TechGuru@25
Organizations must outsource tasks strategically based on project... Pg23

Interview: Vivek Srivastava, Fortinet
"Human Firewall" is the first step towards organizational... Pg 31

Volume 13
Issue 01
Apr-June 2024
₹150

25th ANNIVERSARY
CIO&LEADER
TRACK TECHNOLOGY • BUILD BUSINESS • SHAPE SELF

7 Strategic Steps to Outsmart Modern Cybersecurity Threats

Pg. 15

A 9.9 Group Publication

LAUNCHING

digit SQUAD

Here is your chance to become a Digit certified tech influencer

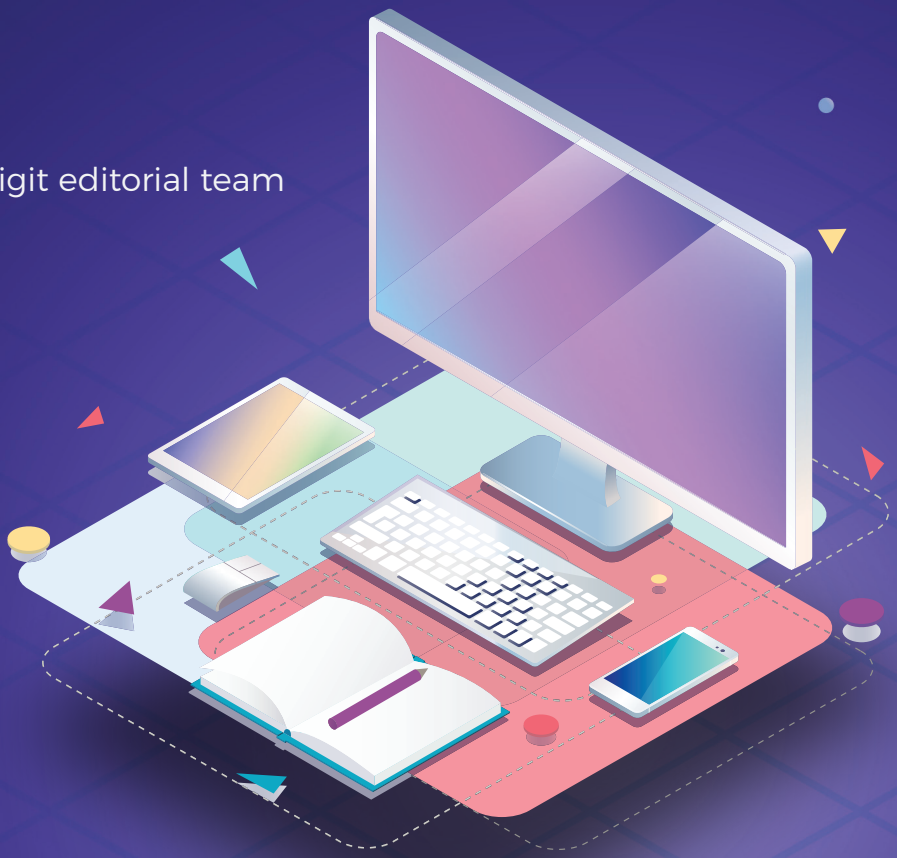
Benefits of Digit Squad Member

Launch your own tech channel on Digit.in

Become a Digit Certified tech influencer

Engage with digit editorial team

Make money



Apply now by scanning the QR code

www.digit.in/digit-squad/apply.html

Human error and AI: The twin challenges of modern cybersecurity

At a recent conference, the CIO of one of India's leading banks made an honest confession, emphasizing the gravity of escalating cybersecurity concerns in the AI age. He pointed out that businesses often downplay these issues in public—a fact that should not be taken lightly. This understatement could be due to the fear of losing customer trust, attracting regulatory scrutiny, or facing unnecessary bottlenecks in their AI innovations.

Despite enterprises' efforts to prioritize cybersecurity investments, human weakness remains one of the most persistent challenges. Numerous industry surveys over the past few years reveal that human errors are responsible for over 70% of organizational breaches. This stark reality highlights the need for technology leaders to focus on conducting comprehensive user training programs and enhancing capabilities for monitoring and controlling sensitive content.

In today's world, data is considered as good as gold for organizations, and their success, innovation, and growth depend heavily on the security of their data protection strategies. However, executing their long-term and short-term goals remains challenging, especially when there is a lack of talent, resources, and huge disparate systems.

In an era of LLMs and Generative AI, the problems around cybersecurity will only be compounded, underscoring the urgent need for action. Cybercriminals can inject malicious data into the data that an organization's employees continuously feed into public and private LLMs to bias the model's output, compromising the systems that rely on these models. If training data is not properly sanitized, information leakage and data poisoning can aggravate the situation.

It is not that CIOs are unaware of these issues. However, as an industry, we must unite and collaboratively identify the best approaches to mitigate these threats and ensure they do not impede innovation. My colleague Praneeta, in her first cover story, engaged with many of you to grasp the gravity of the situation and the necessary steps to outsmart modern cybersecurity threats. While there is no foolproof strategy for complete security, it is crucial to focus on the most effective steps to remain vigilant and strengthen our approach to cybersecurity. ■

In an era of LLMs and Generative AI, the problems around cybersecurity will only be compounded, underscoring the urgent need for action.

JATINDER SINGH
Executive Editor
jatinder.singh@9dot9.in

CONTENT APR-JUNE 2024

Cover Design by:
Shokeen Saifi

Please Recycle This Magazine And Remove Inserts Before Recycling

CIO&LEADER

www.cioandleader.com

MANAGEMENT
Managing Director: **Dr Pramath Raj Sinha**
Printer & Publisher / Editorial Director: **Vikas Gupta**
Executive Director - B2B Tech:
Sachin Nandkishor Mhashilkar (+91 99203 48755)

EDITORIAL
Group Editor - 9.9 Group: **R Giridhar**
Executive Editor - B2B Tech: **Jatinder Singh**
Correspondent - B2B Tech: **Praneeta**

DESIGN
Creative Director: **Shokeen Saifi**
Sr. Designer: **Vipin Rai**

SALES & MARKETING
Director - B2B Tech:
Vandana Chauhan (+91 99589 84581)
Sales Director - B2B Tech:
BN Raghavendra (+91 98453 81683)
National Sales Head (CSO Forum):
Vaibhav Kumar (+91 97176 74460)
Senior Manager Brand & Strategy: **Pratika Barua**
Brand Manager: **Sheena Dawar**

COMMUNITY ENGAGEMENT & DEVELOPMENT
Head - Projects:
Dipanjan Mitra
Senior Manager - Community Development:
Neelam Adhangale
Assistant Manager Community Development:
Vaishali Banerjee
Assistant Manager Community Development:
Snehal Thosar
Assistant Manager Community Development:
Shabana Shariff
Assistant Manager Community Development:
Reetu Pande
Senior Executive Audience Development:
Merly Davidson

OPERATIONS
Head - Digital & Event Operations: **Naveen Kumar**
Head - Digital Operations: **Atul Kumar Pandey**
Senior Executive Commercial: **Nitika Karyet**

PRODUCTION & LOGISTICS
Senior Manager - Operations: **Mahendra Kumar Singh**

OFFICE ADDRESS
9.9 Group Pvt. Ltd.
(Formerly known as Nine Dot Nine Mediaworx Pvt. Ltd.)
121, Patparganj, Mayur Vihar, Phase - I
Near Mandir Masjid, Delhi-110091
Published, Printed and Owned by 9.9 Group Pvt. Ltd.
(Formerly known as Nine Dot Nine Mediaworx Pvt. Ltd.)
Published and printed on their behalf by
Vikas Gupta. Published at 121, Patparganj,
Mayur Vihar, Phase - I, Near Mandir Masjid, Delhi-110091,
India. Printed at Tara Art Printers Pvt Ltd., A-46-47,
Sector-5, NOIDA (U.P.) 201301.
Editor: **Vikas Gupta**

99GROUP

Cybersecurity challenges and how enterprises can fight the ever evolving threat

Cyber attacks are on the rise globally, with rise significant rise in the first quarter of 2024, almost 5% more than last time, marking an urgent need for updated ways to deal with the evolving challenges

By **Praneeta** | praneeta@9dot9.in

Check Point released its cybersecurity report for the first quarter of 2024. The report shed light on the evolving cybersecurity challenges that emerged in Q4 2024 and also discussed how far the enterprises are from solving AI-powered cybersecurity challenges.

According to Check Point, a software providing company, there was a significant rise in cyber attacks, with organizations facing an average of 1308 attacks per week. This is 5% higher than the same period last year and 28% higher than the previous quarter. This increase from Q4 2023 showcases the rise in attacks and also highlights the ever-evolving landscape of cyber threat and security.

Omer Dembinsky, Data Research Group Manager at Check Point Software, said, "As we witness the dynamic landscape of cyber threats in Q1 2024, it is clear that our approach to cybersecurity needs to be equally dynamic and proactive. The significant rise and volume of cyber attacks in regions like Europe, Africa, and particularly in North America, where 59% of the known ransomware attacks were concentrated, signals an urgent need for enhanced vigilance and robust cybersecurity measures."

"The startling 96% surge in ransomware attacks YOY on the Manufacturing sector and the unprecedented 177% increase YOY in the Communications sector are indicative of the vulnerabilities introduced by rapid digital transformation and the critical nature of these industries. These figures are not just statistics; they represent an urgent call for organizations across all sectors to bolster their defenses and prioritize cybersecurity, underscoring the need for adaptive, AI-powered defense strategies," he added.

Industry-wise data

According to the report, the Education sector experienced the most attacks, with an average of 2454 attacks per organization weekly, followed by the Government/Military sector with 1692 attacks per week and the Healthcare sector with 1605 attacks per organization.

However, what's concerning is the big jump in cyber attacks on hardware vendors. These attacks increased by 37% compared to last year. It shows that cyber criminals are targeting these companies more because they rely heavily on hardware for things like smart devices and the Internet of Things (IoT).

IBM X-Force Exchange, a cybersecurity threat intelligence team and platform operated by IBM, in its Threat Intelligence Index 2024, names Manufacturing as the top attacked industry in 2023 for the third year in a row, representing 25.7% of incidents within the top 10 industries year over year.

The finance and insurance industry was in second place, representing 18.2% of incidents. The share of attacks across the energy, retail and wholesale, healthcare, transportation, and arts, entertainment, and recreation sectors increased year over year.

The Communications sector saw a significant increase in attacks, likely due to rapid digital trans-

SHARE OF ATTACKS BY INDUSTRY 2019-2023

Industry	2023	2022	2021	2020	2019
Manufacturing	25.7%	24.8	23.2	17.7	8
Finance and insurance	18.2%	18.9	22.4	23	17
Professional, business and consumer services	15.4%	14.6	12.7	8.7	10
Energy	11.1%	10.7	8.2	11.1	6
Retail and wholesale	10.7%	8.7	7.3	10.2	16
Healthcare	6.3%	5.8	5.1	6.6	3
Government	4.3%	4.8	2.8	7.9	8
Transportation	4.3%	3.9	4	5.1	13
Education	2.8%	7.3	2.8	4	8
Media and telecommunications	1.2%	0.5	2.5	5.7	10

SOURCE: IBM X-FORCE THREAT INTELLIGENCE INDEX 2024

Region	Percent out of Published Ransomware Attacks	YoY Change in Amount of Published Attacks
North America	59%	+16%
Europe	24%	+64%
APAC	12%	-13%
Latin America	4%	+14%
Africa	1%	+18%

SOURCE: CHECKPOINT REPORT

formation and the integration of technologies like 5G and IoT.

Regional trends

According to the IBM XForce report in 2021 and 2022, the Asia-Pacific region was hit the hardest by cyber incidents, followed by Europe in second place. In 2023 Europe became the most affected region, making up 32% of incidents responded to by X-Force. North America accounted for 26% of incidents, Asia-Pacific for 23%, Latin America for 12%, and the Middle East and Africa for 7%.

However, in the first quarter of 2024, North America faced the highest impact from ransomware attacks, with 59% out of nearly 1000 reported attacks, according to the Check Point report. Europe followed with 24%, and APAC with 12%. Europe experienced the largest increase in attacks compared to the same period in 2023, with a significant 64% rise.

This increase could be due to factors like increased digitization and regulatory environments that are making organizations more vulnerable. Meanwhile, North America saw a 16% increase, suggesting attackers continue to focus on this region.

These trends highlight the evolving cyber threat landscape and the need for robust cybersecurity measures to safeguard organizations and critical infrastructure.

What can enterprises do

Check Point suggests enterprises develop and adopt a multi-faceted approach to cybersecurity. Data backups, cyber awareness training, timely security patches, strong user authentication, and advanced anti-ransomware solutions are to be made a regular practice.

"Proactive engagement with AI-powered defenses can significantly bolster an organization's resilience against these threats," the report adds.

IBM states that to minimize the risk of credential harvesting attacks, enterprises should deploy Endpoint Detection and Response (EDR) tools across all servers and workstations in their environment. These tools help detect malware, including infostealers and ransomware and can identify abnormal behavior, such as data exfiltration or unauthorized account creation. They also suggest to consider leveraging experts to establish and operationalize threat hunting within your environment.

If resources are limited, consider using AI to manage up to 85% of alerts, allowing for 24/7 threat detection and response services. Additionally, it utilizes threat intelligence to identify opportunities for mitigating new threats. Strengthen credential management practices by implementing Multi-Factor Authentication (MFA) and robust password policies, including passkeys. Employ hardened system configurations to make accessing credentials more challenging.

Credential harvesting attacks often occur through phishing and watering hole attacks. Regularly educate employees on updated phishing techniques and scrutinize all third-party traffic. Treat third-party traffic as untrusted until verified. Watering hole attackers may exploit legitimate resources to deliver malware.

To reduce the cybersecurity blast radius, consider the potential impact of an incident on users, devices, or data. Implement solutions to minimize damage in case of a security incident, mainly focusing on data security and identity management.

Conclusion

Cyber attacks are evolving rapidly, faster than enterprises can keep up. This is the right time to integrate AI and leverage AI-powered tools to counter the attacks and protect businesses and the people. Enterprises need to evolve with time and technology as well, using different methods and upskilling to help ward off the pesky attacks and malware. ■

90% of cybersecurity experts consider detecting insider attacks more challenging than external cyber attacks

The shift to remote work and the advent of new technologies add to the challenge, highlighting the gap in effective threat management strategies.

By **Nisha Sharma** | nisha.sharma@9dot9.in

The Securonix 2024 Insider Threat Report provides an insightful analysis of the escalating challenges of insider threats in cybersecurity. It delves into the increased frequency of these threats, remote work's impact, and emerging technologies' influence. This introduction sets the stage for a deeper examination of how these evolving factors shape the cybersecurity landscape.

Increased frequency of insider attacks

The report points to a significant increase in insider attacks, focusing on the escalating severity and frequency of these incidents. From 2019 to 2024, insider attacks surged from 66% to 76% of organizations, marking a striking escalation in identified insider threats. This trend is attributed to various factors, including economic uncertainties and technological advancements, making insider attacks more appealing and accessible.

Malicious insiders and advanced techniques

There's a growing concern over insiders using advanced techniques like ransomware, highlighting insider threats shifting from mere data theft to more destructive tactics. This evolution challenges traditional security measures, which may need to be equipped to handle such sophisticated attacks.

Just 29% of respondents believe they possess the necessary tools to combat insider threats, revealing a significant short-fall in security capabilities within many organizations.

Impact of remote work and emerging technologies

The shift to remote and hybrid work environments is a critical factor exacerbating insider threats. 70% of those surveyed highlight concerns about insider risks in hybrid work scenarios, emphasizing the difficulty in securing distributed environments. 75% reported that emerging technologies like AI and Quantum Computing create new vulnerabilities and attack vectors that organizations must be aware of and prepared for.

Insider threat programs: effectiveness and challenges

The report evaluates current insider threat programs, noting their maturity and effectiveness disparity. While 66% of organizations acknowledge vulnerability to insider attacks, only 41% have partially implemented insider threat programs, highlighting a need for comprehensive monitoring and advanced threat management. Furthermore, just 29% of respondents believe they possess the necessary tools to combat insider threats, revealing a significant shortfall in security capabilities within many organizations. It also sheds light on the challenges organizations face in implementing these programs, such as budget constraints and lack of skilled personnel.

Varied approaches in user behavior monitoring

The survey indicates diverse strategies in user behavior monitoring for cybersecurity. 30% of organizations employ continuous automated monitoring, offering effective real-time surveillance. In contrast, 26% use incident-based tracking, a more reactive approach focusing on post-incident analysis. 20% maintain basic access logs, providing limited insights, while 15% conduct conditional monitoring in specific scenarios. Notably, 7% still need to implement such tracking. This underscores the need for continuous, proactive monitoring to enhance security against insider threats.

Conclusion

The Securonix 2024 Insider Threat Report conveys a clear message about the changing dynamics in cybersecurity. It reveals insider threats' growing complexity and frequency influenced by economic conditions and technological progress. The diverse approaches to user behavior monitoring, from continuous surveillance to essential log maintenance, show the varying readiness levels of organizations to tackle these threats. This situation underscores the need for improved, proactive security measures tailored to the current cyber threat landscape. ■

How firms are updating their AI models for enterprises

With the upgrade the Microsoft Copilot will be able to facilitate faster and more comprehensive answers, while also boost image generation to 100 per day

By **Praneeta** | praneeta@9dot9.in

Microsoft and Google have updated and relaunched their AI models with enhanced tools to enhance the productivity and time management for the enterprises.

Microsoft introduced Copilot for Microsoft 365 last year and recently upgraded It for its business users. The American technology company announced on its official website that it is officially upgrading its AI-powered Copilot assistant with GPT-4.

The announcement came as a part of another upgrade, including enhancing Copilot's image generation for enterprises. The Microsoft Designer's image generation feature is powered by the DALL-E 3 model and is set to undergo significant enhancement.

Microsoft will provide early access to the GPT-4 Turbo Model to business users. According to the firm, this model will include removing constraints on daily chat limits and conversation length, facilitating faster and more comprehensive responses.

For the image generation feature, Microsoft will offer an image generation boost to 100 per day, enabling the quick creation of custom images from prompts. It is to help businesses streamline workflows, reduce waiting times, and unleash newfound productivity potentials.

Microsoft's Work Trend Index Special Report, shows that 70% of Copilot users felt more productive, and 68% said it improved the quality of their work.

AI tools for businesses

According to Microsoft blog, Copilot is currently being used by different enterprises such as Accenture, Bayer, Dentsu Creative, Hargreaves Lansdown, EY Americas, and Wipro Limited. Businesses have adopted AI in their respective fields at different levels to save time, enhance productivity, and swift through research data to help organize and compile it for easy consumption.

In Microsoft's last Work Trend Index Special Report, the data shows that 70% of Copilot users felt more productive, and 68% said it improved the quality of their work. Overall, the report claimed that users were 29% faster in tasks like searching, writing, and summarizing.

As per the report, 64% of users felt that Copilot helped them spend less time processing mail, and 77% said that once they used it, they didn't want to give up. The report also showed how Copilot affected the different roles in an enterprise. Salespeople cited Copilot as helping them identify sales opportunities (75%) and compile marketing and sales data (74%).

"Customer service agents cited intelligently routing issues to appropriate agents (70%) and detecting trends across agent-customer interactions (68%). In finance, people cited simplifying financial reporting (73%) and validating data quality (72%)," the report added.

The Copilot for Microsoft 365 is priced at $30 per month for business users, while Google also launched its AI powered-tools for enterprise customers, priced $30 per month. The tools included "Duet AI in Workspace" to assist with writing, drafting emails, generating custom visuals, and more.

Learning from mistakes

Google on the other hand updated its AI model Gemini, announcing at the company's first annual cloud conference in Las Vegas, promoting it for enterprises. Thomas Kurian, Cloud Executive Officer at Google, said, "Enterprises have been piloting with us a number of scenarios with generative AI; now they're deploying them in production," as reported by Business Standard.

Though first introduced in February for the enterprises, Gemini was paused after the Google image generation mishap, which was addressed by Sundar Pichai, CEO of Google and Alphabet in a press release. The chatbot, when it was called Bard, also shared incorrect images of planet outside the solar system in a promotional video which caused its shares to fall by 9%, reported by Forbes.

Uber and Palo Alto Networks also utilize Google AI to solve their customer-related issues while also making work efficient.

Under the update, the business users will get Vids, a new AI powered Workspace app which will be released in June, while Meet will be able to transcribe in 52 new languages. A new AI security add-on was also introduced at the cost of $10 per month to identify, classify and protect sensitive files.

Google is pushing its AI platform towards enterprise and business use, trying to be at the forefront of the AI shift in the tech industry. Pichai claimed in the blog that "more than 60% of funded generative AI startups and nearly 90% of gen AI unicorns are Google Cloud customers."

AI companies like Anthropic, Al21 Labs, Contextual AI, Essential AI and Mistral AI are using Google infrastructure, as per Google. Google and Mercedes-Benz partnered to utilize Google's AI tools, including Vertex AI and Gemini, to enhance customer experience, efficient data analysis, and technology innovation.

Uber and Palo Alto Networks also utilize Google AI to solve their customer related issues while also making work efficient. Uber launched new tools to summarize customer communication while Palo Alto is using Gemini's cybersecurity capabilities.

The learning curve

According to Goldman Sachs GENAI can deliver a $7 Trillion boost in global GDP over the next 10 years. IDC estimates that India will be the third fastest AI-adopting country in Asia by 2026 after China and Australia.

Deepak Agarwal, Ex-Executive Director of Indian Oil Corporation shared tips for CIOs to get started using AI. He suggests getting the data house in order. Cloud skills are essential since most GENAI cases require massive data and computing capacity. Work Backwards... First, understand the customer challenge, get the ideal solution, and build the product that solves the challenge. Build responsible and sustainable solutions and select the right foundation model for the right use case, while starting small with PoV.

Shweta Srivastava, head of IT for Matix Fertilisers and Chemicals Ltd, describes the impact of LLMs, saying, "By integrating LLMs into our production and maintenance systems, we've been able to preempt equipment failures and significantly enhance our demand forecasting. This proactive approach reduces downtime and ensures we're operating at peak efficiency."

The race toward the AI launches and upgrades only highlights the need for caution and slow integration of AI models into businesses. CIOs can leverage these models and their AI-powered tools in their businesses to enhance customer services and provide security to the internal system. ■

CIO MOVEMENTS

Palanikumar Arumugam joins Hinduja Leyland Finance as CISO

Palanikumar Arumugam has joined Hinduja Leyland Finance as CISO. Before this, he was Vice President of Information Security at Equitas Small Finance Bank. He was earlier associated with Shiksha Financial Services, Veritas Finance, Imatics Technologies, Sobha Applied DSP, and Maxwell Industries.

Jeetesh Patel starts a new position as Senior Vice President of Technology at HDFC Bank Limited

Jeetesh Patel has started a new position as Senior Vice President of Technology at HDFC Bank. Before this, he was Vice President of Information Technology at the same company. He was earlier associated with HPE, Welspun Group, and Wipro.

Tirthankar Dutta starts a new position as Head Enterprise IT & Cybersecurity (CIO) at Disney Star

Tirthankar Dutta has started a new position as Head Enterprise IT & Cybersecurity (CIO) at Disney Star. Before this, he was CISO at the same company. He was associated with Forbes, Infoedge, Expedia, Religare, HCL Technologies and IBM earlier.

Dheeraj Sinha joins Sun Pharma as Group CIO

Dheeraj Sinha has joined Sun Pharma as Group CIO. Before this, He was EVP and Group CIO at JSW Group. He is a long-time NEXT100 jury member. He was earlier associated with Apollo Tyres, Infovergix, UMIT, and Xerox.

NEXT100 Winner Satadal Basu joins Aeon Credit India as Vice President-Head IT Planning and Development

NEXT100 2023 winner **Satadal Basu** has joined Aeon Credit India as VP- Head IT Planning and Development. Before this, he was the Lead Business Automation & Marketing Technology at Rustomjee. He was earlier associated with Tata Realty And Infrastructure Ltd, Tata Housing, and DLF.

Benjamin Ambrose starts a new position as CISO at National Payments Corporation Of India (NPCI)

Benjamin Ambrose has started a new position as Chief Information Security Officer at National Payments Corporation Of India (NPCI). Before this, he was a Senior Security Consultant at Amazon Web Services (AWS). He was earlier associated with CITI, Ciber Inc, and Wipro Technologies.

Mahesh Toshniwal Appointed as General Manager-Group Head of IT Operations at Jindal Steel & Power Ltd

Mahesh Toshniwal assumes the role of General Manager-Group Head of IT Operations at Jindal Steel & Power Ltd, bringing his extensive experience from STL Digital, Vedanta Limited, Sterlite Copper, and UltraTech Cement.

Vijay Balakrishnan Joins Godrej & Boyce as Chief Digital and Information Officer

Vijay Balakrishnan takes on the position of Chief Digital and Information Officer at Godrej & Boyce, leveraging his previous role as Senior Vice President and Chief Data & Analytics Officer at United Phosphorus Limited, along with experience at Michelin, GE, and Oracle.

Sudesh Sharma Assumes Role as Head of Information Technology at Panasonic India

Sudesh Sharma transitions to the position of Head of Information Technology at Panasonic India, following his tenure as Director Asia at Whirlpool Co India Limited and prior engagements with Bennett Coleman and Co. Ltd. (Times Group), HCL Technologies, Steria India, Xansa India, and SAP Labs.

Dheerendar Kumar Srivastav starts a new position as Vice President of Information Technology at Anand Rathi Global Finance Limited

Dheerendar Kumar Srivastav has started a new position as Vice President of Information Technology at Anand Rathi Global Finance Limited. Before this, he was General Manager - IT at Poonawalla Finance. He was earlier associated with Bajaj Capital Ltd.

Girish Kulkarni joins the International Institute of Information Technology, Bangalore as CISO

Girish Kulkarni has joined the International Institute of Information Technology, Bangalore as the Chief Information Security Officer (CISO). Before this role, he served as an Information Technology Specialist at NIMHANS. His previous experiences include positions at Chinmaya Mission Hospital, M/s SVPIMSR, HIMSS Asia Pacific India, Simplified Healthcare, Cytecare Cancer Hospitals, Takshasila Healthcare, Columbia Asia Hospitals, and Value Point Systems.

Ganesan Sivaramakrishnan starts a new position as Head of IT & SAP at GMMCO Ltd

GMMCO LIMITED has appointed **Ganesan Sivaramakrishnan** to head its IT and SAP operations. Ganesan Sivaramakrishnan brings over 25 years of experience to GMMCO, having previously served as Head of IT, SAP, and Digital Initiatives at BGR Group. During his tenure at BGR Group, he spearheaded the development and management of their IT infrastructure and SAP systems. Prior to that, Ganesan Sivaramakrishnan co-founded a company, where he honed his leadership skills for over a decade.

Nikhil Shembekar Joins Brigade Group as Chief Information Officer

Nikhil Shembekar has joined Brigade Group as Chief Information Officer. He brings extensive experience to his new role, having previously worked in various positions across the technology sector. This appointment reflects Brigade Group's commitment to leveraging technology for its business growth.

Udit Pahwa starts a new position as CIO at Blue Star Limited

Udit Pahwa has begun his role as Chief Information Officer (CIO) at Blue Star Limited. Prior to this, he served as Group CIO at Kirloskar Management Services and has held positions at various organizations including Huhtamaki India, Polycab Wires, Oracle India, Cap Gemini Ernst & Young India Consulting, Global Electronic Commerce, and the Jasubhai Group.

7 Strategic Steps to Outsmart Modern Cybersecurity Threats

By **Praneeta** | praneeta@9dot9.in

Just a month ago, Andres Freund, a 38-year-old German Microsoft engineer, stumbled upon a potential breach while optimizing his computer's performance. He noticed an unusual spike in processing power usage by a program and identified malicious code that could have exposed sensitive information of countless unsuspecting users. By thwarting this threat, he potentially safeguarded millions of computers from compromise, earning accolades from industry leaders and experts.

The world sighed but enterprises had their eyes glued. Every publication rushed to secure an interview with the heroic employee. However, the incident raised a crucial question: if such an event can happen within one of the largest multinational corporations, how prepared is the rest of the world against new age cyber threats?

In the ever-evolving digital age, the significance of a robust cybersecurity posture cannot be overstated. As enterprises grow, both in size and technological complexity, so do the threats that target them. From small businesses to large corporations, every network is susceptible to attacks that can cripple systems, steal data, and endanger both financial and reputational equity.

According to the Cybersecurity Readiness Index report by networking major Cisco, half of organizations worldwide, 54% to be exact, have faced some sort of cybersecurity incident in just the last year. And it doesn't stop there. A staggering 73% believe they're on the hit list for potential disruptions due to cyber incidents in the next year or two. It's clear, the cyber threat isn't slowing down; it's evolving and as real as ever for businesses everywhere.

In this month's cover story, we delve into the critical challenges facing enterprises as they navigate cybersecurity threats. We consulted industry experts and technology leaders to pinpoint key problem areas and outline actionable steps to prevent them, ensuring readiness for the future.

1. Mitigating Human Error with User Awareness and Training

For two consecutive years now, human error has been tagged as the leading cause of data breaches, with 34% of enterprises acknowledging this painful truth. It seems the old adage 'to err is human' holds particularly true in the realm of cybersecurity. According to the CIO&Leader 2023-24 State of Enterprise Technology Survey, human error is the primary cause of data breaches, emphasizing the adage that man is the weakest link in cybersecurity. Despite advanced tools, human error (22%), social engineering leading to employee mistakes (12%), and occasional misconfigurations (34%) remain top contributors

Sridhar Govardhan, Senior Vice President & Head of Information Security at CoinDCX talked about the critical role of human factors in cybersecurity. He stressed that while technology is essential, the human element often becomes the weakest link in security chains.

"Educating employees about the risks and signs of cyber threats is as crucial as the technological defenses that protect an organization's digital assets," he stated. This approach highlights the need for continuous training and awareness programs within organizations to enhance their overall security posture.

And if you think that's troubling, consider the compliance issues. 40% of respondents in India failed a compliance audit in the past year. This isn't just a small oversight; it's a significant miss that points to a bigger issue—many organizations are struggling to keep up with the ever-changing regulatory and threat landscapes.

The data situation is equally concerning. Only about one-third of Indian organizations can fully classify all their data. And a worrying 20% classify very little or none of their data at all. This lack of data management exposes them to increased risks and makes effective security measures much harder to implement.

2. Network and Access Control Through Zero Trust

Zero Trust approach involves verifying everyone's identity rigorously, ensuring they have only the access they need, and keeping tight controls on different network segments to limit any damage from breaches. It makes sure that each connection, whether it's a user accessing an app, or an application reaching out to a database via an API, is fully checked out.

Dr. Ram Kumar G, Cyber Security & Risk Leader, Nissan Motor, discussed implementing cybersecurity best practices across three key dimensions: people, processes, and technology. Dr. Kumar emphasized the importance of a holistic approach, which includes security by design, zero trust frameworks, and defense-in-depth strategies.

He pointed out the necessity of integrating security considerations early in the software development life cycle (SDLC), advocating for "secure by design" principles that ensure security measures are embedded at the requirement-gathering stage of software development. Dr. Kumar elaborated, "Security by design is crucial—it ensures that we address potential security issues right at the stage when requirements are being gathered, significantly reducing risks downstream."

Zscaler in its Threatlabz 2024 Phishing Report talks about the importance of implementing Zero Trust Architecture that reduces attack surface, prevents lateral movement and lowers the risk of a breach. "Employ granular segmentation to compartmentalize your network, enforce least-privileged access to restrict user permissions, and maintain continuous traffic monitoring," the report mentions as an important step to ensure cyber safety.

Harish Kumar GS, Checkpoint echos the statement. "Implementing a Zero Trust strategy is crucial, ensuring only authorised personnel access sensitive data. Technological aids like two-factor authentication and automated security protocols compensate for human weaknesses. AI and machine learning tools help predict and prevent breaches by identifying unusual patterns, providing critical insights into potential risks."

Here's how Gartner recommends enterprises prepare in its Guide for ZTNA:

1. Start by crafting a comprehensive zero trust strategy, focusing on identifying key risk reduction opportunities and ensuring robust identity and access management before implementing ZTNA solutions.
2. Deploy ZTNA in stages, prioritizing either highly sensitive applications for immediate security enhancement or lower-risk areas with tech-savvy users to minimize disruption. Gradually expand ZTNA adoption across more applications and users.
3. Use clientless ZTNA to replace traditional VPNs for BYOD and extended workforce scenarios, and integrate agent-based ZTNA into a broader SASE framework to enhance overall network security.
4. Choose vendors that support a broad range of security needs and can help reduce the attack surface while offering dynamic, adaptive access control policies that align with zero trust principles, rather than those only focused on replacing VPNs.

"In India, we have witnessed a rise in cyberthreats like financial fraud, data breaches, identity theft, and sophisticated cyber espionage campaigns. According to the data from our Kaspersky Security Network (KSN), around 33% of web users in India have faced cyberthreats in one form or another."

– Jaydeep Singh
GM- India, Kaspersky

3. Proactive Risk Assessment and Continuous Threat Intelligence

The acceleration of sophisticated cyber attacks is fueled not only by the rapid increase in hybrid working policies within organizations but also by their growing dependence on third-party providers for infrastructure, storage, and security solutions.

Technology and security leaders are finding it challenging to develop proactive strategies to minimize the likelihood of cyberattacks. Many CIOs and CISOs acknowledge facing difficulties in maintaining control and visibility over underlying measures and configurations. This limitation hampers their ability to implement

customized security controls aligned with specific requirements and industry regulations.

According to Vivek Srtivastava from Fortinet, "Essential tools such as next-generation firewalls, intrusion detection and prevention systems, endpoint protection, and Security Information and Event Management (SIEM) solutions are crucial in risk assessment and threat intelligence. However, their effectiveness hinges on their integration into a platform that enhances responsiveness, reduces vendor sprawl, and improves visibility and control through centralized management."

Moving on to Threat Intelligence which involves using threat feeds, which are external databases that provide information on known threats, like malware signatures or compromised IP addresses. It's not just about gathering data, though. It's about contextualizing this intelligence with our internal data to understand how these threats could impact us specifically.

Now, let's talk about Response and Remediation. This includes automated responses where the system takes immediate action, like isolating affected systems or blocking suspicious traffic when malicious activity is detected. There's also incident response management, which provides a structured approach to handle and recover from security incidents.

Continuous monitoring is another critical part of TDR services. This means constantly scanning for anomalies and threats, which allows for early detection of potential breaches. Behavioral analysis is also key here; using machine learning to understand what normal behavior looks like so we can spot deviations that might indicate a problem.

And, of course, integration plays a huge role. TDR services need to work seamlessly with existing security measures like firewalls and intrusion prevention systems. Plus, many TDR solutions offer APIs for custom integration, enhancing flexibility and ensuring the security measures fit perfectly with our existing systems.

"Educating employees about the risks and signs of cyber threats is as crucial as the technological defenses that protect an organization's digital assets."

– Sridhar Govardhan
Senior Vice President & Head of Information Security at CoinDCX

"In any cybersecurity strategy, the emphasis lies in adopting a holistic approach, encompassing security by design, zero trust frameworks, and defense-in-depth strategies."

– Dr. Ram Kumar G
Cyber Security & Risk Leader, Nissan Motor

Why are TDR services so critical? They provide:

- **Real-Time Defense:** The ability to detect and respond immediately minimizes the potential damage from cyber attacks.
- **Compliance:** With TDR services, organizations can meet regulatory requirements that demand specific security protocols.
- **Advanced Security:** Employing the latest technologies, including AI and machine learning, TDR services are continuously adapting to the evolving threat landscape.

IBM, an American multinational technology company, suggests businesses dealing with limited resources to expand their team with some AI assistance. With AI stepping in, they can manage up to 85% of those pesky alerts, ensuring round-the-clock protection with threat detection and response services. And don't forget about leveraging threat intelligence to spot those crucial chances to tackle new and emerging threats.

4. Fortifying Information Walls

The Information Walls are like virtual barriers within organizations, meant to stop sensitive information from flowing between different departments or groups. The main goal? To steer clear of any conflicts of interest and stay on the right side of federal regulations.

In the banking sector, where confidentiality is paramount, information walls are vital. A bank's investment division might be working on a high-profile deal. They'd need to keep the details under wraps to prevent insider trading. Information walls help segregate this sensitive information from other parts of the bank, like retail banking or customer service.

Similarly, in industries like health-

care or pharmaceuticals, where patient data and research findings are highly sensitive, information walls play a crucial role. They ensure that confidential patient records or research data don't end up in the wrong hands.

But here's the tricky part:

- They can make teamwork a bit of a challenge. If different teams can't share what they know, it's tough to work together.
- Keeping these walls up-to-date can be a real hassle. Organizations change and grow, and these walls need to keep pace.
- Plus, they can be pretty costly to set up and enforce.

Now, where do these walls really matter?

For businesses, especially those operating in regulated industries like finance, healthcare, or telecommunications, complying with data privacy laws and regulations is essential. Information walls help them meet these compliance requirements by safeguarding sensitive information and preventing unauthorized access.

Overcoming the challenges of these walls isn't easy. They can get in the way of collaboration and drive up costs. But there are ways to make them work better:

- Start by being clear about why each wall is there. Knowing what you're protecting helps design better walls.
- Only put up walls when you really need to. Too many walls can squash innovation.
- Keep checking in on these walls. Business changes, and so do regulations. Regular reviews keep them up-to-date.
- Use tech to keep those walls strong. Automation can make sure the rules are always followed, without adding too much extra work.

5. Transforming Defense through AI-Driven Security Tools

"Data security is something that the security practitioners have been doing for some time now, [at] end of the day, security is all about trying to protect the data, managing the networks, ensuring that the business works."

–Dr Yask Sharma
CISO, IOCL

"Technological aids like two-factor authentication and automated security protocols compensate for human weaknesses. AI and machine learning tools help predict and prevent breaches by identifying unusual patterns, providing critical insights into potential risk."

– Harish Kumar GS
Head of Sales, India and SAARC, Checkpoint

AI systems are like high-speed cameras of data—they can analyze huge volumes with speed, picking out patterns that might indicate a threat. These are patterns that even the sharpest human analysts could miss. Reflecting on trends from the past years, about half of leaders surveyed in the 2022 Global Cybersecurity Outlook believed that automation and machine learning would dominate the cybersecurity landscape. Fast forward to today, and that belief holds strong, with nearly the same percentage endorsing gen AI as the next big influencer in cybersecurity.

"Advancements in AI and ML are revolutionizing cybersecurity defenses. AI enables real-time analysis of vast data sets, swiftly identifying and mitigating evolving threats. Meanwhile, machine learning algorithms can predict future threats by analyzing past attack patterns and subtle indicators of compromise, strengthening proactive defense measures. These technologies automate response actions, such as isolating infected devices, minimizing damage, and allowing security teams to focus on recovery efforts," says Vishal Salvi, Quick Heal.

But it's a double-edged sword. While AI opens up new ways to manage identities and secure data, it also paves the way for new types of cyber threats. The complexity of AI can be manipulated by savvy cybercriminals.

The world of securing AI+ business models is not just about AI itself; it's about securing every step of the AI pipeline. Here's how enterprises can ensure comprehensive security:

- **Securing Training Data:** First, safeguarding the training data used to develop AI models is crucial. We're talking encryption, access controls, and regular integrity checks to keep that data safe and sound.
- **Securing AI Models:** Next, the AI models themselves need protection. Techniques like model

encryption and robustness testing help ensure these models stay resilient against attacks.

- **Securing Model Use and Inferencing:** When it's time to deploy those models, we've got to be on guard. Secure APIs, anomaly monitoring, and real-time protection are key to keeping them safe during inferencing.
- **Securing Infrastructure:** Don't forget about the infrastructure supporting AI. That means locking down servers, networks, and cloud services to fend off any potential threats.
- **Establishing Governance and Operational Guardrails:** Last but not least, governance frameworks and operational guardrails are essential. They keep everything in check, ensuring compliance, accountability, and transparency every step of the way.

6. Secure DevOps Services

Crowdstrike explains DevSecOps as a method that blends development, security, and operations, focusing on integrating security throughout the entire process of software development. This approach is particularly important for companies using cloud technologies or containers, as it helps maintain strong security standards.

DevSecOps ensures that security is an integral part of the development process, not something added on at the end. Here are the key steps involved:

- Companies start by understanding their security risks and how much risk they can tolerate.
- They create a thorough plan to tackle potential security issues and keep up with new threats.
- Security controls are added from the start and throughout the development process.
- To keep up with fast development cycles, security tasks are automated.

"Essential tools such as next-generation firewalls, intrusion detection and prevention systems, endpoint protection, and Security Information and Event Management (SIEM) solutions are crucial. However, their effectiveness hinges on their integration into a platform that enhances responsiveness, reduces vendor sprawl, and improves visibility and control through centralized management."

–Vivek Srivastava
Country Manager,
India and Saarc, Fortinet

The DevSecOps CI/CD Pipeline:
The continuous integration and delivery (CI/CD) pipeline in DevSecOps involves four main stages:

1. **Build:** This is where the code is compiled into a final product ready for deployment.
2. **Test:** The software undergoes thorough testing to ensure new features work correctly and don't break existing ones.
3. **Deliver:** After testing, the software moves to a staging area for final checks and quality assurance.
4. **Deploy:** Once everything is confirmed to work well, the software is officially released.

DevSecOps vs. Traditional DevOps:
Unlike the traditional DevOps approach where security checks might happen late in the development process, DevSecOps incorporates these checks from the start. This helps spot and fix security issues early without slowing down the development.

Best Practices for Implementing DevSecOps:

1. **Include security experts in teams:** Having security specialists within development teams helps integrate strong security measures from the beginning.
2. **Educate and train the IT team:** Equip your IT staff with the skills needed to handle security as a regular part of their job.
3. **Automate security checks:** Use tools that automatically apply security rules and scan for vulnerabilities.
4. **Promote a security-focused culture:** Encourage everyone in the organization to prioritize security in their work.
5. **Choose effective tools:** Opt for tools that are designed for modern, cloud-based environments and that integrate well with existing systems.

By following these guidelines, companies can create a DevSecOps environment that not only speeds up development but also strengthens security, leading to safer, more reliable software.

7. Continuous monitoring and testing

Continuous Security Monitoring (CSM) is a method that automatically checks for cybersecurity risks in a system. It helps organizations make better risk management decisions by giving them real-time updates on potential security threats and weaknesses in their infrastructure.

Organizations now need constant monitoring of their networks to spot any signs of security issues or vulnerabilities quickly. Traditional methods like firewalls and antivirus software aren't enough on their own anymore, as attackers continually find new ways to exploit systems, and new vulnerabilities are reported daily.

Even the best security policies can fail; for instance, many data breaches happen because of weak or stolen passwords. That's why more companies are adopting tools like UpGuard BreachSight, which not only monitors security but also tracks leaked credentials and other exposed data across the internet, including the deep and dark web.

"Over the years, malware has continuously evolved. Ransomware attacks remain a dominant force, and there is a worrying shift in their occurrence. While individual incidents are less frequent, the overall volume of malware detections has risen significantly."

–Vishal Salvi
CEO, Quickheal

"SMEs should remain vigilant and have a clear understanding of the risks involved. It's crucial to allocate enough resources—people, IT infrastructure, and budget—to implement the needed security measures."

–Rishi Baviskar
the Global Head of Cyber Risk Consulting at Allianz Commercial

But what makes Continuous monitoring so important?

Continuous security monitoring is crucial because it allows companies to constantly check and adapt their security practices to align with their internal policies, especially when changes are made. It's vital for any organization that relies on technology for essential tasks to keep its data safe and operations running smoothly.

Growing need for CSM:

1. More sensitive data is being stored digitally.
2. Countries are adopting general data protection laws similar to the EU's GDPR.
3. Laws now require companies to report data breaches, increasing the potential damage to their reputation.
4. Many businesses use third-party vendors, which can increase security risks.

According to NIST SP 800-137, continuous monitoring helps organizations by keeping an updated overview of all systems and vendor interactions, understanding current threats, evaluating security measures, collecting and analyzing security data, communicating security status to all relevant parties, and actively managing risks through informed decisions.

For effective monitoring, it's important that the information collected is based on standard metrics and checked regularly. The strategy should also be updated frequently to reflect any new risks or assets.

Organizations implement continuous monitoring to get a live view of their security status. This includes using security ratings to assess and track the security level of an organization continuously. These ratings are helpful because they:

"With the increased frequency and sophistication of attacks, enterprise security teams are often overwhelmed. Coupled with the continued talent gap and endless sea of disconnected tools and alerts, it's time for technology to meet CISOs and their teams where they are."

– Kim Anstett
CIO of Trellix

- Provide a snapshot of third and fourth-party risk.
- Keep security assessments up to date with simple ratings for easy understanding.
- Help compare security measures with industry peers.
- Continuous security monitoring offers numerous benefits, like:
- It clarifies how much risk an organization can tolerate and helps prioritize security efforts.
- It keeps track of all IT assets and changes within the system.
- It provides ongoing validation that security measures work as expected.
- It ensures compliance with security policies and regulations.
- It raises awareness of threats and vulnerabilities, which helps prevent data breaches.

"With the increased frequency and sophistication of attacks, enterprise security teams are often overwhelmed. Coupled with the continued talent gap and endless sea of disconnected tools and alerts, it's time for technology to meet CISOs and their teams where they are," adds Kim Anstett, CIO of Trellix.

As Kim mentions, cybersecurity efficiency can be enhanced by providing open platforms, integrated capabilities, and AI security agents for streamlined operations, advanced detection and event correlation, malware analysis, and auto-generated response playbooks.

What's next?

As we look forward, the integration of emerging technologies like blockchain, quantum computing, and advanced predictive analytics are set to redefine the paradigms of enterprise cybersecurity. Blockchain, for example, offers a way to secure multipoint transactions and data exchanges, providing transparency while maintaining confidentiality.

In an era where cyber threats are becoming more sophisticated and pervasive, taking proactive steps to enhance cybersecurity is not just advisable; it's imperative. Enterprises must adopt a holistic and agile approach to cybersecurity, incorporating advanced technologies like AI, fostering a culture of continuous learning and vigilance, and aligning security strategies with business objectives.

Enterprises can prepare themselves before a threat hits them, and effectively navigate themselves through the storm with the help of security services and AI tools. We are still behind attaining complete 100% cybersecurity, and whether achieving it is even possible is another question. Dr. Yask Sharma, CISO at IOCL, aptly stated, "data security is something that security practitioners have been prioritizing for some time now. At the end of the day, security revolves around protecting data, managing networks, and ensuring business continuity." Thus, by embracing a holistic approach to cybersecurity, organizations can enhance their resilience and mitigate risks effectively. ■

Organizations must outsource tasks strategically based on project needs and lifecycle

Sandeep Dewangan, Group Chief Information Officer at Safexpress, discusses how integrating outdated production control systems into a unified digital framework enabled real-time monitoring and management, digitalizing manual processes, connecting software across production lines, and transferring IoT data to the cloud for instant access.

By **Nisha Sharma** | nisha.sharma@9dot9.in

Sandeep Dewangan, Group CIO, Safexpress

The tech landscape experienced a significant shift from the mid-2000s to the early 2010s with the advent of the Convergence Era. This period was marked by efforts to create seamless, interoperable digital ecosystems that integrated disparate technology platforms.

The development of industry-driven standards and protocols facilitated the adoption of large-scale Internet of Things (IoT) programs and digital data integration, revolutionizing particularly data-heavy sectors like oil and gas. This shift underscores a strategic transformation in IT management that reshaped industry practices and set new benchmarks for technological deployments.

In an interview with Nisha Sharma, Principal Correspondent at CIO&Leader, Sandeep Dewan-

gan, Group Chief Information Officer at Safexpress, offers valuable insights on the critical factors for navigating digital transformation.

Teaming up for success

One important idea is that companies can't do everything themselves. The Sandeep Dewangan highlights the value of working with other companies (partners) on digital transformation projects. "It's impossible for any organization to keep doing these within their own and hence partners become the only and obvious choice to go along and work with," he says. This makes sense because different companies often have specific areas of expertise. By teaming up, businesses can get the best skills for the job, use resources wisely, and innovate faster.

Communication is key

Leading tech teams well requires clear communication and teamwork. The Sandeep Dewangan emphasizes a multi-year plan that aligns with the company's overall goals. "We have a multi-year roadmap of IT and digital at SafeExpress, which is tied with the multi-year vision of business," he explains. This plan acts like a roadmap, ensuring everyone achieves the same objectives. He also suggests structuring the team to handle different tasks: running existing systems, building new solutions, and constantly improving. Regular check-ins and open communication keep everyone on the same page and ensure everyone contributes effectively.

Security matters more than ever

As businesses connect more online, cyber threats become more serious. Sandeep Dewangan recognizes the need for a comprehensive security approach. This includes clear rules about acceptable online behavior and who can access what information.

Additionally, robust security software like firewalls is crucial for protecting essential systems. But security goes beyond technology. He emphasizes having good security practices and constantly monitoring systems for threats. "This is continuously evolving," he says. "There are there are few fundamentals in terms of an organization having a clear recognized policy and approach on cyber and information security, to having right technology fundamentals on all that we have or we do new, and then also having right practices and SOPs [Standard Operating Procedures] in place. And fourth and very important, must have tech platforms and solutions for continuously monitoring all implementations, all internal, external transactions and information exchange, including end-user behaviors." Companies can build a strong defense against cyberattacks by taking a well-rounded approach.

The future of technology

Looking back at how technology has changed, the Group CIO is impressed by the widespread use of artificial intelligence (AI) and machine learning. These technologies fundamentally change how many industries operate, from logistics to manufacturing. "Today, none of these conversations can be without artificial intelligence and machine learning," Sandeep Dewangan says. However, he believes that quantum computing has the potential to be even more transformative. While still under development, quantum computing promises to revolutionize areas like data encryption, materials science, and the development of new medicines.

"It's impossible for any organization to keep doing these within their own and hence partners become the only and obvious choice to go along and work with."

The Group CIO anticipates that when combined with advancements in AI, edge computing (processing data closer to where it's used), and 5G (faster internet), quantum computing will usher in a new era of technological disruption. "This is something that can become transformational," he says of quantum computing, "We have everything as much what some of these big themes with quantum, and we can be looking at something extraordinarily and absolutely different in the near future for all of us."

A roadmap for the digital age

The conversation with Sandeep Dewangan provides valuable guidance for CIOs and tech leaders navigating the complexities of digital transformation. He emphasizes the importance of strategic partnerships, clear communication within teams, and prioritizing cybersecurity. The CIO's perspective on emerging technologies like quantum computing offers a glimpse into the exciting possibilities. Organizations can thrive in the ever-changing digital landscape by embracing these lessons and staying up-to-date on technological advancements. ■

AI integration in cybersecurity both a boon and challenge

DR. YASK SHARMA
CISO, IOCL

Dr. Yask Sharma, *Chief Information Security Officer at Indian Oil Corporation Ltd., discusses the integration of artificial intelligence (AI) in cybersecurity and the challenges it poses, emphasizing the need for regulation to balance benefits and risks and the future of LLMs in cybersecurity.*

By **Praneeta** | praneeta@9dot9.in

The integration of artificial intelligence (AI) in cybersecurity is seen as both a boon and a challenge. AI helps in managing security alerts and operations, yet its use requires careful regulation to balance its advantages against potential risks.

The ongoing discussions around AI regulation highlight the need for clear guidelines to help security practitioners navigate this evolving terrain. The disparity in security controls between devices within an organization's premises and those used remotely by employees complicates the ability to maintain consistent data protection as well.

In an interview with Praneeta, Correspondent at CIO&Leader, Dr. Yask Sharma, Chief Information Security Officer at Indian Oil Corporation Ltd., offers valuable insights on AI adoption and cybersecurity challenges faced by industries.

Data protection and compliance

"I think it stems from the compliance's point of view," Dr. Yask explains how security practitioners have been

involved in data security for some time now. "[At the] end of the day, security is all about trying to protect the data, managing the networks, ensuring that the business works."

He notes the increase in compliance over the last five to seven years. Data security and managing the networks, making sure the business works smoothly, are all key focuses in security. Governing bodies across the globe are also shifting their focus to restricting data access, also known as data sovereignty.

"I think what is now becoming important is that how one protects the data and also ensures compliance with the statutes that are there." He emphasizes the balance between security services offered and meeting security and compliance requirements.

Security challenges in hybrid work

The trend of remote work, which has gained momentum post-COVID, Dr. Yask comments, has led to a widespread distribution of data as companies offer their employees the flexibility to work from various locations using different devices. "Trying to have the same set of controls which are there in a controlled environment, in a typical organizational level, versus the same kind of control on a privately owned machine," he mentions, raises issues of data sovereignty due to differing legal requirements across borders.

There's a growing need for solutions that comply with legal standards, not just security measures. Security professionals, traditionally focused on protecting data, now find themselves navigating these legal complexities as well.

AI integration in cyber threats

AI has been integral to technological advances for a long time, but the prominence of Large Language Models (LLMs) has recently increased, benefiting security practices significantly. "It's actually a boon for the security practice, especially the L1, L2, L3 people. They get a lot of help in triaging the alerts and all these things," Dr. Yask explains.

Security professionals, traditionally focused on protecting data, now find themselves navigating these legal complexities as well.

However, the dual nature of technology, having both positive and negative impacts, calls for stringent regulation. There is already significant discussion on the need to regulate AI more tightly. As compliance and regulations evolve, they will play a crucial role in guiding security practitioners about permissible actions and limitations.

"There is no way that you can control the use of these AIs and LLMs; [they] are just going to increase," he emphasized.

Upcoming cybersecurity trends

"LLM is something that we are very closely watching. This is something that I think is going to add a lot of value," he pointed out while talking about how managing what LLM can do presents a challenge to security practitioners. "This is, I think, the biggest transformational technological solution or technology that has come up in recent years."

Dr. Yask also mentions how security is increasingly being intertwined with geopolitics. In the next few years, this connection will significantly influence the types of solutions and partnerships countries pursue. "Geopolitics is going to be amongst the key factors which would decide what kind of solutions, what kind of partnerships countries would have...the collaborations they would have or would not have." ■

Employee cybersecurity awareness is as critical as tech defenses

SRIDHAR GOVARDHAN
Senior Vice President & Head of Information Security, CoinDCX

Sridhar Govardhan, *Senior Vice President & Head of Information Security at CoinDCX, underscored the evolving nature of cyber threats and the dynamic strategies required to counter them.*

By **Nisha Sharma** | nisha.sharma@9dot9.in

In an increasingly digital world, the specter of cyber threats continues to loom large over businesses and IT leaders. This pressing issue was the focus of a recent webinar hosted by the CSO Forum and the 9.9 Group, featuring cybersecurity expert Sridhar Govardhan, Senior Vice President & Head of Information Security at CoinDCX. With nearly 25 years of experience in building enterprise networks, Sridhar Govardhan is a seasoned veteran in the field, known for his strategic insights into combating cyber threats effectively.

The resurgence of ransomware

The year 2023 has marked a disturbing increase in cyberattacks, particularly ransomware and extortion attempts. Govardhan pointed out, "Hackers are increasingly targeting IT and physical supply chains, launching mass cyber-attacks, and finding new ways to extort money

from companies and individuals." This resurgence is compounded by the integration of artificial intelligence in attacks, creating a new generation of AI-powered malware and phishing messages that are sophisticated and difficult to detect.

The digital transformation and its implications

A significant part of the webinar was devoted to understanding how technological and economic shifts influence cybersecurity vulnerabilities. The transition from physical to digital and virtual economic systems has revolutionized how transactions are conducted, but it has also introduced new avenues for cyber exploitation. Govardhan explained, "As we digitize our monetary systems—from physical cash to digital transactions and now to cryptocurrencies—we are increasingly exposed to cyber threats that exploit these platforms."

The crucial human factor

One of the recurring themes in Govardhan's presentation was the critical role of human factors in cybersecurity. He stressed that while technology is essential, the human element often becomes the weakest link in security chains. "Educating employees about the risks and signs of cyber threats is as crucial as the technological defenses that protect an organization's digital assets," he stated. This approach underscores the need for continuous training and awareness programs within organizations to enhance their overall security posture.

Strategic approaches to cybersecurity

To effectively combat the sophistication of modern cyber threats, Govardhan recommended a multifaceted and tailored approach to cybersecurity:

- Identifying core assets is crucial, as protecting these ensures that the most critical elements of the business are safeguarded.
- Customized security measures must be implemented based on specific industry needs and the unique threats each sector faces.
- Adaptation and vigilance are key; organizations must stay on top of emerging threats and adapt their defenses accordingly.

Future trends and the role of AI

Looking ahead, Govardhan predicted that AI would play an even more significant role in cybersecurity, both as a tool for cybercriminals and as a defense mechanism. "AI-driven attacks are expected to become more autonomous, capable of conducting end-to-end breaches with minimal human intervention," he noted. This potential future makes it imperative for cybersecurity measures to evolve in anticipation of these advanced threats.

"AI-driven attacks are expected to become more autonomous, capable of conducting end-to-end breaches with minimal human intervention."

As businesses continue to navigate this challenging landscape, Govardhan's wisdom offers a valuable roadmap for enhancing their cybersecurity measures.

The discussions and strategies highlighted in the webinar reflect a deep understanding of both the technical and human aspects of cybersecurity. As we look forward, the emphasis on continuous adaptation and education appears more relevant than ever. By embracing these principles, organizations can better prepare themselves against the ever-changing tide of cyber threats that challenge our digital world. ■

Navigating the New Realities of Global Applications and Cybersecurity

ARUL ELUMALAI
GM Security & Distributed Cloud (SDC) Product Group, F5

Arul Elumalai, *GM Security & Distributed Cloud (SDC) Product Group at F5, and* ***Shawn Wormke,*** *Vice President and General Manager of NGINX,- discuss recent trends, reflecting a comprehensive view of the current and future states of application development and cybersecurity.*

By **Nisha Sharma** | nisha.sharma@9dot9.in

The global application landscape has experienced a significant transformation catalyzed by advancements in digital technologies and an increasing emphasis on robust cybersecurity measures. This evolution presents opportunities and challenges for businesses as they adapt to a rapidly changing environment. Here, we delve deeper into the dynamics shaping this landscape, the complexities introduced by new technologies, and the strategies enterprises adopt to secure their digital assets.

In a recent exploration of the rapidly evolving global application landscape, Nisha Sharma engaged in a revealing conversation with Arul Elumalai, GM Security & Distributed Cloud (SDC) Product Group at F5, and Shawn Wormke, Vice President and General Manager of NGINX.

The discussion focused on the current challenges and advancements shaping how businesses approach digital transformation and cybersecurity. Arul provided insights into the strategic management of application

demands within today's fast-paced digital economy. Shawn complemented this by discussing methods to enhance modern application deployment through innovative technologies. Together, their expert perspectives shed light on effective strategies for navigating the complexities of technological advancement and robust cybersecurity in an increasingly interconnected world.

The evolution of global applications

The number of applications enterprises utilize in the digital era has surged dramatically. This isn't just a quantitative increase but also a qualitative one, where applications have become more integral to business operations across various sectors and regions. The shift towards digital-first strategies has necessitated the modernization of application architectures, embracing microservices and distributed cloud environments to enhance agility and scalability.

"Across Big IP and NGINX, we are seeing a portfolio build-out that supports these modernized architectures, leading to further distribution and fragmentation of both applications and data," explained Arul Elumalai, GM Security & Distributed Cloud (SDC) Product Group at F5; this development underscores a broader industry trend towards decentralization, where applications are not just stored in a centralized data center but are spread across multiple cloud environments, from public to private and hybrid models.

Moreover, the rise of public-facing APIs has introduced new layers of complexity and vulnerability. APIs have become the backbone of digital interaction, facilitating data exchange and functionality between software applications. However, they also represent a significant security risk if not properly managed and secured, highlighting the need for comprehensive API security strategies.

Cybersecurity challenges and strategic responses

As applications become more complex and distributed, securing them becomes increasingly challenging. The fragmented nature of modern applications introduces numerous vulnerabilities, making traditional perimeter-based security measures insufficient. "Managing the risk associated with this distributed architecture is paramount, as each node and service within the system potentially opens up new avenues for attack," noted Shawn Wormke, Vice President and General Manager of NGINX.

Companies like F5 have developed distributed cloud platforms that integrate security directly into the application environment to address these challenges. This integration allows for consistent security policies across all applications, regardless of where they are deployed. It simplifies management and enhances the ability to respond to threats in real-time.

"By connecting applications across all environments with a secure network layer and embedding security services within, we can tame the complexity and ensure comprehensive protection," said Shawn Wormke This approach is critical in an era where cyber threats are becoming more sophisticated and pervasive, as evidenced by the staggering number of cyber attacks reported annually.

Future directions

Looking ahead, artificial intelligence (AI) and machine learning (ML) are set to play pivotal roles in shaping the future of application development and cybersecurity. These technologies offer the potential to automate complex processes, provide predictive insights, and enhance the efficiency of security protocols.

F5, for example, is integrating AI capabilities across its portfolio to offer advanced behavioral analysis, automate threat detection, and streamline management processes.

SHAWN WORMKE
Vice President and General Manager, NGINX

"Our AI-driven tools are designed to not only detect and respond to threats in real-time but also provide predictive capabilities that help prevent incidents before they occur," shared Arul Elumalai at F5.

Moreover, as enterprises increasingly adopt AI-driven applications, the complexity of managing and securing these applications will escalate. Integrating AI into cybersecurity strategies is expected to mitigate these challenges by enhancing the intelligence and responsiveness of security systems.

Conclusion

The evolution of the global application landscape and the corresponding cybersecurity challenges require a nuanced understanding and a proactive approach. Enterprises must embrace innovative technologies and strategies to secure digital assets while fostering growth and innovation. ■

"Human Firewall" is the first step towards organizational security

VIVEK SRIVASTATVA
Country Manager, India & SAARC, Fortinet

Vivek Srivastava, *Country Manager for India & SAARC at Fortinet, highlights the critical importance of cybersecurity and the potential of AI to counter AI threats. He emphasized the need for a cybersecurity-aware culture and robust cybersecurity governance.*

By **Praneeta** | praneeta@9dot9.in

As the world rapidly advances towards AI, industry experts are voicing concerns about its impact on enterprise security. Fortinet, a leading cybersecurity company, is continuously collaborating with brands like IBM and Samsung to offer innovative services such as firewalls, endpoint security, and intrusion detection systems.

In a recent conversation with CIO&Leader, Vivek Srivastava, Country Manager for India & SAARC at Fortinet, highlighted the critical importance of cybersecurity and the potential of AI to counter AI threats. He emphasized the need for a cybersecurity-aware culture and robust cybersecurity governance.

Vivek Srivastava, with 23 years of experience in technology and cybersecurity, has successfully scaled start-ups and small businesses to multi-million-dollar enterprises, managing businesses over $50 million. Having led numerous significant projects for enterprises, service providers, and government entities

in India and the SAARC region, Vivek believes cybersecurity is essential for the survival and success of digital enterprises.

CIO&Leader: Could you elaborate on the role of artificial intelligence (AI) in enhancing cybersecurity measures across various sectors? How is AI being leveraged to mitigate cyber threats effectively?

Vivek Srivastava: Artificial intelligence is playing an increasingly critical role in enhancing cybersecurity across various sectors by enabling more sophisticated threat detection and response mechanisms. AI algorithms excel at analyzing vast datasets in real-time, which allows for the rapid and accurate detection of potential threats. This capability extends to intelligent monitoring, where AI automates the observation of system logs and network traffic, proactively identifying any anomalies that may indicate a breach. Moreover, AI leverages predictive analytics to utilize historical data in predicting and preventing potential security incidents before they occur. Its capacity for automated responses not only provides immediate alerts but also suggests remediation strategies, thereby optimizing incident management.

At Fortinet, we harness AI's potential to revolutionize cybersecurity. We've developed over 40 AI-powered solutions that enhance our ability to identify and neutralize threats swiftly—from taking days to less than an hour. Our AI-driven systems conduct context-aware analysis and offer targeted remediation guidance, which markedly reduces investigation and response times. This advanced technology supports security operations teams in achieving faster detection and responses, enhancing their overall security posture.

As we move forward into 2024 and beyond, AI's role in cybersecurity is set to become even more transformative, particularly in the integration within physical security systems. Expect AI to drive proactive threat detection, intelligent monitoring, and adaptive security responses, with Fortinet leading the way in these innovations.

Wide-spread adoption of hybrid work and proliferation of devices has led some organizations to lag in maintaining software and system patching, further expanding the attack surface.

CIO&Leader: Addressing human error is crucial in minimizing cybersecurity risks. From your perspective, what strategies or best practices can organizations adopt to reduce instances of human error in cybersecurity?

Vivek Srivastava: Addressing human error is a pivotal aspect of minimizing cybersecurity risks, as anyone within an organization can inadvertently become a vector for cyber threats. Whether it's through falling prey to phishing or social engineering attacks, misconfiguring systems, failing to apply security patches, or introducing vulnerabilities in code, the human factor often plays a critical role in security breaches.

Our research at Fortinet, detailed in the 2023 Security Awareness and Training report, underscores this point. It revealed that 81% of organizations experienced malware, phishing, and password attacks last year that specifically targeted individual users. Moreover, over 90% of leaders agree that enhancing cybersecurity awareness among employees significantly contributes to reducing attack incidences. Regular and comprehensive training on common cyber threats and adversary tactics is crucial to construct a robust "human firewall" that can prevent initial breaches.

Cultivating a cybersecurity-aware culture within an organization requires time and commitment at every level. By ensuring that all employees are actively involved and aware of their roles in safeguarding the organization, we can foster a proactive approach to risk mitigation and incident response. Effective training empowers employees to take action against potential threats, thereby enhancing the organization's overall cyber resilience and establishing a solid first line of defense against cyberattacks.

CIO&Leader: What is your evaluation of the present status of cyber-

security legislation and regulation, and how effective do you find it in responding to the dynamic challenges posed by the evolving cyber threat landscape?

Vivek Srivastava: The laws governing cybersecurity must be designed to be proportional to the threats, reflecting the growing concerns around cyber risks. Laws like the Data Protection Bill and breach disclosure mandates have made it evident that cybersecurity transcends IT and touches on broader organizational accountability.

With regulators intensifying compliance demands, it's imperative for organizations to implement robust cyber-risk and cybersecurity governance frameworks. This responsibility extends to the board level, where there is a crucial need to understand and monitor potential cyber threats that could impact the organization. It's essential for those in governance roles to ensure that comprehensive strategies, policies, and procedures are in place to effectively mitigate these risks.

Moreover, there must be a robust incident response plan ready to activate in the event of a security breach, aimed at minimizing the impact. Additionally, organizations are required to maintain systems capable of detecting, investigating, and eradicating any intrusions, ensuring adherence to contractual, legal, and regulatory obligations. This comprehensive approach is critical in responding to the dynamic challenges posed by the evolving cyber threat landscape.

CIO&Leader: Looking ahead, what emerging cyber threats do you foresee impacting organizations in the near future?

Vivek Srivastava: The increasing weaponization of generative AI by cybercriminals allows them to increase their attacks, from circumventing social engineering detection to replicating human behaviours more convincingly. Ransomware attacks remain prevalent, with adversaries utilizing sophisticated techniques like double extortion. They are targeting essential infrastructures and demanding substantial ransoms. Moreover, some ransomware campaigns are becoming more targeted and hands-on, allowing cybercriminals to customize their approach, avoid detection, and enhance the success of their operations. Advanced Persistent Threat (APT) groups are refining their tactics, techniques, and procedures (TTPs), often outpacing traditional security solutions that rely on outdated analytics.

Regarding Operational Technology (OT), threats are escalating beyond mere data encryption. Attackers are increasingly engaging in extortion-driven supply chain attacks, aiming to disrupt critical services and organizations. Additionally, the widespread adoption of Internet of Things (IoT) devices introduces significant vulnerabilities due to often insufficient security measures. These devices are becoming prime targets for exploitation.

CIO&Leader: In light of the rapidly evolving cybersecurity landscape, how do you perceive the current challenges and opportunities for enterprises?

Vivek Srivastava: As companies digitize and integrate their Information Technology (IT) and Operational Technology (OT) networks, the complexity of protecting these interconnected systems from cyberattacks increases. Additionally, the widespread adoption of hybrid work and proliferation of devices has led some organizations to lag in maintaining software and system patching, further expanding the attack surface.

To stay ahead of these cyber threats, enterprises must invest in advanced security technologies. Essential tools such as next-generation firewalls, intrusion detection and prevention systems, endpoint protection, and Security Information and Event Management (SIEM) solutions are crucial. However, their effectiveness hinges on their integration into a platform that enhances responsiveness, reduces vendor sprawl, and improves visibility and control through centralized management.

This holistic approach should also accommodate solutions like Secure Access Service Edge (SASE), which are critical for securing the expanding network edge and remote work environments. Moreover, the inclusion of Artificial Intelligence (AI) and Machine Learning (ML) within these platforms is essential to accelerate threat detection, analysis, and response across distributed networks.

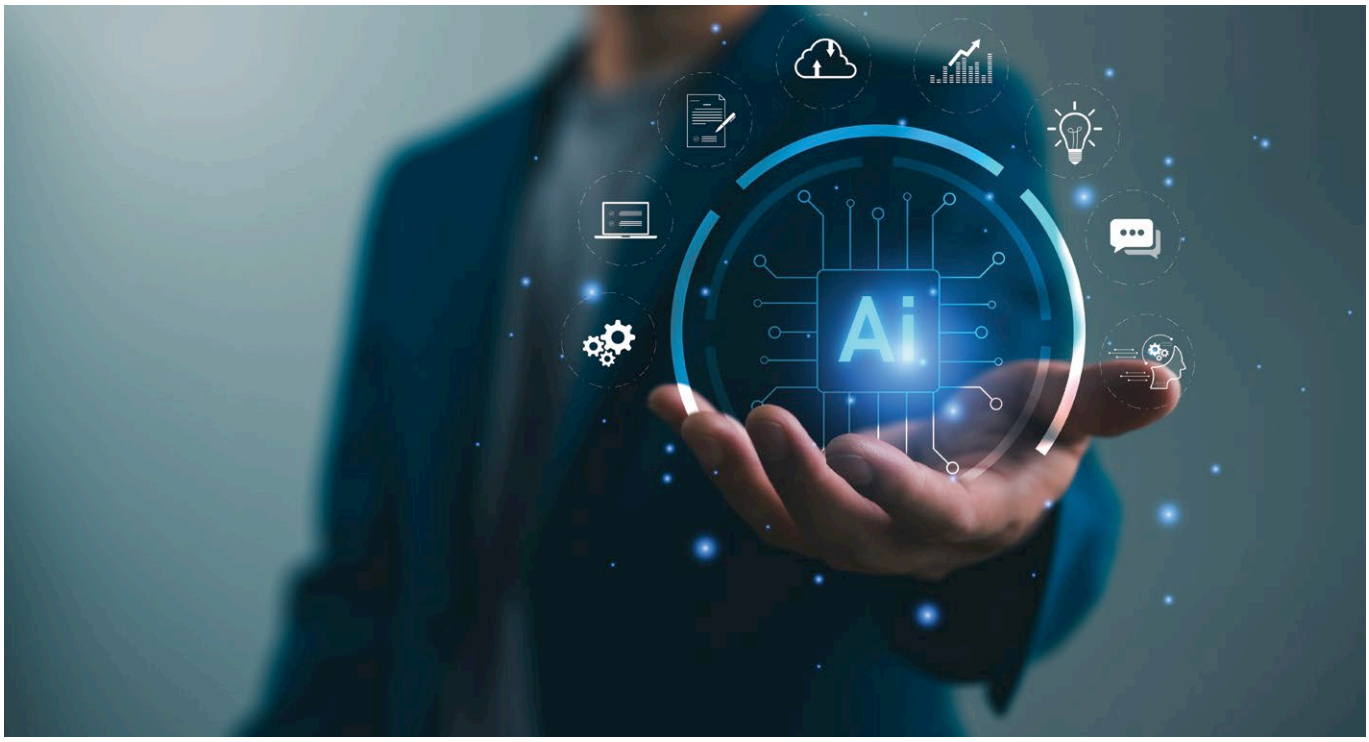
CIO&Leader: What strategies and best practices do you recommend for protection against cyber threats?

Vivek Srivastava: To effectively combat cyber threats, adopting a strategic combination of detection, remediation, and automation is key. Investing in advanced detection technologies like Endpoint Detection and Response (EDR), Network Detection and Response (NDR), and User and Entity Behavior Analytics (UEBA) is crucial. Seamless Integration of security tools and systems is essential for a comprehensive view of the security landscape, enhancing detection and response capabilities.

Continuous training is vital for reducing risks from phishing attacks and other cyber threats.

Proactive training has helped reduce such risks by 84% in some cases, highlighting the importance of ongoing education. Partnering with Managed Security Service Providers (MSSPs) offers additional expertise and ensures continuous monitoring, allowing internal teams to focus on strategic initiatives. ■

Generative AI's Game-Changing Impact on InsurTech



Generative AI's data processing and analysis capabilities are invaluable for predictive risk assessment.

By **Sachin Panicker** | editor@cioandleader.com

Insurance is one of the key sectors where Generative AI is expected to have a revolutionary impact – enhancing operational efficiency and service delivery, and elevating customer experience. From automating claims processing to predictive risk assessments, let us take a deeper look at some of the Generative AI use-cases that will redefine InsurTech in the years ahead.

Automated and Efficient Claims Settlement

Lengthy and complex claims settlement processes have long been a pain-point for insurance customers. Generative AI addresses this by streamlining the claims process through seamless automation.

AI analyzes images or other visual data to generate damage assessments. It can extract and

analyze relevant information from documents such as invoices, medical records and insurance policies – enabling it to swiftly determine the validity of the claim, as well as the coverage, and expedite the settlement. This serves to improve process efficiency, reduce the administrative burden on staff, and significantly boost customer satisfaction.

Optimized Underwriting and Streamlining Risk Assessment

Underwriting is another key area where this technology can create immense value for insurance firms. With their ability to analyze vast amounts of data, Generative AI models build comprehensive risk assessment frameworks that enable them to swiftly identify patterns and highlight potential risks. It automates evaluation of a policy applicant's data, including medical and financial records submitted, in order to determine the appropriate coverage and premium.

Leveraging AI, underwriters are empowered to better assess risks and make more informed decisions. By reducing manual effort, minimizing the possibility of human error, and ensuring both accuracy and consistency in risk assessment, Generative AI is poised to play a pivotal role in optimizing underwriting processes.

Empowering Predictive Risk Assessment

Generative AI's ability to process and analyze complex data is immensely valuable in terms of building capabilities for predictive risk assessment. Analyzing real-time and historical data, and identifying emerging patterns and trends, the technology enables insurers to develop more sophisticated models of risk assessment that factor in a wide range of parameters – past consumer behavior, economic indicators, weather patterns, to name a few. These models allow insurers to assess the probability of specific claims, for instance those related to property damage, or automobile accidents. Moreover, the predictive capabilities of Generative AI helps insurers offer more tailored coverage and align their pricing strategies with a dynamic environment.

The ongoing risk monitoring, and early detection of potential issues that the technology facilitates can also prove highly effective when it comes to fraud prevention. Through continuous analysis of data streams, AI identifies subtle changes and anomalous patterns that might be indicative of fraudulent activity. This empowers insurers to take proactive measures to identify possible fraudsters, prevent fraud and mitigate potential losses.

The robust predictive risk assessment capabilities offered by Generative AI thus serve to strengthen insurer's business models, secure their services against fraud and other risks, and enhance customer trust and confidence in the coverage provided.

Unlocking Personalized Customer Service

In a digitally driven world, personalization has emerged as a powerful tool to effectively engage customers and elevate their overall experience. By analyzing vast amounts of consumer data, including interactions across the insurer's digital touchpoints, Generative AI gains insights into consumer behavior and preferences, which in turn enables it to personalize future customer service interactions.

The predictive capabilities of Generative AI help insurers offer more tailored coverage and align their pricing strategies with a dynamic environment.

For instance, analyzing customer profiles, historical data, and various other factors, AI can make personalized policy recommendations, tailored to an individual customer's specific needs, circumstances and risk profile.

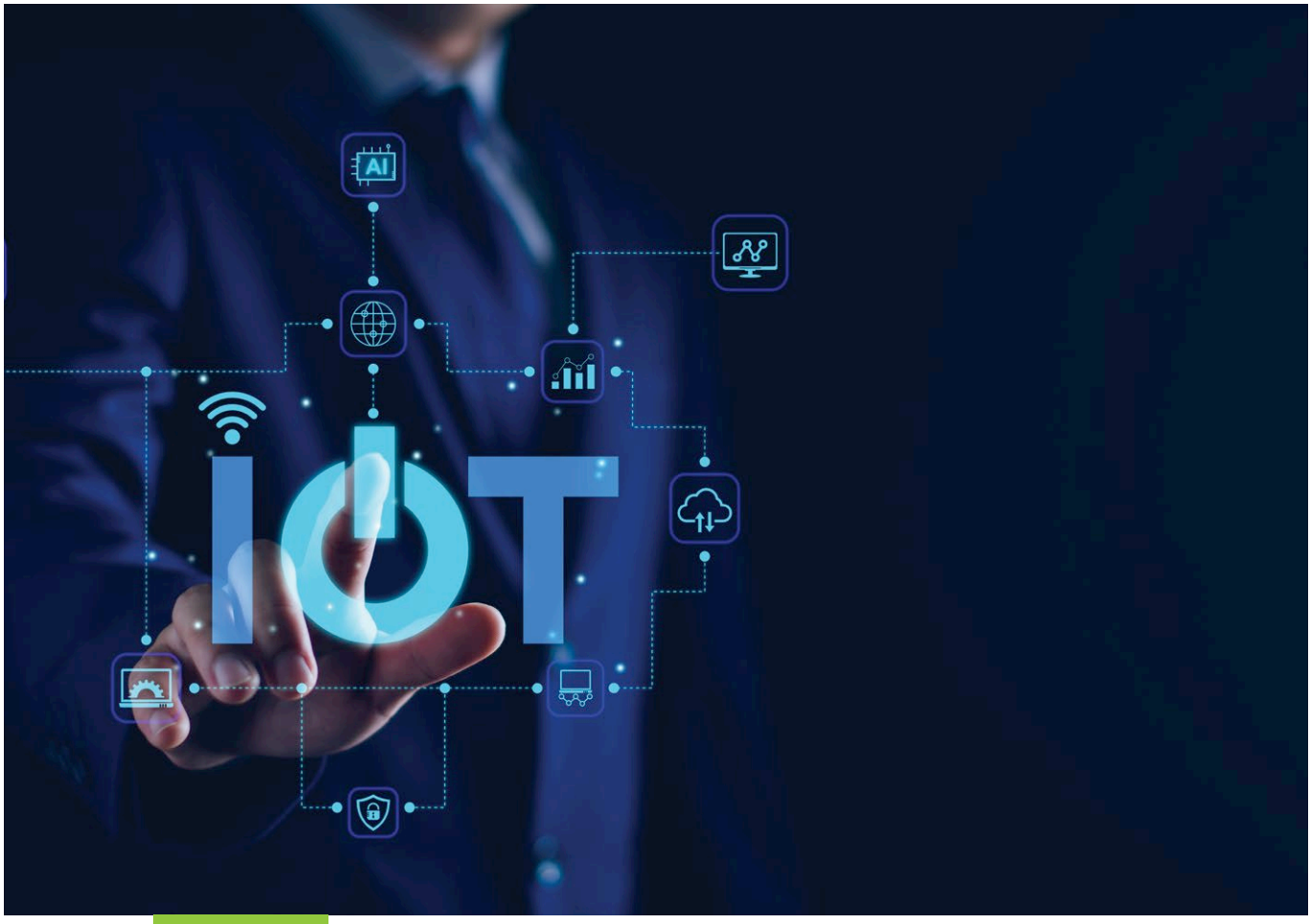
Simulating human-like conversation with near-perfection, Generative AI can also engage with customers across an insurer's support channels, resolving queries and providing guidance or making recommendations based on their requirements.

The personal touch that Generative AI brings to customer engagement, as compared to other more impersonal digital interfaces, coupled with the valuable tailored insights and offerings they provide, will go a long way towards helping insurers build long-term relationships with policyholders.

Charting a Responsible Course with Generative AI in Insurance

The outlook for Generative AI across sectors looks bright, and insurance is no exception to the trend. Insurance firms that embrace the technology, and effectively integrate it into their operations, will certainly gain a significant competitive advantage through providing innovative solutions, streamlining processes, and maximizing customer satisfaction. This optimism however must be tempered with an acknowledgement of concerns by industry stakeholders, and public at large, around data privacy and the ethics of AI-driven decision-making. Given that insurance is a sector heavily reliant on sustained consumer trust, it is essential for leaders to address these concerns and chart a course towards responsible AI adoption, in order to truly reap the benefits of the technology and usher in a bold new era of InsurTech. ■

—Sachin Panicker is the Chief AI Officer at Fulcrum Digital



The Vulnerability Conundrum: Are all IoT devices hackable?

The interconnected IoT ecosystems increase risks, emphasizing the need for strong security measures.

By **Karan Patel** | editor@cioandleader.com

As technology advances, proactive efforts to fortify IoT infrastructure are imperative to safeguard against potential breaches.

In our digital era, where smart homes and interconnected gadgets are ubiquitous, the specter of security threats looms large. Imagine the far-reaching consequences of a compromised smart home hub. It's not just about the immediate impact on the homeowner, but also the potential for a domino effect of network infiltration. This breach could extend beyond personal data compromise to affect a wide range of interconnected devices, from security cameras to smart appliances. The interconnected nature of IoT ecosystems amplifies the risks, underscoring the critical need for robust security measures.

In April 2019, Microsoft uncovered a chilling reality: Strontium, also known as the notorious 'Fancy Bear,' had exploited IoT devices as gateways to infiltrate internal networks. Their strategy was deceptively simple yet devastatingly effective—exploit default passwords and target unpatched devices lacking crucial security updates. These vulnerabilities handed hackers unrestricted access to sensitive networks, a nightmare scenario for any cybersecurity professional.

One glaring vulnerability lay in the default passwords of IoT devices. Some devices retained their factory-set passwords, providing hackers with a backdoor entry. This oversight, compounded by the sheer volume of IoT devices permeating modern households, created a veritable goldmine for cybercriminals. The lesson here is clear: neglecting to change default passwords is akin to rolling out the welcome mat for hackers.

Equally concerning was the prevalence of unpatched IoT devices. Failing to update firmware and security protocols made these gadgets susceptible to exploitation. In the hands of efficient hackers, these unsecured devices became conduits for malicious activity, enabling unauthorized access to internal networks. The repercussions of such breaches are profound, ranging from data theft to network disruption, underscoring the urgent need for stringent security measures.

The crux of the matter lies in the inherent trade-off between convenience and security. IoT devices promise seamless integration and enhanced functionality, but at what cost? As evidenced by the Fancy Bear incident, the convenience of interconnected gadgets can inadvertently compromise security, inviting exploitation by malicious actors.

So, can all IoT devices be hacked? Unfortunately, the answer is a resounding yes. While not every device may have obvious vulnerabilities, the widespread use of IoT technology means that no device is completely immune to exploitation. This places a shared responsibility on manufacturers and consumers to prioritize security measures and stay alert to potential threats. Only through this collective effort can we hope to mitigate the risks associated with IoT security.

In conclusion

There is an urgent need for heightened cybersecurity measures. The Fancy Bear episode is a stark reminder of the digital age's precarious balance between innovation and security. As technology advances, proactive efforts to fortify IoT infrastructure are imperative to safeguard against potential breaches. After all, in the realm of cybersecurity, vigilance is the best defence against the looming threat of exploitation. ■

—Karan Patel, Co-founder, CEO and Technical Director, Redfox Security.

Empower Your Business with Digital Defenses with Proactive and Comprehensive Cybersecurity Services

Rising cyberattacks on IoT devices emphasize the need for manufacturers, service providers, and cybersecurity professionals to collaborate on robust security measures.

By **Mukul Kulshrestha** | editor@cioandleader.com

In today's rapidly evolving digital landscape, organizations spanning various industries are intensifying their security measures to combat the escalating cyber threats. The exponential growth of digital technology coupled with its integral role in daily operations has prompted this proactive stance. Driven by the surge in digital transformation, widespread adoption of cloud technology, the transition to remote work, and the increasing prevalence of targeted cyberattacks, cybersecurity has emerged as a multifaceted and costly challenge for all enterprises.

Cyberattacks, characterized by their increasing frequency and sophistication, now pose a significant risk not only to large corporations but also to small and medium-sized businesses. Threat actors are continually refining their tactics, leveraging advanced techniques to evade conventional security measures effortlessly.

Meanwhile, the financial implications of a data breach have reached unprecedented heights, as shown in the IBM and Ponemon Institute report – an average cost of USD 4.45 million in 2023, marking a 2% increase from the previous year's figure

of USD 4.25 million. In light of these figures, organizations cannot afford to underestimate the importance of robust cybersecurity measures. Neglecting adequate security protocols and resource allocation for managing IT infrastructure not only exposes sensitive information to compromise but also subjects businesses to significant financial and reputational risks. In addition to these challenges is the scarcity of cybersecurity experts, further intensifying the vulnerability of organizations to cyber threats. In this context, the implementation of a comprehensive security program, supported by sufficient resources and specialized services, is imperative to mitigate these risks effectively.

Key trends that shape the cybersecurity industry

The adoption of AI-enabled technologies is crucial in combating increasingly sophisticated threat actors, enhancing threat detection, and streamlining security processes. However, the rapid advancement of AI also poses the risk of intelligent AI-powered attacks, compelling continuous refinement of algorithms. Additionally, the intersection of 5G and cybersecurity demands robust measures to safeguard digital assets, requiring collaborative efforts from cybersecurity professionals, telecom providers, and government entities. The rise of deep fakes and clones presents concerns for brand reputation and trust, urging organizations to invest in advanced detection tools and boost cybersecurity measures. Escalating cyberattacks targeting IoT devices highlight the need for collaboration among manufacturers, service providers, and cybersecurity professionals to implement robust security measures. Finally, as Extended Reality (XR) technologies become more pervasive, organizations must prioritize user education and secure communication protocols to address security concerns effectively.

Proactive approaches mitigate risks, uphold regulatory standards, cultivate customer confidence, and streamline reactive security measures.

Benefits of proactive cybersecurity

Proactive cybersecurity empowers organizations to predict and counter potential threats with preemptive measures. These include ongoing monitoring of networks and systems, regular penetration testing, and timely application of software updates and patches. Furthermore, strengthening defenses by installing firewalls, intrusion detection systems, and access controls enhances security posture. Proactive approaches mitigate risks, uphold regulatory standards, cultivate customer confidence, and streamline reactive security measures. By preempting data breaches, financial losses, and reputational damage associated with cyber-attacks, proactive cybersecurity reinforces organizational integrity and resilience.

Network security services protect computing devices and systems from potential threats and data leakage, enhancing network performance, visibility, and compliance with security standards.

Need for a comprehensive range of cybersecurity services

Cyber Security Service Providers offer comprehensive cybersecurity services aimed at safeguarding organizations' digital assets and data from malicious actors. These services include a wide range of offerings, such as advanced threat detection, threat intelligence, network security, cloud security, endpoint security, incident response services, and security education and training capabilities.

Advanced threat detection empowers organizations to identify and neutralize cyber threats before they inflict harm by analyzing automated monitoring, network traffic, user behavior, and system logs for anomalies and potential breaches.

Threat intelligence involves analyzing data using various tools and methods to glean insights into present or future threats, aiding in risk mitigation and enabling proactive defense strategies against cyberattacks.

Network security services protect computing devices and systems from potential threats and data leakage, enhancing network performance, visibility, and compliance with security standards. When combined with endpoint-specific protections, these services effectively mitigate risks posed by malware, phishing attacks, and unauthorized access attempts.

Cybersecurity Service Providers also offer cloud security measures such as data encryption and access control to ensure the confidentiality, integrity, and availability of sensitive data and applications hosted in the cloud. Additionally, security awareness training educates employees about the latest cyber threats and best practices, significantly reducing the risk of successful cyberattacks.

Measures to secure customers' sensitive data

Cybersecurity Service Providers empower customers to enhance their security posture by implementing adaptable and agile security frameworks. Embracing a continuously evolving cyber resilience model is essential for organizations to effectively defend against next-generation threats. Given the growing trend of granting vendors access to business systems, managing third-party risks is now vital. To ensure a secure and compliant adoption of cloud services, organizations should utilize cloud governance solutions. Implementing advanced automation models can strengthen resilience against the rising threat of ransomware incidents. Furthermore, investments in advanced machine learning solutions are critical for addressing persistent and ever-evolving cyber threats, enabling real-time remediation and control.

Embracing a proactive perspective toward cybersecurity and integrating robust security protocols enables businesses to outpace emerging threats and reduce the likelihood of security breaches. Whether prioritizing advanced threat detection, incident response strategies, security awareness training, or fortifying cloud security, investing in holistic cybersecurity services and solutions is imperative for protecting business operations amidst the complexities of today's digital environment.. ■

—Mukul Kulshrestha is the Vice President at Cyber Security, Inspira Enterprise.

डिजिट
अब हिंदी में

देश का सबसे लोकप्रिय और विश्वसनीय टेक्नोलॉजी वेबसाइट डिजिट अब हिंदी में उपलब्ध हैं। नयी हिंदी वेबसाइट आपको टेक्नोलॉजी से जुड़े हर छोटी बड़ी घटनाओ से अवगत रखेगी। साथ में नए हिंदी वेबसाइट पर आपको डिजिट टेस्ट लैब से विस्तृत गैजेट रिव्यु से लेकर टेक सुझाव मिलेंगे। डिजिट जल्द ही और भी अन्य भारतीय भाषाओ में उपलब्ध होगा।

digit.in
NOW IN HINDI

www.digit.in/hi
www.facebook.com/digithindi

डिजिट

MEHENG 12896/13/1/2011-TC DATED18/05/2011

AMD

PRESENTS

25th ANNUAL CIO&LEADER CONFERENCE

INTELLIGENT ENTERPRISE AI EDITION

AUGUST 2-4, 2024 | HOLIDAY INN RESORT, GOA

SAVE THE DATE

AUGUST 2-4, 2024

Block your calendar for the
25th Annual CIO&Leader Conference in Goa

#IntelligentEnterprise

PRESENTING PARTNER

AMD

CO-POWERED BY PARTNERS

VERTIV. freshworks

ASSOCIATE PARTNER

Barracuda
Your journey, secured.

MEDIA PARTNER

CNBC TV18

CONCEPT BY

25 CIO&LEADER

A BRAND OF

99GROUP