ITPV

Connecting with Solution Provider in
EMERGING MARKET

Vol XIII | Issue 11 | March 2024 | Pages 32

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

UNRAVELING THE MYTHS: UNLEASHING CYBERSECURITY'S TRUE POTENTIAL

Cherian Thomas
Wysetek Systems

Nityanand Shetty
Essen Vision

Neel Shah
Insight Business Machines

TECHPLUS MEDIA

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
BEST HARD DRIVE AWARD 2023

MOST INNOVATIVE PRODUCT OF THE YEAR 2023

15 dt
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

CHANNEL NEWS 25-29

Unraveling the Myths: Unleashing Cybersecurity's True Potential

In the digital realm, where every keystroke echoes in the vast expanse of the virtual universe, cybersecurity stands as a sentinel, guarding against the encroaching shadows of cyber threats. Yet, amidst its pivotal role in safeguarding our digital lives, cybersecurity often finds itself obscured by myths and misconceptions, hindering its true potential. These myths, like ancient sirens, lure organizations into treacherous waters, preventing them from fully harnessing the power of cybersecurity. Let us embark on a journey to unravel these myths, illuminating the path toward realizing cybersecurity's true value.

Amit Singh

Cybersecurity is solely an IT problem

All too frequently, individuals tend to view cybersecurity as the responsibility of the IT department alone, when in reality, it's everyone's responsibility. Cherian Thomas, Director, Wysetek Systems, explains, "Establishing a company-wide culture that prioritizes cybersecurity and adheres to cyber hygiene is imperative, and this initiative must originate from top-level leadership. The board of directors must recognize the importance of cybersecurity and allocate adequate resources to support the Chief Information Security Officer (CISO). Meanwhile, the IT department should prioritize building security measures by default, and all employees should undergo training to identify phishing attempts and implement multi-factor authentication (MFA) as standard protocol."

Blind to the holistic nature of cybersecurity, many enterprises entrust the safeguarding of their digital assets solely to the IT department. Ignoring the warnings of cyber experts, they neglect to involve other departments in security initiatives. Alas, when a sophisticated cyber-attack strikes, exploiting vulnerabilities in the supply chain management system, chaos ensues. The lack of collaboration between IT, procurement, and logistics departments proves fatal.

The moral is clear: cybersecurity is a collective responsibility that demands collaboration across departments. Only by fostering a culture of shared accountability can organizations fortify their defenses against the ever-evolving threat landscape.

We're too small to be a target

In the vast cosmos of cyberspace, size is but a trivial notion. Cyber adversaries scour the digital horizon in search of vulnerable prey, irrespective of their stature. Small and medium-sized enterprises (SMEs), ensnared by the myth of insignificance, often underestimate the gravity of cyber threats.

As per CyberPeace Foundation's 2022 report, 43% of the cyberattack targets were small businesses and SME startups. The clear rationale is that cyber perpetrators understand

" Meanwhile, the IT department should prioritize building security measures by default, and all employees should undergo training to identify phishing attempts and implement multi-factor authentication (MFA) as standard protocol. "

CHERIAN THOMAS,
Director, Wysetek Systems

these businesses typically possess less robust security measures and limited resources allocated to cybersecurity, making them vulnerable targets.

Many of the smaller organizations deem themselves inconspicuous to cyber predators. Unfortunately, their illusion shatters when a ransomware attack cripples their systems, threatening to extinguish their flickering flame of innovation.

These cyber-attacks serve as a stark reminder that cyber threats spare no one. "SMEs, with their limited resources, must prioritize cybersecurity as a cornerstone of their business strategy. Through prudent investments in robust security measures and employee awareness programs, they can erect a formidable barrier against cyber adversaries," adds Nityanand Shetty, CEO, Essen Vision.

There's no way we can hold back the cyberstorm

The escalating frequency of cyber attacks may seem overwhelming, but it's a consequence of the ongoing AI arms race. Neel Shah, Chairman, Insight Business Machines elaborates, "Attackers are increasingly adopting a scattergun approach to identify vulnerabilities, necessitating organizations to focus on automating their defenses effectively. With a shortage of cybersecurity and AI expertise, many organizations may struggle to acquire the necessary skills internally, making strategic partnerships with cybersecurity solution providers essential."

He points out that in the modern landscape, few organizations develop their software, relying instead on packaged applications, Software as a Service (SaaS), and AI to optimize data utilization and streamline processes. Similarly, in cybersecurity, organizations are increasingly turning to automation to manage significant aspects of their security measures. Strategic partners can provide expertise in leveraging automation tools, identifying threats, and implementing effective response tactics.

Compliance equals security

Compliance does not

> “SMEs, with their limited resources, must prioritize cybersecurity as a cornerstone of their business strategy. Through prudent investments in robust security measures and employee awareness programs, they can erect a formidable barrier against cyber adversaries.”

NITYANAND SHETTY,
CEO, Essen Vision

equal security. Compliance means meeting the minimum standards set by laws or regulations, which may not cover all the risks you face. Being compliant does not guarantee that you are secure.

Entrusted with safeguarding the financial assets of millions, many enterprises meticulously adhere to industry regulations, believing themselves impervious to cyber assaults. However, their complacency proves their undoing when a data breach, orchestrated by a nation-state actor, shatters their illusion of invincibility.

This underscores the inadequacy of compliance as a shield against sophisticated cyber threats. "Organizations must transcend the confines of regulatory mandates, embracing a proactive approach to cybersecurity that encompasses threat intelligence, risk assessment, and continuous monitoring," shares Shetty of Essen Vision.

Cybersecurity is an expense, not an investment

In the ledger of corporate finances, cybersecurity often languishes under the column of expenses, perceived as a drain on resources rather than a strategic investment. This fallacy, rooted in short-sightedness, obscures the immense value that cybersecurity brings to the table.

While investing in cybersecurity may have its expenses, the potential cost of a cyberattack outweighs it significantly. According to IBM's Cost of Data Breach Report, the cost of a data breach in India reached Rs 179 million in 2023. Therefore, prioritizing cybersecurity measures like employee training and security software can ultimately lead to cost savings and prevent expensive breaches for your business.

Recognizing the intrinsic value of cybersecurity, smart organizations reframe it as an investment in their future rather than a mere expense. Thomas of Wysetek, shares, "Through proactive investments in state-of-the-art security technologies and employee training programs, they fortify their digital fortress against incursions. By embracing a proactive stance towards security, organizations can mitigate risks, enhance operational

> With a shortage of cybersecurity and AI expertise, many organizations may struggle to acquire the necessary skills internally, making strategic partnerships with cybersecurity solution providers essential.

NEEL SHAH, CHAIRMAN,
Insight Business Machines

resilience, and unlock new growth opportunities."

Cybersecurity stifles innovation

In the crucible of innovation, where ideas take flight on the wings of creativity, cybersecurity is often perceived as a stifling force, constraining the boundless possibilities of technological advancement. This myth, propagated by detractors of security measures, undermines the symbiotic relationship between cybersecurity and innovation.

Driven by their pursuit of innovation, many organizations view cybersecurity as a hindrance to their quest for knowledge. However, their arrogance leads to a reckoning when a cyber-espionage campaign, orchestrated by rival entities, exfiltrates their groundbreaking research data.

Far from stifling innovation, cybersecurity acts as a guardian of progress, preserving the fruits of creativity from the ravages of cyber threats. By integrating security principles into the fabric of innovation, organizations can forge a path towards sustainable growth and resilience.

Cyber insurance is enough

While some organizations opt for cyber insurance as a safety net, it's essential to recognize that insurance alone cannot substitute robust cybersecurity measures. Cyber risk is complex and challenging to quantify, making it difficult to price insurance policies effectively. Comprehensive cyber audits are within the reach of only the largest organizations, leaving others reliant on crude risk assessment methods. Consequently, cyber insurance should complement cybersecurity and incident response efforts rather than replace them entirely.

As Shetty of Essen Vision highlights, effective cybersecurity doesn't have to be exorbitantly expensive. Cultivating a culture that values data, acknowledges risks, and prioritizes cyber hygiene is crucial. This organizational behavior not only enhances active cyber defense strategies but also makes them more cost-effective.

Automation in cybersecurity not only enhances security measures but also provides real-time insights into risk positions across hybrid environments. This allows CIOs and CISOs to allocate resources based on risk appetite, potentially reducing insurance premiums and prioritizing key risks effectively.

GenAI to Lead Revolutionary Shifts in Cybersecurity Landscape

Generative AI (GenAI) adoption will collapse the cybersecurity skills gap and reduce employee-driven cybersecurity incidents; two-thirds of global 100 organizations will extend directors and officers insurance to cybersecurity leaders due to personal legal exposure; and battling malinformation will cost enterprises more than $500 billion, as per recent Gartner research.

Deepti Gopal, Director Analyst, Gartner, says, "As we start moving beyond what's possible with GenAI, solid opportunities are emerging to help solve several perennial issues plaguing cybersecurity, particularly the skills shortage and unsecure human behavior. The scope of the top predictions this year is not on technology, as the human element continues to gain far more attention. Any CISO looking to build an effective and sustainable cybersecurity program must make this a priority."

Gartner recommends that cybersecurity leaders build the following strategic planning assumptions into their security strategies for the next two years.

By 2028, the adoption of GenAI will collapse the skills gap, removing the need for specialized education from 50% of entry-level cybersecurity positions.

GenAI augments will change how organizations hire and teach cybersecurity workers looking for the right aptitude, as much as the right education. Mainstream platforms already offer conversational augments but will evolve. Gartner recommends cybersecurity teams focus on internal use cases that support users as they work; coordinate with HR partners; and identify adjacent talent for more critical cybersecurity roles.

By 2026, enterprises combining GenAI with an integrated platforms-based architecture in security behavior and culture programs (SBCP) will experience 40% fewer employee-driven cybersecurity incidents.

Organizations are increasingly focused on personalized engagement as an essential component of an effective SBCP. GenAI has the potential to generate hyper-personalized content and training materials that take into context an employee's unique attributes. According to Gartner, this will increase the likelihood of employees adopting more secure behaviors in their day-to-day work, resulting in fewer cybersecurity incidents.

"Organizations that haven't yet embraced GenAI capabilities should evaluate their current external security awareness partner to understand how it is leveraging GenAI as part of its solution roadmap," says Gopal.

Through 2026, 75% of organizations will exclude unmanaged, legacy, and cyber-physical systems from their zero-trust strategies.

Under a zero-trust strategy, users and endpoints receive only the access needed to do their jobs and are continuously monitored based on evolving threats. In production or mission-critical environments, these concepts do not universally translate for unmanaged devices, legacy applications, and cyber-physical systems (CPS) engineered to perform specific tasks in unique safety and reliability-centric environments.

By 2027, two-thirds of global 100 organizations will extend directors and officers (D&O) insurance to cybersecurity leaders due to personal legal exposure.

New laws and regulations — such as the SEC's cybersecurity disclosure and reporting rules — expose cybersecurity leaders to personal liability. The roles and responsibilities of the CISO need to be updated for associated reporting and disclosures. Gartner recommends organizations explore the benefits of covering the role with D&O insurance, as well as other insurance and compensation, to mitigate personal liability, professional risk, and legal expenses.

By 2028, enterprise spending on battling malinformation will surpass $500 billion, cannibalizing 50% of marketing and cybersecurity budgets.

The combination of AI, analytics, behavioral science, social media, the Internet of Things, and other technologies enable bad actors to create and spread highly effective, mass-customized malinformation (or misinformation). Gartner recommends that CISOs define the responsibilities for governing, devising, and executing enterprise-wide anti-malinformation programs, and invest in tools and techniques that combat the issue using chaos engineering to test resilience.

Through 2026, 40% of identity and access management (IAM) leaders will take over the primary responsibility for detecting and responding to IAM-related breaches.

IAM leaders often struggle to articulate security and business value to drive accurate investment and are not involved in security resourcing and budgeting discussions. As IAM leaders continue to grow in importance, they will evolve in different directions, each with increased responsibility, visibility, and influence. Gartner recommends CISOs break traditional IT and security silos by giving stakeholders visibility into the role IAM plays by aligning the IAM program and security initiatives.

By 2027, 70% of organizations will combine data loss prevention and insider risk management disciplines with IAM context to identify suspicious behavior more effectively.

Increased interest in consolidated controls has prompted vendors to develop capabilities that represent an overlap between user behavior-focused controls and data loss prevention. This introduces a more comprehensive set of capabilities for security teams to create a single policy for dual use in data security and insider risk mitigation. Gartner recommends organizations identify data risk and identity risk, and use them in tandem as the primary directive for strategic data security.

Through 2026, 75% of organizations will exclude unmanaged, legacy, and cyber-physical systems from their zero-trust strategies.

Under a zero-trust strategy, users and endpoints receive only the access needed to do their jobs and are continuously monitored based on evolving threats. In production or mission-critical environments, these concepts do not universally translate for unmanaged devices, legacy applications, and cyber-physical systems (CPS) engineered to perform specific tasks in unique safety and reliability-centric environments.

By 2027, 30% of cybersecurity functions will redesign application security to be consumed directly by non-cyber experts and owned by application owners.

The volume, variety, and context of applications that business technologists and distributed delivery teams create means potential for exposures well beyond what dedicated application security teams can handle.

"To bridge the gap, cybersecurity functions must build minimum effective expertise in these teams, using a combination of technology and training to generate only as much competence as is required to make cyber risk-informed decisions autonomously," says Gopal.

Myths vs. Reality: Decoding Cybersecurity Misconceptions with Gartner's Oscar Isaka

OSCAR ISAKA,
Senior Director Analyst, Gartner

In an era where cybersecurity threats loom large, Chief Information Security Officers (CISOs) are at the forefront of safeguarding organizational integrity. Oscar Isaka, Senior Director Analyst at Gartner, sheds light on the pivotal challenges facing CISOs and the prevailing myths hindering effective cybersecurity measures. Delving into topics ranging from CISO effectiveness to debunking common cybersecurity misconceptions, Isaka offers invaluable insights into the evolving landscape of cybersecurity strategy and execution. Join us as we explore the intersection of cybersecurity reality and perception through the lens of Gartner's expertise

As organizations navigate an increasingly complex threat landscape, what do you see as the top challenges that Chief Information Security Officers (CISOs) currently face?

Our recent study on CISO effectiveness has highlighted four key characteristics that are paramount for CISOs to adopt to excel in their positions. Firstly, fundamental leadership is essential, encompassing how they steer the information security company and organization. Secondly, service delivery plays a crucial role in how they provide cybersecurity services to the organization. Thirdly, the scale of governance is critical, determining how they facilitate distributed decision-making and security across the organizational spectrum. Lastly, enterprise responsiveness is pivotal in how they instill the significance of cybersecurity throughout the organization. From a personal perspective, these traits delineate the hallmarks of an effective CISO. Given that many CISOs originate from operational and technical backgrounds, it becomes imperative to evaluate their proficiency in assuming the mantle of a chief officer within the boardroom setting.

Can you elaborate on some of the prevailing myths in cybersecurity that hinder organizations from realizing the true value of their security measures?

Firstly, there's the misconception that more risk analysis equates to more protection. It's a common belief that inundating ourselves with data on paper will enhance our security. However, our research, including a survey conducted two years ago specifically on cyber risk quantification, revealed otherwise. Only 34 percent of Chief Security Officers (CSOs) felt that this approach spurred action. Thus, it's evident that simply conducting more risk analysis doesn't necessarily lead to heightened protection. What's crucial is how we interpret and utilize that information to prompt action promptly. One effective approach we advocate for is employing outcome-driven metrics, such as the tapestry framework, to gain quicker insights and foster actionable responses.

Secondly, there's the fallacy that more technology inherently translates to more protection. We often joke with clients, advising them not to invest in additional 'screwdrivers' unless they precisely understand the type of 'screw' they're tightening. In today's landscape, where there's a shortage of 3.9 million cybersecurity professionals, it's tempting to believe that more tools will streamline our tasks. However, what's imperative is discerning the minimum effective tool set – comprehending how existing tools synergize to bolster protection rather than indiscriminately acquiring more.

Additionally, there's the misconception that increasing the number of cybersecurity professionals automatically results in heightened protection. While it's natural to desire more personnel, the key lies in distributing decision-making across the business effectively. This approach, known as minimum effective expertise, entails empowering employees with cybersecurity knowledge, alleviating the need for constant oversight. Lastly, there's the notion that more controls equate to better protection. However, inundating users with controls often hampers speed and agility, as evidenced by statistics indicating that 93 percent of employees knowingly make insecure decisions due to perceived impediments to efficiency. Therefore, the solution lies in implementing minimal effective friction – identifying the least intrusive measures to enhance security without impeding workflows.

> “To align cybersecurity strategies with broader business objectives, organizations must first understand and prioritize business goals. This requires a shift in mindset, recognizing that the role of the CISO is not just technical but strategic.”

How can debunking these myths lead to more effective cybersecurity strategies?

Let's consider one of these myths, such as the belief that more cybersecurity professionals automatically equate to greater protection. A case study we highlighted during the keynote presentation involved Johnson and Johnson, which revamped its security and risk assessment procedures for employees. By empowering them with a self-service portal for risk assessments, they accelerated the process, enabling employees to better comprehend the risks they faced. The outcome? A staggering hundred thousand new initiatives propelled by cybersecurity, were achieved faster, more efficiently, and without the need for additional full-time equivalents (FTs). This example underscores how facilitating speed and decision-making autonomy empowers employees to proactively address security challenges.

How can organizations cultivate a culture of cybersecurity awareness among employees, and what strategies are effective in mitigating insecure behaviors

that may pose security risks?

Merely instructing employees on what not to click and exposing them to traps isn't an effective approach. It's about initially sensitizing them to the significance of security as an overarching concern. This awareness serves as a foundation for subsequent education initiatives. Following this crucial stage, collaborative efforts and user-centric experiences come into play. By designing security measures to seamlessly integrate with user workflows, organizations can promote a culture where security is perceived as an enabler rather than an obstacle. Whether by making the secure path the easy path or vice versa, these strategies aim to alleviate the need for employees to circumvent controls or perceive security measures as burdensome. Ultimately, it's about fostering a mindset among users that views security not as a hindrance, but as a facilitator of safe and efficient operations. Overcoming this challenge remains a pivotal focus for cybersecurity efforts in recent years.

■ The cybersecurity skills shortage is a widely acknowledged challenge. Do you think that increasing the number of cybersecurity professionals within an organization contributes to a more robust and resilient defense against evolving cyber threats?

The cybersecurity skills shortage presents a well-recognized challenge. However, the mere increase in the number of cybersecurity professionals within an organization doesn't inherently guarantee a stronger or more resilient defense against evolving cyber threats. Rather, the effectiveness hinges on how these professionals are utilized and integrated into the organization's processes. Each individual must grasp their role in what we term distributed risk decision-making. It's unrealistic to expect that a surplus of security personnel can oversee every aspect without drawbacks or inefficiencies.

Hence, the prevailing myth debunked here is the notion that more cybersecurity professionals automatically translate to better protection. Instead, the focus should be on cultivating a minimum effective expertise—a strategic allocation of skilled personnel where their contributions are maximized to address specific needs and challenges.

Often, there is a perception that cybersecurity is a hindrance to business agility. How can organizations align cybersecurity strategies with broader business objectives to ensure a harmonious relationship between security measures and organizational goals?

The crucial initial step, perhaps the cornerstone, is to genuinely grasp the organization's business objectives. Often, individuals in the cybersecurity field originate from a background in security engineering, where they are deeply entrenched in technical operations. However, upon assuming the role of a Chief Information Security Officer (CISO), many may lack a comprehensive understanding of what this position truly entails.

Recognizing that a CISO is not merely a technical expert but a business leader is paramount. This role necessitates an adeptness in discussing and aligning with business strategy and objectives, rather than solely focusing on security engineering jargon and technical intricacies. It's imperative to realize that information security is just one facet of the CISO's domain expertise.

By comprehending the essence of being a chief officer within the organization, one can then grasp the overarching business strategy and trajectory. This understanding empowers CISOs to influence the information security landscape effectively, identifying and mitigating risks that could impede the organization from attaining its objectives.

■ What key performance indicators (KPIs) do you recommend for organizations to gauge the effectiveness of their cybersecurity measures, and how can they continuously improve based on these metrics?

Aligned with the aforementioned rationale, our focus often remains entrenched in operational aspects. To address this, it's imperative to tether metrics to tangible business outcomes, a concept we advocate through Gartner's Outcome Driven Metrics framework. This framework intricately links specific business objectives with identifiable metrics, thereby enhancing the actionability of cybersecurity initiatives.

For instance, consider the often misinterpreted metric of patching cadence. Merely stating the number of patches applied, such as 35,000 in a month, lacks contextual significance. Without understanding the criticality of the assets or the urgency of patching, this figure remains arbitrary. Alternatively, a more insightful metric, as per Outcome Driven Metrics, would gauge the lead time for patching critical systems.

This metric facilitates a more meaningful dialogue, enabling stakeholders to grasp the operational realities. For instance, if it takes 10 days to patch critical systems, stakeholders may deem this timeframe inadequate and aspire for a 24-hour turnaround. Subsequently, discussions can evolve to address resource requirements and associated costs, fostering a deeper awareness among board members regarding the implications of cybersecurity decisions. Ultimately, outcome-driven metrics reframe key performance indicators (KPIs) into actionable insights, enriching cybersecurity discussions at both board and organizational levels.

Giving Shape to Ideas

From Complexity to Clarity: Fortinet's Strategy in the Age of Cybersecurity Consolidation

VIVEK SRIVASTAVA,
Country Manager, India & SAARC, Fortinet

In this exclusive interview, Amit Singh explores the dynamic landscape of cybersecurity challenges with Vivek Srivastava, Country Manager, India & SAARC, at Fortinet. The conversation delves into the pressing issues of tool sprawl, extended response times, automation challenges, and the pivotal role of vendor consolidation in fortifying organizational defenses. Gain insights into how Fortinet's innovative solutions are reshaping cybersecurity strategies, offering rapid responses, and simplifying complex security infrastructures for modern enterprises

How are organizations overcoming challenges associated with tool sprawl in the cybersecurity landscape?

The modern cybersecurity environment often suffers from tool sprawl, where organizations deploy numerous disparate security solutions. This scenario, while intended to bolster defenses, inadvertently complicates management and reduces overall visibility. Tool sprawl leads to significant challenges, including operational inefficiencies and increased vulnerability. The diversity of interfaces and protocols strains resource management and obscures the visibility necessary for effective threat detection and response.

Fortinet addresses these challenges through its Security Fabric platform, offering a unified security ecosystem. This approach simplifies cybersecurity management, consolidating various tools into a cohesive framework that enhances operational efficiency and security visibility. Adopting Fortinet's integrated solutions streamlines operations and improves threat response capabilities. Organizations gain enhanced visibility across their digital landscapes, enabling quicker and more accurate threat detection and mitigation efforts.

As per recent studies, security teams take approximately 6 days, with 60% of organizations taking longer than 4 days, to resolve security alerts. How critical is this extended response time, and what are the potential consequences in a threat landscape where attackers act within hours?

The critical nature of this lag in response time cannot be overstated. Cyber attackers are increasingly agile, often breaching and navigating through networks with speed and precision that current organizational response times cannot match. The average "dwell time"—the average period an attacker remains undetected within a network—still hovers around 6 months, providing ample opportunity for significant damage and data exfiltration.

Fortinet's Security Operations solutions have been pivotal in addressing this critical gap. By implementing Fortinet's advanced security technologies, organizations have seen dramatic reductions in the time to identify threats. The average time to detect threats, which could extend to 168 hours (or about 21 business days) without effective detection tools, is reduced to less than an hour, and in many cases, just seconds with Fortinet's Endpoint Detection and Response (EDR) technologies.

Moreover, the time required to triage these threats has been reduced from an average of eight hours to just 10 minutes. Most impressively, containment times have dropped from 4.2 hours to a mere one minute, showcasing Fortinet's commitment to rapid response and containment capabilities.

What are the challenges faced by organizations while automating their defenses?

The deployment of automation and orchestration in cybersecurity is critically undermined when organizations rely on poorly integrated security tools. Disjointed security solutions create an environment where data is siloed, and automation efforts can't reach their full potential. Automation relies on the seamless flow of information between tools to trigger responses to detected threats. When these tools are poorly integrated, the lack of cohesive data and operational inconsistencies result in slower threat detection, delayed responses, and ultimately, a higher risk of successful cyber-attacks.

Fortinet tackles these challenges with its comprehensive suite of CARA (Cybersecurity Automation, Response, and Analysis) components. This integrated approach ensures that automation and orchestration are not hampered by the limitations of disparate tools. By harmonizing data across the security landscape, Fortinet enables organizations to employ more sophisticated and efficient automated defenses.

With Fortinet's solutions, the time to investigate threats has been drastically reduced from 6 hours to 1 minute or less. This acceleration is a testament to the power of integrated automation and orchestration, which can sift through vast amounts of data to identify threats with unparalleled speed and accuracy. Furthermore, the time to remediate identified threats has been cut from 12.5 hours to between 5 and 10 minutes in most cases, showcasing the effectiveness of Fortinet's automated response capabilities.

In light of the increasing trend toward cybersecurity vendor consolidation, how does Fortinet address the industry's need for a streamlined and effective defense ecosystem?

The strategic shift towards cybersecurity vendor consolidation is a clear response to the complexities and inefficiencies stemming from a sprawling security tool landscape. Organizations are increasingly recognizing the imperative to streamline their cybersecurity infrastructure to bolster their defense mechanisms against sophisticated cyber threats.

According to a recent Gartner survey, the trend of organizations pursuing a vendor consolidation strategy has surged from 80% in 2022 to an impressive 97% in 2023. This sharp increase underscores a widespread industry realization that a consolidated cybersecurity approach not only simplifies security operations but also enhances the effectiveness of an organization's overall security posture.

Fortinet has been at the forefront of this consolidation movement with its Security Fabric platform, which has been instrumental in providing over 50 integrated security products. This convergence of networking and security solutions within a single platform empowers organizations with seamless threat intelligence sharing and comprehensive visibility across their entire digital attack surface.

With the majority of organizations now favoring vendor consolidation, it is clear that the market is moving towards solutions that can offer an integrated and streamlined approach to security. Fortinet's Security Fabric platform is perfectly aligned with this trend, offering organizations a robust, scalable, and effective defense ecosystem that can adapt to the ever-changing cyber landscape.

> “In the battle against tool sprawl, Fortinet's Security Fabric acts as a unifying force, transforming complexity into cohesion for enhanced cybersecurity.”

What essential steps and technologies should organizations prioritize in creating a comprehensive incident response plan, communication strategy, and integrated cybersecurity system to enhance resilience against evolving cyber threats?

Improving cybersecurity resiliency is crucial for modern organizations to protect themselves against today's evolving cyber threats. The question is no longer if you'll be attacked but when. So the key issue organizations need to grapple with is, “What happens then?” As always, the building blocks are technologies, people, and processes. But how they're implemented and what they include are what make the difference between successfully navigating a concerted attack and struggling to recover.

Create a comprehensive incident response plan and related playbooks that outline the steps to take in the event of a cybersecurity incident. Develop a communication plan that outlines how the members of your organization will communicate with internal and external stakeholders in the event of a cybersecurity incident.

Stay ahead of cyber threats by investing in systems and platforms designed to function as an integrated system to enhance responsiveness, reduce vendor sprawl, enhance visibility and control, and centralized management. At the same time, any platform under consideration needs to include integrated artificial intelligence (AI) and machine learning (ML) technologies to accelerate threat detection, analysis, and response anywhere across your distributed network.

CISOs are Looking for a Consolidated Platform that Provides Integration of Consoles for Monitoring and Managing Platforms: Essen Vision

NITYANAND SHETTY,
CEO, Essen Vision

In a world where cyber threats are ever-evolving and organizations grapple with increasing complexities in their security landscapes, insights from industry leaders are invaluable. Nityanand Shetty, CEO of Essen Vision, provides expert perspectives on the challenges posed by disparate security tools, the importance of automation and orchestration, trends in cybersecurity consolidation, and the advantages of unified security offerings, in a brief interaction with Amit Singh

Studies indicate that organizations use an average of 31.58 disparate security tools. How does this complexity impact visibility and hinder effective detection and response to cyber threats?

The higher number of security tools organizations use today slows down the response as the ability to detect and respond gets more complicated as many of these tools lack integration capabilities. The lack of effective playbooks and automated orchestration of response also hinders effective response to cyber threats in these environments.

How does the deployment of automation and orchestration get affected when organizations rely on poorly integrated security tools? What role does this play in the meantime to detect and respond to cyber threats?

The cybersecurity landscape has become more complex than ever. Moreover, with multiple tools and technologies addressing various security needs, the integration of all of these has become difficult most of the time. That is where a strong SIEM integrated with an automated SOAR system comes in to monitor data in real-time and use UEBA to detect suspicious behavior. Upon detection, an alert is sent out, and a series of incident response actions is immediately launched. These actions can work to quarantine the threat, shut down affected devices, or offer additional actions to mitigate the threat.

Are you seeing enterprises consolidating their cybersecurity vendor landscape and reducing complexities in cybersecurity stacks? How does this consolidation contribute to better crisis management and overall resilience during cyber threats?

CISOs would like to stay on top of the multiple cyber threats their organizations face today and are looking for a consolidated platform that provides integration of consoles for monitoring and managing platforms, automating threat response, and security at the endpoints, applications, perimeter, cloud, and data level with an end-to-end Zero Trust Strategy and having a strong AI/ML-driven intelligence engine.

> “The higher number of security tools organizations use today slows down the response as the ability to detect and respond gets more complicated as many of these tools lack integration capabilities. The lack of effective playbooks and automated orchestration of response also hinders effective response to cyber threats in these environments.”

What, in your opinion, are the key advantages of a unified security offering, and how does it address the visibility gaps and integration challenges seen in organizations using disparate security tools?

Interoperability, better visibility, reduction in false alarms, improved functionality, data centralization, effective sharing of threat intelligence among tools, smooth orchestration, and an improved MTTR in the environment in case of any breach, are some of the key advantages of a unified security platform.

What are the best practices you would suggest to improve cyber resilience through reduced complexities, increased visibility, and effective detection and response?

To enhance cyber resilience, I recommend implementing several best practices:

- Conduct comprehensive employee cybersecurity training, consistently aiming to refine policies and procedures.
- Adhere to industry standards such as NIST and CertIN guidelines.
- Regularly review internal cybersecurity strengths and weaknesses.
- Integrate the Zero Trust framework to validate all access requests before granting access.
- Foster collaboration among tools and technologies using APIs to enhance integration and partnerships.
- Utilize robust AI/ML-based platforms to proactively defend against and protect from emerging threats.

What are the major cybersecurity trends you see as organizations move towards digital transformation and cyber resilience?

As the role of the CISO continues to evolve, aligning with the priorities of the board, it signifies a notable shift in cybersecurity strategy. With increased budget allocations, leadership is actively engaging in cybersecurity initiatives. Achieving cyber resilience hinges on fostering enhanced collaboration across various organizational functions, including Application, Cloud, Infrastructure, and Security teams.

In the upcoming year, discussions around generative AI and Privacy will take center stage, considering their profound impact on the industry. Additionally, cybersecurity stack consolidation is emerging as a prominent trend, streamlining security measures and optimizing resource utilization.

Code Generation and Optimization are the Primary Areas Where GenAI is being Used Significantly: Ascendion

KRISHNENDU CHAKRABARTY,
Associate Director of Platform Engineering at Ascendion

In this engaging discussion with Amit Singh, Krishnendu Chakrabarty, Associate Director of Platform Engineering at Ascendion, shares insights into the challenges and considerations in building and upgrading engineering platforms, the transformative impact of Gen AI, integration of cloud and metaverse technologies, and the importance of user experience design and security in platform engineering. Join us as we explore the future of engineering platforms and the strategies Ascendion employs to stay ahead in this dynamic landscape

Amit: What are some common challenges enterprises face in building and upgrading engineering platforms? What should enterprises consider while upgrading their engineering platforms in 2024?

Krishnendu: It has always remained a challenge to strike a balance between engineering excellence, the allocated budget, and target timelines in any large platform engineering endeavor and it remains one of the major points of contention. Additionally, with the level of advancement we are experiencing in the fields of AI and quantum computing, it has become extremely challenging to build a secured platform capable of protecting user data.

A frugal approach, where a lot of care has been taken towards measuring how much engineering is needed along with being very mindful of the business needs, can go a long way. Optimizing the solution for items like cloud economics, SecOps and automation along with the right technology selection can significantly help. GenAI enablement during solutioning, as well as implementation, can be a game changer in this context.

Amit: How platform engineering is beneficial for Gen AI to automate repetitive coding tasks, suggest improvements to existing code, and even generate new code snippets based on developer intent?

Krishnendu: It's revolutionary, to say the least, code generation and optimization is one of the primary areas where GenAI is getting used significantly. It can produce code in almost all the known languages with varied degrees of accuracy depending on the problem. The conversational GenAI tools and GenAI-enabled IDE plugins can make this very effective for the developers. The critical part is that the developer needs to be equipped with the right system knowledge on the ground as well as command over the technology to reap the benefits.

> “A frugal approach, where a lot of care has been taken towards measuring how much engineering is needed along with being very mindful of the business needs, can go a long way.”

Amit: Cloud and Metaverse are shaping the digital landscape. How does Ascendion incorporate these technologies into its platform engineering solutions, and what advantages do they offer in terms of user experience, data insights, and practical applications?

Krishnendu: It's safe to say that cloud engineering has become one of the de-facto technologies for almost everything in software engineering, and it has reached the position of a fully emerged technology and no longer remains a niche. Ascendion embraces this omnipresence of cloud technologies with dedicated COEs (Centers of Excellence), for all the premier cloud technologies which helps to find the right solution for a client problem. We also have a dedicated cloud economics COE backed by a set of powerful homegrown tools to enable the optimization of cloud costs.

We fully understand the power of Metaverse technologies and leverages the use of case-based implementations and frameworks to solve any client problem in this area. Along with providing the right solution around Metaverse technologies, Ascendion COEs take extra care in finding the suitability of Metaverse technologies for a given solution as this tech is going through the hype phase in the industry.

Amit: User experience is pivotal in platform adoption. How does Ascendion prioritize user experience design in platform engineering, and what strategies are employed to ensure intuitive and engaging interfaces for end-users?

Krishnendu: Dedicated COE, a very large library of pre-built designs that keep getting refreshed based on industry best practices and Ascendion's own experiences interacting with the clients, special focus on accessibility and inclusive UI designs – are our ways of offering user experience solutions. A lot of effort goes into striking the right synergy between user experience designing and then backing it by optimum UI technology that is the best fit for the job. The usage of GenAI in creating rapid prototypes and rich UX components is another area where we have put a lot of focus around.

Amit: Building scalable platforms requires a balance between flexibility and standardization. How can enterprises strike this balance to create platforms that are adaptable to unique client needs while maintaining a standardized and efficient engineering approach?

Krishnendu: Creating high-quality and independently scalable components, with an API-first approach, would be the way to go. This enables the implementation teams to rewire the orchestration to meet various customer needs with relative ease. As a technology, containerization has reached the next level of maturity, and this provides a lot of benefits in creating a hyper-flexible application consisting of individually engineered components working together to achieve a common goal. The component-ization of software solutions lets teams with different skill sets focus on their part of the solution bringing in quality and an API-based integration provides flexibility.

Amit: Security is paramount in digital innovation. How does Ascendion approach security considerations in platform engineering, and what best practices should enterprises adopt to safeguard their platforms and user data?

Krishnendu: Ascendion believes in embedding security in all aspects of software engineering rather than keeping it as a separate exercise. Left shifting of security via automation and DevSecOps engineering is the single most important item for making the application security practices sustainable – this enables bringing in the security culture from the very first day and standardizing the security practices across the organization.

Amit: Could you elaborate on how enterprises can effectively implement adaptive development workflows, and what advantages these workflows bring to the software and tech development process?

Krishnendu: Adaptive development workflows help an implementation team prepare for continuous changes and pivot based on real user feedback. This could be extremely helpful in navigating through all the unavoidable changes that the industries are going through. To have an effective adaptive software development methodology, deep user interactions are a must – a feasible way to ensure this would be needed. Adaptive development methodology depends on extensive testing at all stages; hence an integrated development, QE, and DevOps team and sufficient automation are critical for the success of such a model.

Amit: Success metrics are vital. How should organizations measure the success of their platform engineering projects, and what key performance indicators (KPIs) are essential for enterprises to monitor when evaluating the success of their platform development initiatives?

Krishnendu: KPIs play an extremely vital role in making sure any platform engineering program follows the right trajectory and allows all the stakeholders to take objective decisions on whether any course correction is needed. By the inherent nature of the business – some of the KPIs become more important than others and here, the expertise of the consultants plays a big role. In general, all the KPIs that measure security vulnerabilities, quality of the deliverables, and compliance with the timelines give the best insight into the health of the program.

Amit: What is your outlook for the engineering platforms space over the next 3-4 years?

Krishnendu: Platform engineering will remain one of the key drivers of organizational transformations and will embrace newer technologies more deeply. GenAI, with all its potential, is poised to become one of the most important platform engineering tools. GenAI-infused solutions will become more and more commonplace and it will contribute towards improving quality and reducing the implementation time of the platform engineering projects. Other technologies like blockchain and metaverse will also have their niche based on the business use case. Security and performance, which have remained important aspects throughout, will continue to do so but will be aided by new-age technologies.

Intel Unveils New AI Initiatives to Propel Innovation in PC Acceleration

AI PC Acceleration Program
Leadership in the Age of AI Software
intel

Intel Corporation has announced the launch of two new initiatives within its AI PC Acceleration Program, aimed at optimizing and maximizing AI capabilities across more than 100 million Intel-based AI PCs by 2025. These initiatives include the AI PC Developer Program and the inclusion of independent hardware vendors (IHVs) in the program, marking significant milestones in Intel's efforts to foster a thriving ecosystem for AI software and hardware.

The AI PC Developer Program targets software developers and independent software vendors (ISVs), providing them with tools, workflows, AI deployment frameworks, and developer kits tailored to facilitate the adoption of new AI technologies at scale. By offering access to the latest Intel hardware featuring the Intel® Core™ Ultra processor, this program aims to streamline the developer experience and accelerate the integration of AI capabilities into applications.

Furthermore, Intel has expanded its collaboration with IHVs by inviting them to participate in the AI PC Acceleration Program. IHVs joining this initiative gain access to Intel's Open Labs, where they receive technical support and co-engineering assistance to optimize their hardware solutions for Intel AI PCs. Additionally, qualified IHV partners can leverage reference hardware provided by Intel to test and optimize their technology, ensuring efficient performance upon launch.

Matt King, Senior Director of Client Hardware Ecosystem at Intel, emphasized the company's commitment to scaling innovative hardware and software solutions through its broad ecosystem of partners. Intel aims to empower developers and IHVs to elevate the AI PC experience and drive advancements in AI technology.

The significance of these programs lies in the transformative potential of AI, which is poised to revolutionize various aspects of daily life. With optimized software and hardware powered by Intel's leading-edge platform, users can harness the benefits of AI across diverse applications. By collaborating with a wide ecosystem of partners, Intel seeks to enhance performance, productivity, innovation, and creativity in the AI PC era.

Through these initiatives, Intel offers developers improved compatibility, performance optimization, and expanded market opportunities, fostering a conducive environment for AI innovation. The company's extensive range of AI toolkits and forthcoming AI-accelerated features underscores its commitment to driving advancements in AI technology and empowering developers worldwide.

Vertiv Becomes a Member of the NVIDIA Partner Network

Vertiv, a renowned global provider of critical infrastructure and continuity solutions, has recently joined the NVIDIA Partner Network (NPN) as a Solution Advisor and consultant partner. This collaboration aims to enhance the support for the adoption of accelerated computing and AI workloads by leveraging Vertiv's expertise in high-density power and cooling infrastructure.

As part of the NVIDIA Partner Network, Vertiv will offer its full range of power and cooling solutions to address the unique infrastructure challenges associated with accelerated computing. This partnership provides access to various benefits, including technical support, training, and collaboration opportunities, enabling partners to deliver innovative solutions to their clients worldwide.

Giordano (Gio) Albertazzi, CEO at Vertiv, highlighted the long-standing collaboration between Vertiv and NVIDIA in research, development, and engineering, resulting in innovative products and solutions supporting the global deployment of NVIDIA technologies. Together, they aim to develop state-of-the-art liquid cooling solutions for next-generation NVIDIA accelerated data centers powered by GB200 NVL72 systems.

Vertiv's high-density power and cooling solutions are tailored to support the next generation of GPUs, ensuring safe operation, optimal performance, and high availability for compute-intensive AI workloads. The portfolio includes liquid cooling technologies such as Vertiv Liebert XDU coolant distribution units, Vertiv™ Liebert® XDM split indoor chillers, and Vertiv Liebert DCD rear-door heat exchangers, catering to various application requirements. Additionally, the Vertiv Geist rack power distribution units (PDUs) family has been expanded to accommodate higher power draw within the rack, optimizing efficiency while minimizing footprint.

Brother International India Introduces Innovative Connectable Label Printer for B2B Sectors

ALOK NIGAM,
Managing Director,
Brother International India

Brother International (India) Pvt Ltd, a renowned provider of labeling solutions for corporate and B2B sectors, has launched a cutting-edge range of IoT-enabled connectable label printers tailored to meet the needs of various industries including manufacturing, logistics, pharmaceuticals, and hospitality. These connected labeling solutions leverage IoT integration to enhance efficiency and productivity in the modern workplace.

The new range of label printers includes handheld, desktop, and professional label printers, catering to the diverse labeling requirements of organizations. Alongside the IoT-enabled printers, Brother India also offers professional labeling and mobile printing solutions, enabling organizations to streamline asset-tracking processes while reducing costs associated with label making and reprinting.

With over three decades of expertise in labeling technology, Brother International India continues to lead the industry with its commitment to quality, reliability, and cost-effectiveness. The company's offerings are not only globally renowned for their dependability but also for their smart features, aimed at enhancing wireless connectivity and mobile productivity.

Alok Nigam, Managing Director at Brother International India, anticipates a significant surge in label printer sales in India, driven by the expanding manufacturing sector and the growing labeling needs across various industries such as packaging, transportation, and logistics.

Brother's label printers are designed to withstand high-volume printing demands while incorporating innovative features and connectivity options to streamline labeling processes. They offer long-lasting labels, enhanced productivity with built-in labeling templates, and seamless printing through various connectivity options including Wi-Fi and smart device connectivity.

The advanced laminated labels provided with Brother's label printers are durable and resistant to abrasions, water, spills, heat, and harsh environments, ensuring longevity and legibility over time. Additionally, Brother offers a wide range of specialty supplies such as flexible ID tapes, self-laminating tapes, flag tapes, and heat shrink tubes to cater to specific labeling requirements.

To further facilitate the deployment of smart labeling systems, Brother India offers industry-specific solutions customized to meet the labeling needs of manufacturing, warehouse and logistics, electrical and automation, telecom, healthcare and laboratories, hospitality and food production, packaging, and general business applications.

Implications of China's New IT Guidelines for Intel, AMD, and Microsoft: What You Need to Know

According to a report by the Financial Times, China has implemented guidelines aimed at phasing out the use of U.S. microprocessors, specifically those from Intel and AMD, in government computers and servers. The procurement guidelines also advocate for reducing reliance on Microsoft's Windows operating system and foreign-made database software, in favor of domestic alternatives. Government agencies at or above the township level are instructed to prioritize "safe and reliable" processors and operating systems in their procurement processes.

In late December, China's industry ministry released a statement featuring three separate lists of CPUs, operating systems, and centralized databases considered "safe and reliable" for three years. Notably, all options listed were from Chinese companies, as confirmed by checks from Reuters.

Intel and AMD have not yet responded to requests for comment from Reuters. The U.S. government has been actively working to boost domestic semiconductor production and reduce dependence on countries like China and Taiwan, notably through initiatives like the Biden administration's 2022 CHIPS and Science Act. This legislation aims to strengthen the U.S. semiconductor industry by providing financial assistance for domestic chip production, including subsidies for the manufacturing of advanced chips.

AWS and EkStep Partner to Drive Innovation in Digital Public Infrastructure

Amazon Web Services (AWS) India Private Limited has joined forces with EkStep Foundation to establish a Joint Innovation Center (JIC) in India. This collaboration aims to facilitate the development of innovative digital solutions for public service delivery, with a focus on creating digital public goods (DPGs) and digital public infrastructures (DPIs). The JIC, built upon Amazon's culture of innovation, aims to bring together stakeholders across the digital value chain to drive social transformation on a large scale.

The Nasscom-Arthur D. Little report highlights the potential economic value addition from DPIs to India's GDP, indicating significant growth opportunities. The JIC will serve as a platform for key stakeholders, including DPG/DPI owners, developers, enablers like startups and system integrators, and adopters/implementers such as governments and private sector entities, to collaborate and develop solutions for various sectors like education, agriculture, finance, healthcare, and climate change.

The focus of the JIC will be on supporting startups, ISVs, and SIs in leveraging technologies such as cloud computing and artificial intelligence to innovate and enhance existing DPGs and DPIs. These solutions will be made easily accessible through the AWS Partner Network, facilitating one-click deployment and global distribution through platforms like AWS Marketplace.

Shalini Kapoor, Director and Chief Technologist at AWS India Private Limited, highlighted the importance of leveraging cloud computing and open-source solutions to accelerate public service transformation. Shankar Maruwada, Co-founder and CEO of EkStep Foundation, emphasized the collaborative effort required to build and implement digital solutions at scale, expressing excitement about the partnership with AWS to drive inclusive innovation in India's Digital Public Infrastructure.

The establishment of the JIC signifies a significant step towards fostering innovation and driving scalable impact in India. Examples of open-source digital solutions like MOSIP and Namma Yatri demonstrate the potential for leveraging technology to benefit citizens at scale, further underscoring the importance of collaborative efforts in advancing India's digital landscape.

JK Tech Collaborates with Google Cloud to Expedite Digital Innovation and Enhance Gen AI Capabilities

JK Tech has partnered with Google Cloud to expedite digital innovation and enhance its Gen AI capabilities. With a strong contingent of GCP-certified professionals, JK Tech aims to enhance its services in Application Development, Cloud Migration, Data Management, and Machine Learning across the US and the UK. This collaboration seeks to drive advancements in cloud capabilities, leveraging Gen AI to fully utilize Google Cloud technologies. JK Tech's Gen AI Accelerator- JIVA leads the charge in innovating enterprise data solutions, reflecting the organization's commitment to integrating Google Cloud capabilities into all its offerings.

JK Tech's expertise lies in three primary domains: Gen AI and Analytics, industry-specific knowledge in Retail & CPG, and insurance sectors, and strategic partnership with Google Cloud. By broadening its service portfolio, JK Tech ensures efficient and scalable deployment of cloud solutions, enabling agile responses to diverse customer requirements.

Vedang Singhania, Head of Marketing and Alliances at JK Tech, underscores the significance of this collaboration, stating that it underscores the company's dedication to providing cutting-edge technology solutions for business growth and innovation. He emphasizes the synergy between Google Cloud's infrastructure and JK Tech's domain knowledge, aiming to expedite clients' digital transformation journeys. Additionally, JK Tech plans to establish a dedicated Strategic Business Unit (SBU) for Google Cloud services, focusing on specialization and customized solutions for clients. The company will also participate in Google Next'24 event to further its engagement with Google Cloud services.

Palo Alto Networks' Unit 42 Study: Ransomware Hits Indian Manufacturing Sector Hardest

Palo Alto Networks' Unit 42 recently published its Ransomware Retrospective 2024: Unit 42 Leak Site Analysis and Incident Response report. This report delved into 3,998 leak site posts from various ransomware groups, which are platforms where stolen data is publicly disclosed to coerce victims into paying ransom.

Key findings of the study reveal a 49% year-over-year increase in multi-extortion ransomware attacks globally from 2022 to 2023. Notably, in India, the manufacturing sector stood out as the primary target for ransomware extortion in 2023. Among the 3,998 leak site posts globally, LockBit ransomware was the most active, affecting 928 organizations, constituting 23% of the total. LockBit also remained highly active in APAC and India. Additionally, 25 new ransomware leak sites emerged in 2023, with Akira being the most prominent.

Anil Valluri, Managing Director and Vice President for India and SAARC at Palo Alto Networks emphasized the concerning trend of the manufacturing sector being vulnerable to ransomware attacks due to limited visibility into operational technology systems, inadequate network monitoring, and suboptimal cyber-hygiene practices. Valluri stressed the need for organizations to adopt a Zero Trust network architecture to enhance security layers.

Valluri further noted the cybersecurity challenges in India, with organizations grappling with a mix of modern and legacy systems, leaving significant security gaps. He advocated for integrated cybersecurity solutions to mitigate these challenges effectively.

The report highlighted a significant increase in ransomware leak site posts compared to the previous year, attributed to zero-day exploits targeting vulnerabilities in systems like MOVEit Transfer SQL Injection and GoAnywhere MFT.

Unit 42's analysis of over 600 incidents from 250 organizations for the 2024 Incident Response Report revealed a decline in phishing as an initial access tactic, replaced by the exploitation of software and API vulnerabilities. Threat actors were found to indiscriminately gather data in 93% of incidents, indicating a shift towards broad data collection rather than targeting specific datasets.

Huzefa Motiwala, Director of Systems Engineering for India and SAARC acknowledged the alarming rise in ransomware incidents but noted positive shifts in organizations' response strategies. Despite increased ransom demands, median payouts decreased, suggesting organizations' readiness to engage Incident Response teams, deterring threat actors.

Microsoft Appoints Co-Founder of DeepMind to Head New AI Division

Microsoft has enlisted the expertise of Mustafa Suleyman, co-founder of DeepMind, to lead its newly established consumer AI division, overseeing products such as Copilot, Bing, and Edge. Suleyman, along with key personnel from his startup Inflection AI, including Karen Simonyan as chief scientist, will steer this venture. As CEO of Microsoft AI, Suleyman will report directly to Satya Nadella, the company's CEO, with Nadella expressing optimism about the accelerated progress this infusion of talent will bring.

Suleyman's journey in the AI domain includes co-founding DeepMind in 2010, later acquired by Google in 2014. Following a merger with Google Brain in 2023, Suleyman moved on to found Inflection AI after a stint at Google. Notably, Inflection AI, supported by Microsoft and Nvidia, developed Pi, a conversational AI chatbot. Amidst plans to license its technology to Microsoft and pivot towards serving enterprise clients, the consolidation within Microsoft reflects its commitment to maintaining a competitive edge against Google, which is reportedly exploring integration of its Gemini AI model into Apple's iPhone.

Nadella praised Suleyman's track record as a visionary leader and emphasized Microsoft's dedication to harness AI for global benefit while ensuring safety and responsibility.

Research Shows Less Than 20% of Decision-Makers Prioritize Critical Thinking Skills, Potentially Stalling AI Advancements

Research conducted by Alteryx suggests that the current upskilling priorities of decision-makers may hinder the progress of artificial intelligence (AI) in India. Less than one-fifth of business leaders in the country prioritize critical thinking skills, despite concerns about the accuracy of AI-generated responses.

The findings, released by Alteryx, reveal a growing need for a shift in workforce skills as India prepares for an AI-driven labor market. However, there seems to be a disconnect between the skills currently emphasized in hiring processes and those required to fully leverage AI's potential benefits.

New roles are expected to emerge as organizations adapt to the changing landscape, with many anticipating the need for a Chief AI Officer to oversee holistic AI strategies. Additionally, roles such as AI applications engineers, AI/ML engineers, and AI research scientists are identified as urgent hiring priorities.

As the future of work evolves, certain technical skills are projected to become obsolete, including database administration and repetitive coding. However, there is optimism about the availability of advanced tech talent, driven by the increasing accessibility of generative AI technology.

Despite the increasing importance of soft skills in collaborating with AI systems, the research highlights a continued emphasis on recruiting for roles with technical expertise. This raises questions about whether organizations are prioritizing the right skills for the evolving landscape.

While creativity and critical thinking are recognized as essential skills in an AI-driven world, they are not consistently prioritized in upskilling efforts. Instead, there is a focus on hard skills such as AI expertise and data analysis.

Libby Duane-Adams, Chief Advocacy Officer at Alteryx, emphasizes the importance of building a workforce equipped with creative problem-solving skills and data literacy to harness the potential of AI responsibly. Souma Das, Managing Director for India Sub-continent at Alteryx, underscores the need for continuous learning and adaptability to ensure that organizations in India can navigate the evolving AI landscape effectively while prioritizing societal well-being alongside economic development.

Statiq and GLIDA Collaborate to Extend Electric Vehicle Charging Network Across India

Statiq and GLIDA have announced a strategic partnership to enhance the electric vehicle (EV) charging infrastructure in India. Under this agreement, the entire GLIDA charging network will be integrated into the Statiq App, allowing users to easily locate and utilize any public charger within the GLIDA network. This initiative aims to promote interoperability between Statiq and GLIDA charging stations, streamlining the charging process for EV users and reducing the need for multiple applications. Additionally, GLIDA's charging solutions will continue to be accessible through its app and the Charge-Thru web link, providing users with diverse options. Raghav Arora, Co-founder & CTO of Statiq, expressed enthusiasm for the collaboration, emphasizing its role in accelerating the transition to electric mobility in India. Awadhesh Kumar Jha, Executive Director of GLIDA, highlighted the partnership's importance in advancing EV charging infrastructure and promoting green mobility solutions. With over 850 GLIDA charging points now accessible through the Statiq app, this collaboration aims to support India's shift towards sustainable transportation by enhancing the availability and convenience of EV charging solutions.

Channel Point

Dear Readers,

As technology continues to evolve at an unprecedented pace, the intersection of artificial intelligence and cybersecurity has become a focal point of innovation and transformation.

In this issue, I am thrilled to present our cover story on "GenAI Leading Revolutionary Shifts in the Cybersecurity Landscape." In today's rapidly evolving digital world, the role of artificial intelligence in cybersecurity has become increasingly pivotal. This issue delves into the groundbreaking advancements in GenAI and its profound impact on reshaping the cybersecurity landscape. From proactive threat detection to adaptive defense mechanisms, GenAI is at the forefront of safeguarding digital ecosystems against ever-evolving cyber threats.

We have meticulously curated insights from industry experts, thought leaders, and innovators to provide you with a comprehensive understanding of how GenAI is revolutionizing cybersecurity practices. From threat detection to predictive analysis, GenAI is at the forefront of safeguarding our digital infrastructure.

I invite you to immerse yourself in the compelling narratives, expert analyses, and real-world applications featured in this issue. Together, let's explore the transformative potential of GenAI in fortifying our cybersecurity defenses and staying ahead of emerging threats.

Thank you for being part of our journey in unraveling the intricate web of GenAI and its profound implications for cybersecurity.

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

TECHPLUS MEDIA™

EDITOR: KALPANA SINGHAL
CONTENT HEAD: Amit Singh
CONSULTING EDITOR: Rajneesh De
NEWS ANALYST: Ishita Gupta
CORRESPONDENT: Bhawna Thapliyal
NEWS REPORTER: Anindita Majumder, Urmi Saha

INTEGRATED MARKETING COMMUNICATION:
Arunim Agrawal, Mamta Kapoor

ASSOCIATE ANALYST
Shaithra S

SALES:
Anushikha Singh | Pratap Jana

PRODUCTION HEAD:
Aji Kumar

WEBSITE:
Gaurav Rana

PROMOTION:
Amit Pandey, Nikita Gurung

CIRCULATION:
Pratap Ram

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: 91-8178321837 | **Mumbai:**91-98997 01316
Kolkata & Guwahati: 91-9331072026
Bangalore: 91-8851119532

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

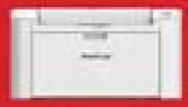
Vibrant 18 Series

Elite Series

PT-L280 Series

PT-L380 Series

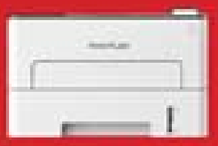
PT-B680 Series



Simple&Smart Series

Simple&Smart Series

Mighty Series



45 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

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**

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