smart Series

Simple&Smart Series

Mighty Series

4S Efficiency Series

Max Series

PANTUM SERVICE TOLL FREE NO.: 18003098240

WWW.PANTUM.IN

SALES REGION	PHONE NOS.	SALES REGION	PHONE NOS.
West Bengal & North East	98302 28532	Bihar & Jharkhand	9334317035

f Know more on @PantumIndia

Postal Registration No. - **DL(S) 01/3377/2019-21 Posting Date - 13-14, 27-28**
Registered with Registrar of Newspapers of India under RNI No. **DELENG/2010/32787**

SAMSUNG

Interactive display for future-ready education.

WAC Series

Experience an intuitive digital board that fulfils the demands of modern education.

Key features

- Android OS-based
- Easy multitasking
- Multi-screen sharing
- Intelligent app for classes

Scan to know more

Image simulated for representational purposes only.
Please dispose off e-waste and plastic waste responsibly. For more information of for e-waste pick up, please call 180057267864.

Cheil-17001/23

OWNED, PRINTED & PUBLISHED BY ANUJ SINGHAL, Place of Publication: 370A, 2nd Floor, Sant Nagar, East of Kailash, New Delhi-110065, EDITOR: Anuj Singhal