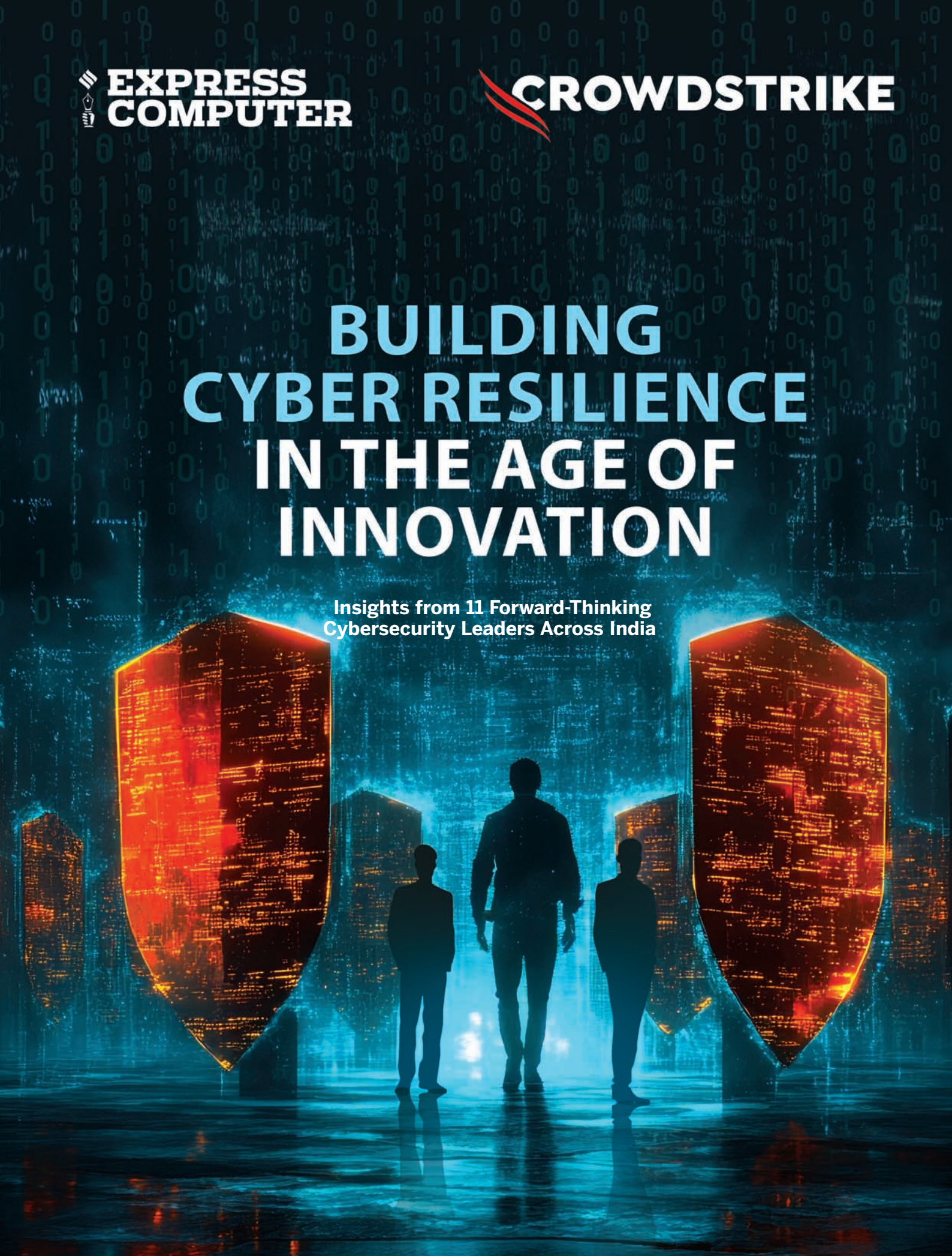
EXPRESS COMPUTER

CROWDSTRIKE

BUILDING CYBER RESILIENCE IN THE AGE OF INNOVATION

Insights from 11 Forward-Thinking Cybersecurity Leaders Across India



CONTENTS

CONTENTS

PROJECT TEAM

Editor
Srikanth RP

Consulting Senior Associate Editor
Sudipta Dev

Deputy Associate Editor
Nivedan Prakash

Assistant Editor
Salvi Mittal, Harshal Y Desai

Editorial Team
Aaratrika Talukdar,
Sayantan Mondal,
Mansi Singh,
Atreyee Chakraborty,
Bidhi Rajput,
Kopal Jain

Design Team
Pravin Temble, Rakesh Sharma

AVP & National Head - IT
Prabhas Jha

GM & Regional Head - West
Ravi Nair

GM & Regional Head - South
Durgaprasad Talithaya

Praveen Kumar Soman (Bangalore),
Deepak Patel (Mumbai),
Sunil Kumar
Navneet Negi (Delhi)

Shwetank Verma

Global CISO, Sagility

PROACTIVE PROTECTION: THE ADVANTAGE OF RISK-BASED CYBERSECURITY

Shwetank Verma champions a risk-based approach to cybersecurity - prioritising resilience over perfection. With a focus on Zero Trust, AI-driven operations, and information technology (IT) and operational technology (OT) convergence, his philosophy blends business alignment and proactive defense to build trust in a dynamic threat landscape.

By Salvi Kotian

In an exclusive interaction with Express Computer, Shwetank Verma, Global CISO at Sagility, shares his personal journey in cybersecurity leadership, the evolution of enterprise security strategies, and his views on cloud, AI-driven operations, IT-OT convergence, and the future of cyber defense.

CYBERSECURITY AS A PERSONAL MISSION

For Shwetank Verma, the shift from being an IT leader to a business-aligned CISO has been deeply personal:

"It became personal as my role evolved from overseeing IT infrastructure to becoming a strategic business leader responsible for enterprise-wide cyber risk. With cyber threats

becoming more sophisticated and breaches carrying severe reputational damage, I now stand at the intersection of technology and risk management, accountable for aligning cybersecurity strategies with overall business goals."

RISK-BASED SECURITY AND LEADERSHIP PHILOSOPHY

One of the most pivotal leadership decisions for Verma was embracing a risk-based cybersecurity approach:

"Rather than focusing on every technical vulnerability, we prioritised mission-critical assets and business priorities.

> 100% security is a myth. The real goal is resilience. My focus is on setting realistic objectives, nurturing proactive and collaborative team culture, and uniting teams around a shared mission

This not only strengthened enterprise protection but also transformed my leadership philosophy - encouraging collaboration across departments and fostering a culture of shared responsibility."

THE MYTH OF 100% SECURITY

Verma acknowledges that chasing perfection in security is unrealistic:

"100% security is a myth. The real goal is resilience. My focus is on setting realistic objectives, nurturing proactive and collaborative team culture, and uniting teams around a shared mission. It's about being confident in response, knowing

perfection isn't possible, but resilience is."

REIMAGINING ENDPOINT SECURITY

As attackers increasingly favour malware-free and identity-driven intrusions, endpoint security strategies are evolving: "The future lies in AI-powered behavioural analytics, integrated identity controls, and real-time threat intelligence, all built on a Zero Trust framework. Unified platforms that automate detection and adaptive response will be crucial to defending against sophisticated credential and malware-free attacks."

THE NEXT-GEN CLOUD SECURITY BLUEPRINT

Looking ahead, Verma outlined his two-year cloud security vision: "Cloud security will evolve into a unified, adaptive, intelligence-driven model - leveraging Zero Trust, AI and machine learning (ML), and automation to secure globally distributed ecosystems."

◆ **Zero Trust as default:** Continuous authentication, least privilege, and micro-segmentation across hybrid and multi-cloud setups

◆ **AI/ML-driven detection:** Real-time anomaly detection and automated response in dynamic cloud environments

◆ **Automated compliance:** Platforms that continuously validate posture and adapt to evolving regulations

◆ **Quantum-ready encryption:** Preparing for emerging quantum threats

TACKLING SIEM FATIGUE WITH AI

The industry-wide struggle with security information and event management (SIEM) fatigue is another concern: "The answer lies in AI-driven behavioural analytics, automation, and smarter alert prioritisation. Modern SOCs must reduce false positives, automate repetitive triage, and let human analysts focus on complexinvestigations. AI brings balance - faster response, smarter insights, and reduced burnout."

IT-OT CONVERGENCE: NEW FRONTIERS, NEW RISKS

With enterprises increasingly merging IT and OT systems, Verma highlights both challenges and opportunities: "IT-OT convergence opens up opportunities but also creates unique risks. A collaborative, tailored security strategy is essential."

◆ **Challenges:** Expanded attack surface, conflicting security priorities, patching complexities, cultural gaps, and insider threats

◆ **Opportunities:** Holistic risk management, extending IT security strengths into OT, operational efficiency, and innovation in Industry 4.0 and IoT

ROLE OF CROWDSTRIKE IN HEALTHCARE RESILIENCE

Verma also highlights the role of CrowdStrike in enabling cyber resilience, especially in healthcare: "CrowdStrike is delivering AI-driven endpoint and identity protection across thousands of devices, helping us strengthen our security

posture and align with stringent regulatory requirements. Its lightweight, automated approach is critical for resource-strapped healthcare environments, including securing Internet of Medical Things (IoMT) devices."

WHAT WILL BECOME OBSOLETE IN 5 YEARS?

Looking ahead, Shwetank Verma believes traditional defences will fade.

He predicts: "Password-based authentication and legacy signature-based antivirus will become obsolete. They'll be replaced by AI-driven adaptive authentication, next-gen endpoint detection and response (EDR) and extended detection and response (XDR), Zero Trust architectures, blockchain for identity, and cloud-native automated platforms."

As attackers increasingly favour malware-free and identity-driven intrusions, endpoint security strategies are evolving

Sanjeev Jain

CIO, Integreon

CYBERSECURITY LEADERSHIP: THE CIO'S EVOLVING ROLE

For **Sanjeev Jain**, CIO of Integreon, cybersecurity is no longer an IT checklist-it's a leadership responsibility. His approach blends resilience, Zero Trust, and collaboration with security teams to protect clients, enable growth, and build trust in an evolving digital landscape.

By Salvi Kotian

Cybersecurity is no longer just an Information Technology (IT) checklist item-it sits at the heart of how organisations protect their operations and the people who depend on them. According to Sanjeev Jain, the CIO's journey in this space is as much about leadership and empathy as it is about technology and controls.

FROM TECHNICAL CONCERN TO STRATEGIC PRIORITY

For Jain, cybersecurity evolved from being a technical responsibility to becoming a deeply personal mission. Having witnessed the impact of security incidents on teams, clients, and business reputation, he believes cybersecurity deserves a permanent seat at the leadership table. It's not merely about

configurations and controls-it's about conversations, awareness, and building a shared sense of responsibility across the organisation.

At Integreon, a strong partnership between the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) lies at the heart of this strategy. By joining forces, Jain and his CISO ensure that security by design is integrated into every project from inception. This collaboration embeds security into day-to-day operations rather than treating it as an add-on. The Information Security team regularly reviews processes and provides guidance to strengthen defences and maintain readiness against emerging threats. Together, they are building a safer, more resilient organisation where every employee plays a role in security.

> As cyber threats grow increasingly sophisticated - with challenges such as malware-free attacks and insider risks - Integreon continues to evolve its protection strategies

Jain emphasises that chasing 100% protection is like chasing a mirage. Instead, his focus remains on balancing risk, building resilience, and planning for continuity-an approach that depends on collective awareness and shared responsibility across teams.

EVOLVING PROTECTION STRATEGIES

As cyber threats grow increasingly sophisticated-with challenges such as malware-free attacks and insider risks-Integreon continues to evolve its

protection strategies. The company leverages AI-driven analytics to detect anomalous behaviour, adopts Zero Trust principles to verify every user and device, and enforces strong authentication for enhanced access control.

CLOUD AND IDENTITY: THE ROAD AHEAD

While cloud technology has accelerated business operations, Jain maintains that security and governance must remain in sync. Integreon prioritises visibility, effective policy implementation, and compliance across cloud environments. With identity management becoming central to cybersecurity, the organisation has increased its focus on Identity and Access Management (IAM) and continuous monitoring to safeguard access without compromising productivity. Key security integrations include:

- **Multi-directory protection:** CrowdStrike integrates with both on-premises and cloud environments, ensuring consistent security across hybrid infrastructures.

- **Automated threat response:** Policies are configured to automatically terminate sessions, disable accounts, or enforce step-up authentication when identity threats are detected.

- **Integrated threat hunting and investigation:** CrowdStrike tools enable efficient incident investigation, organising login events and account actions for rapid response.

To combat alert fatigue, machine learning is employed to prioritise critical events and automate

routine responses, allowing analysts to focus on high-value investigations. Jain underscores the importance of privacy measures and third-party risk assessments to safeguard client data.

CYBER RESILIENCE: MORE THAN DEFENCE

For Jain, being a CIO today means acting as an enabler of growth and innovation while ensuring organisational safety. Cyber resilience, in his view, extends beyond mere defence-it is about trust, empowerment, and strengthening the organisation every day. He believes the future of security leadership lies in blending technology with empathy and fostering a shared commitment across teams to do what's right-together.

While cloud technology has accelerated business operations, Jain maintains that security and governance must remain in sync. Integreon prioritises visibility, effective policy implementation, and compliance across cloud environments

Burgess Cooper

CEO, Adani Cybersecurity

WAR ROOMS AND WISDOM: CYBERSECURITY LEADERSHIP IN INDIA'S DIGITAL DECADE

Burgess Cooper views cybersecurity as more than technology - it is a responsibility to society. His philosophy, grounded in resilience, identity, and Zero Trust, shapes a forward-looking approach to protecting enterprises in India's rapidly evolving digital landscape.

Cybersecurity is no longer just about protecting data. In an era where digital threats can disrupt hospitals, ground flights, or even shut down power plants, the stakes are profoundly human. For Burgess Cooper, CEO of Adani Cybersecurity, this realisation marked the moment when security became personal.

"When you see the direct connection between a firewall rule and someone's life, you stop thinking about security as a technical discipline and start treating it as a responsibility to society. That moment never leaves you."

From that perspective, Cooper has shaped his leadership philosophy and security blueprint around resilience, identity, and Zero Trust - principles he believes

will define the next era of enterprise defense.

FROM PERIMETERS TO ZERO TRUST

One of the toughest yet most transformative decisions of Cooper's journey was the move from the traditional "castle-and-moat" approach to a "Zero Trust by design" architecture:

"It forced us to challenge decades of habits, re-architect networks, and rethink how trust is earned in digital interactions. Resilience isn't about defending perimeters - it's about assuming compromise and designing for recovery."

This shift not only reshaped the organisation's security posture but also influenced Cooper's leadership style, teaching him that agility and adaptability matter more than comfort.

> "Our strategy is shifting from 'protect the device' to 'verify the user, every time, everywhere.' Privilege controls, authentication, behavioural analytics are the future

BUILDING TEAMS THAT BEND WITHOUT BREAKING

Absolute protection is a myth, especially for vast enterprises. Cooper's approach is to instill resilience and confidence in his teams:

"Our job is not to create perfect security; it's to create confidence that even in the worst-case scenario, we can bend without breaking."

Through simulations, red-team

exercises, and a culture-first mindset, he fosters trust and agility across both technical and business leaders.

THE HARD TRUTH: BREACHES ARE INEVITABLE

Cooper doesn't shy away from calling out uncomfortable realities:

"Too many leaders live in denial, hoping a breach won't happen on their watch. But hope is not a strategy. Breaches are inevitable - what matters is resilience, detection, and response."

Identity as the New Perimeter
With attackers shifting toward identity-driven and malware-free intrusions, endpoint protection is evolving:

"Our strategy is shifting from 'protect the device' to 'verify the user, every time, everywhere.' Privilege controls, continuous authentication, and behavioural analytics are the future."

For large-scale enterprises, this also means building unified identity fabrics across both IT and OT environments, ensuring secure access while maintaining uptime.

TURNING THE CLOUD INTO AN ADVANTAGE

Looking ahead, Cooper views the cloud not merely as infrastructure but as an operating model:

"Security should be embedded into the DevOps pipeline - policy as code, automated guardrails, and sovereign control of sensitive workloads. The cloud can become a strategic advantage,

not just a perceived risk."

SMARTER SOCS WITH AI AND AUTOMATION

Addressing the problem of "SIEM fatigue," Cooper sees AI as a critical force multiplier:

"Traditional SIEMs bury analysts under noise. The next-gen SOC must be built on AI-driven triage, automated playbooks, and decision augmentation. Humans should focus on judgment, not log chasing."

IT-OT CONVERGENCE: THE HUMAN LAYER

In sectors like energy, ports, and logistics, IT and OT convergence is inevitable but challenging. He believes that OT is not just old IT. It has its own rhythms and fragility:
"Real convergence happens when OT engineers and IT security teams work shoulder to shoulder, with joint command structures."

FUTURE-PROOFING SECURITY

If resources were no constraint, Cooper's top priorities would be talent and threat intelligence:

"Tools can be bought; insight and instincts cannot. Building the next generation of cyber defenders, fused with real-time

intelligence, is the best investment any enterprise can make."

Looking further ahead, he predicts the end of passwords and static firewalls, to be replaced by adaptive identity assurance, micro-segmentation, and software-defined perimeters.

THE WAY FORWARD

Burgess Cooper's outlook reflects a broader shift in cybersecurity leadership: from compliance-driven checklists to resilience-driven culture. As enterprises embrace digital transformation, his message is clear - the future of security lies not in walls, but in wisdom, agility, and people.

Disclaimer: Views expressed are personal.

One of the toughest yet most transformative decisions of Cooper's journey was the move from the traditional "castle-and-moat" approach to a "Zero Trust by design" architecture

Dr. Yusuf Hashmi

Group CISO, Jubilant Bhartia Group

CYBERSECURITY: A STRATEGIC BUSINESS FUNCTION

For Jubilant Bhartia Group, cybersecurity goes beyond firewalls and compliance - it is central to business resilience. By focusing on identity, cloud governance, and automation, the company treats security as a strategic enabler of trust, continuity, and long-term competitiveness.

By Mansi Singh

When cyberattacks first made headlines, the focus was on stolen data - spreadsheets filled with names, addresses, or account numbers. For Dr. Yusuf Hashmi, Group CISO, Jubilant Bhartia Group, the defining shift came when breaches began eroding trust.

"Breaches were no longer about numbers on a spreadsheet," he reflects. "They were about people's identities, reputations, and even careers. Customers couldn't get loans. Executives resigned. Boards asked, 'Could this happen to us?' That was when cybersecurity stopped being an IT problem. It became everyone's problem."

DELIVERING BUSINESS VALUE

Traditionally, cybersecurity sat

under IT, hidden behind server patching and firewall rules. Dr. Hashmi believes this view is outdated and dangerous:

"Cybersecurity is not an IT function. It is a business function. You are protecting the business, safeguarding trust among customers, and enabling competitiveness in the industry. Leaders must give this function autonomy and recognition so it can deliver business value."

This shift means embedding security into organisational culture, compliance frameworks, and growth strategies. Security cannot operate in isolation; it must move with the rhythm of the business.

> What matters is resilience — the ability to contain, recover, and learn from incidents. You can't promise absolute protection, but you can promise recovery and survival

RESILIENCE OVER PERFECTION

One uncomfortable truth leaders often ignore: Absolute security is impossible. Attackers evolve faster than defenses, and no investment guarantees safety. Dr. Hashmi says:

"What matters is resilience - the ability to contain, recover, and learn from incidents. You can't promise absolute protection, but you can promise recovery and survival."

This philosophy reframes the CISO's role from gatekeeper to strategist, focusing not just on preventing breaches but on ensuring business continuity when they occur.

IDENTITY: THE NEW PERIMETER

As organisations move deeper into cloud and digital ecosystems, the front line of defense has shifted to identity. Dr. Hashmi explains:

"Before someone gains access to a system, they target identity - who you are, what you can access. That's why privileged access management and just-in-time rights are critical. One company cut identity risk by 40% simply by revoking always-on access. It didn't cost billions - just discipline and process."

And the challenge goes beyond human users. With AI agents, bots, and automated systems proliferating, machine identities are becoming a major vulnerability.

He warns, "Managing machine identities will be one of the biggest cybersecurity challenges in the years ahead."

CLOUD SECURITY: FROM PERIMETER TO POLICY

Cloud adoption is no longer optional - it is essential for scalability and agility. But it has also transformed the threat landscape.

Dr. Hashmi says:

"In cloud environments, identity becomes the backbone of security. It's about ensuring the right person has the right access to the right resource at the right time."

Identity governance, access management, and privileged controls now form the foundation of cloud-native security.

AI AND AUTOMATION

Security operations centres are drowning in alerts, most of them false positives. This is where AI and automation bring relief. Dr. Hashmi notes: "Analysts often say they are drowning in alerts. AI-driven SOCs can filter noise, detect anomalies, and even automate responses."

A WORD OF CAUTION

"Attackers are using AI too - deepfake voice calls, adaptive malware, compelling phishing campaigns. AI is not a silver bullet. It's a force multiplier that clears the noise so humans can focus on high-risk, complex analysis."

UNLIMITED BUDGET, CLEAR PRIORITIES

If the budget was unlimited, Dr. Hashmi's investments would not begin with tools. Instead, he highlights three priorities: talent, automation, and resilience.

"You need skilled people who can think strategically. You need automation to respond at machine speed. And you need resilience, because incidents are inevitable, but collapse is not."

He cites global leaders who combine massive investments with realistic strategies - not chasing perfect protection but building organisations that can withstand and adapt to digital shocks.

IT-OT CONVERGENCE: A NEW FRONTIER

With Industry 4.0, the boundary between IT systems and operational technology (OT) like pipelines, plants, and power grids is vanishing. Dr. Hashmi says:

"For decades, IT focused on data while OT focused on physical systems. Now they are colliding. In IT, downtime means financial loss. In OT, it can mean hazards to human safety and the environment."

EVOLUTION, NOT OBSOLESCENCE

Looking five years ahead, Dr. Hashmi predicts not the disappearance of existing tools but their transformation. Firewalls and antivirus will remain but must evolve. Meanwhile, security orchestration, automation, and response (SOAR) platforms may give way to AI-driven automation, and SIEM systems may shift toward data lakes for broader, contextual analytics.

Traditionally, cybersecurity sat under IT, hidden behind server patching and firewall rules. Dr. Hashmi believes this view is outdated and dangerous

Harsh Kedia

Country Head - UK and Head of IT Procurement and Vendor Management, Fusion CX

CYBERSECURITY AS A BUSINESS IMPERATIVE: FOCUS ON BUILDING RESILIENCE

At Fusion CX, cybersecurity is treated as a business imperative. With resilience, trust, and compliance at its core, the company embeds security across strategy, operations, and partnerships - ensuring stronger protection, faster recovery, and confidence for clients worldwide.

By Salvi Kotian

For Harsh Kedia, cybersecurity is no longer just a technology investment - it is a business imperative. As the Country Head - United Kingdom and Head of IT Procurement and Vendor Management at Fusion CX, Kedia believes that trust, compliance, and resilience form the foundation of a secure digital enterprise:

"We must make sure that we get the best out of our suppliers and partners, with clearly defined roles and responsibilities that make them accountable. A small mistake at their end could put a large business at risk."

That statement isn't hypothetical. He recalls a specific incident where a

vendor's misconfigured sales platform system led to thousands of illegitimate calls being made from Fusion CX's network:

"That small misconfiguration became very personal. It showed me how cybersecurity risks can't be treated as someone else's problem."

RESILIENCE OVER PERFECTION

Kedia is pragmatic about the limits of protection:

"No system in this world is perfect. Rather than chasing 100% protection, which is impossible, organisations are shifting focus towards resilience - faster detection and faster recovery."

> "We have recently partnered with CrowdStrike to implement their EDR solutions and managed detection and response (MDR) services

Quarterly reviews, both internal and external, are central to his approach. The focus, he adds, is no longer only on blocking threats but on how quickly enterprises can recover when breaches occur.

STRENGTHENING THE SECURITY STACK

Fusion CX has been investing heavily in endpoint security, with partnerships that bring cutting-edge AI-driven capabilities.

"We have recently partnered

with CrowdStrike to implement their EDR solutions and managed detection and response (MDR) services. Their expertise helps us quickly detect and mitigate threats. Along with robust firewalls, this ensures our environment is well-guarded."

On the cloud security front, Fusion CX operates with a hybrid model, guided by cost efficiency and compliance. For cloud workloads across Azure and AWS, Kedia insists on strong multifactor authentication, limited administrator rights, and regular audit log reviews. He adds, "We also review compliance reports and data residency norms regularly to ensure alignment with global standards."

AI AND MODERN DETECTION

As organisations face "SIEM fatigue," Kedia sees the rise of AI-driven detection and response as a necessary evolution:

"AI-driven SIEM reduces noise for analytics and prioritises real threats. It's about filtering signal from noise and responding effectively."

IT AND OT CONVERGENCE

Fusion CX is also preparing for the growing convergence of IT and OT systems:

"Through smart buildings, solar panels, and connected physical systems, we are integrating energy savings

with IT cores. This convergence will demand a stronger cybersecurity posture."

CROWDSTRIKE PARTNERSHIP: A FOUNDATION OF TRUST

Harsh Kedia emphasises that their partnership with CrowdStrike has been pivotal in embedding cybersecurity into the core of Fusion CX operations.

"Security is no longer just a technology issue - it is embedded into our business. With CrowdStrike's AI-driven platform, we can scale securely, remain compliant, and deliver confidence to our global clients. The foundation will always be trust and compliance."

For cloud workloads across Azure and AWS, Kedia insists on strong multifactor authentication, limited administrator rights, and regular audit log reviews

Mukul Jain

CTO, Axis Max Life Insurance

CYBERSECURITY IS NOT ABOUT PERFECTION, IT'S ABOUT ACCOUNTABILITY

Mukul Jain believes cybersecurity is not about perfection but about accountability. Anchored in Zero Trust, cloud-first security, and AI-driven detection, his approach blends resilience and responsibility to safeguard trust in an increasingly digital insurance landscape.

By Salvi Kotian

Cybersecurity is not about eliminating risk - it's about building resilience, trust, and accountability," says Mukul Jain, Chief Technology Officer, Axis Max Life Insurance Ltd. His perspective reflects both realism and conviction, shaped by years of navigating the evolving threat landscape.

RETHINKING ENDPOINT PROTECTION

Highlighting how attackers have shifted gears, Jain says, "They're moving away from traditional, easily detectable malware and toward malware-free, identity-driven attacks - stealing credentials, performing lateral movement, and abusing legitimate system tools."

To combat this, Axis Max Life has deployed a market-leading

XDR solution powered by behavioural analytics and AI/ML. Integrated with industry-best SIEM and SOAR platforms, this approach centralizes data, enables automated playbooks, and strengthens the Zero Trust principle by linking endpoints tightly with identity protection. He emphasizes: "Customer privacy and data security must remain at the forefront of every interaction."

A CLOUD-FIRST BLUEPRINT

As cloud workloads accelerate, Axis Max Life is moving toward a cloud-native security architecture. Security is embedded from the earliest stages through DevSecOps, automated code scanning, secrets detection, and container hardening.

> "Every enterprise will face a breach at some point. Accepting this is not failure — it is maturity

The company is investing in ransomware protection, immutable backups, disaster recovery automation, and periodic recovery testing.

"We're focused on being secure by design, compliant by default, and resilient by architecture," Jain explains. This includes strong encryption, data loss prevention (DLP), RegTech for compliance automation, AI/ML-driven anomaly detection, and a progressive shift to multi-cloud environments aligned with IRDAI's evolving requirements.

IDENTITY AS THE NEW PERIMETER

"Identity is both the front door and a vulnerability," Jain says. Axis Max Life has anchored identity and access management (IAM), identity threat detection and response (ITDR), and access governance in a cloud-first, Zero Trust framework. Adaptive, context-aware controls ensure that no user, device, or API is trusted by default. Advanced ML models detect anomalies such as credential misuse or privilege escalation, while automated provisioning and least-privilege enforcement minimise insider risks. He notes, "Identity is evolving from being a vulnerability to becoming a growth enabler."

TACKLING SIEM FATIGUE WITH AI

Many organisations today struggle with SIEM fatigue. Jain's response is clear: "We've built an AI-driven, adaptive SOC to cut through the noise." By prioritising threats based on risk and behaviour, Axis Max Life's security teams can focus on subtle deviations that traditional systems miss. Automated playbooks allow for rapid containment - revoking credentials, isolating endpoints, or stopping lateral movement - so teams spend more time on proactive threat hunting. "A modern SOC must evolve into an intelligent, learning ecosystem where AI amplifies human judgment," he says.

THE FUTURE SECURITY STACK

Looking ahead, Jain predicts the decline of perimeter-based defenses and static, signature-driven antivirus. Password-only authentication will also give way to stronger methods like passwordless logins, MFA, device trust scoring, and continuous identity validation. Legacy, fragmented tools will be replaced by unified, AI-powered platforms that integrate detection, response, and automation. "Cloud-native models and Zero Trust adoption are the future of adaptive and resilient security," he asserts.

A DEFINING LEADERSHIP MOMENT

One of Jain's formative

leadership decisions was during the launching of a new digital platform. Under immense pressure to go live, he made the call to delay the launch until security could be embedded end-to-end. "It wasn't popular, but it sent a strong message: Security isn't just IT's responsibility - it's foundational to trust and business continuity," he recalls. That moment reshaped his leadership philosophy, anchoring security as a design principle rather than an afterthought.

LEADING WITH ACCOUNTABILITY

Jain is candid about the limitations of cybersecurity: "100% protection is not possible - but 100% accountability is." His leadership rests on three pillars:

- **Culture of shared responsibility:** Where every employee, from developer to architect, owns security
- **Preparedness at every level:** Through DevSecOps, VA/PT, red teaming, and rehearsed incident playbooks
- **Empathy and psychological safety:** Ensuring mistakes become opportunities for learning, not blame

THE HARD TRUTH

Perhaps the most sobering statement Jain shares is this: "Every enterprise will face a breach at some point. Accepting this is not failure - it is maturity." By acknowledging inevitability, organisations can shift from prevention to resilience, focusing on rapid detection, recovery, and customer trust. For Axis Max Life, this is especially vital given the long-term relationships it builds with policyholders.

INVESTING FOR THE FUTURE

If given five times the current budget, Mukul Jain would accelerate investments in AI-driven detection, self-healing capabilities, comprehensive Zero Trust infrastructure, and continuous red teaming. He would also scale partnerships in threat intelligence and invest deeply in talent upskilling. He affirms:

"The goal is not to reinvent but to accelerate responsibly."

Sumeet Khokhani

Senior VP and Global CISO, WNS

FROM TRUST TO TRANSFORMATION: HOW WNS IS REDEFINING CYBERSECURITY IN THE AI ERA

Sumeet Khokhani views cybersecurity as a mission to safeguard trust, not just technology. Anchored in AI, identity protection, and risk translation, his approach redefines security as a business enabler in today's digital era.

By Salvi Kotian

For Sumeet Khokhani, Senior VP and Global CISO at WNS, cybersecurity stopped being about ticking boxes the day he witnessed a misconfigured cloud storage bucket expose sensitive data. The real fear wasn't regulatory fines or negative headlines - it was the risk of losing trust that had taken decades to build. He recalls:

"That was the moment security became personal for me. Every control I design, every risk I assess starts with one question: Will this continue to preserve the trust that the business has earned over time?"

This philosophy has guided Khokhani throughout his 23-year career, transforming his approach from traditional security management to a

mission-driven pursuit of trust and resilience. For him, security is about protecting relationships, reputation, and business continuity - not just technology.

SECURITY AS A BUSINESS ENABLER

Khokhani believes cybersecurity is not just a technical function but a business enabler:

"The most transformative decisions are rarely purely technical. Security is about translating complexity into a language executives can understand. This shifted my role from being a security expert to a risk translator, helping teams see security as a shared responsibility."

> *//*
>
> Not everything needs equal protection. Security leaders must understand what matters most to the business and articulate potential technical risks as business risk or financial impact

He emphasizes contextual risk scoring and aligning technical findings with business impact to ensure that security investments deliver real value.

IDENTITY, AI, AND THE NEW PERIMETER

With threats evolving toward malware-free and identity-driven attacks, Khokhani stresses the importance of behaviour-based detection and AI-powered security:

"Traditional endpoint solutions have blind spots against fileless attacks and credential misuse. AI-driven anomaly detection

helps identify deviations, like lateral movement or unusual access patterns, before they cause damage."

Identity has become the new perimeter. Protecting it requires integrating identity and access management, privilege access management, continuous authentication, and hardened core systems.

"Zero Trust enforcement, conditional access policies, device posture checks, and micro-segmentation are crucial to contain threats - even if credentials are compromised."

FROM REACTIVE TO PROACTIVE DEFENCE

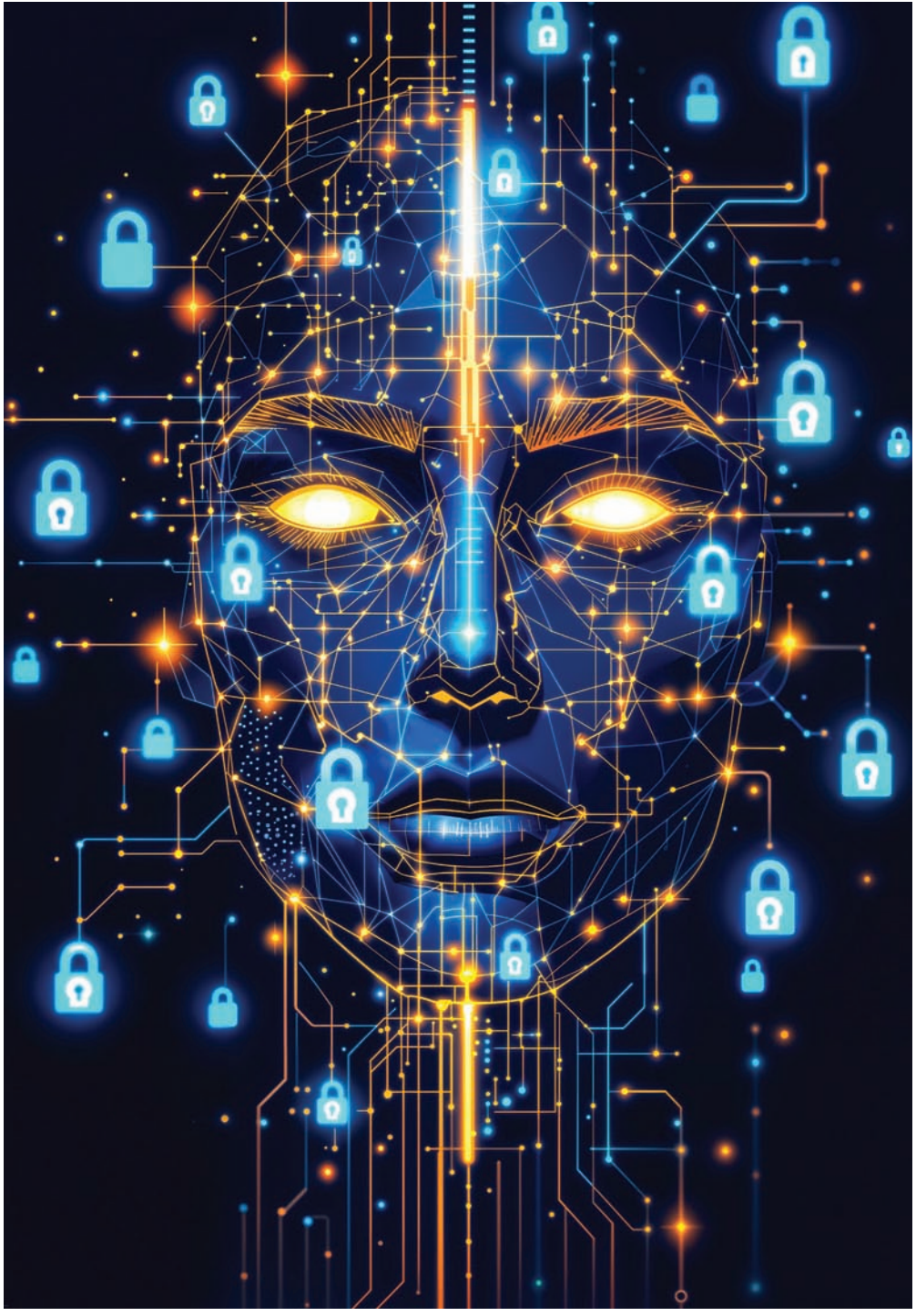
Khokhani champions a proactive security posture, leveraging AI for faster threat detection and response:

"It's not just about prevention anymore - it's about resilience. AI-powered solutions enable faster triage, quicker detection, and rapid response, helping organisations stay ahead of dynamic threats."

PRIORITISING RISK IN BUSINESS TERMS

A key challenge for security leaders is translating technical risk into business impact. Khokhani uses cyber risk quantification to map risk scenarios to business processes and estimate potential financial losses.

"We ask: What if this risk materialises? What is the financial impact? Translating technical risk into business risk creates a shared language with leadership and drives smarter investment decisions."



THE FUTURE OF CYBERSECURITY

Khokhani predicts the phasing out of legacy security systems in favour of unified detection and response platforms:

"Legacy architectures struggle with rigid data ingestion, alert fatigue, and delayed detection. The future is AI-native platforms that unify endpoints, cloud workloads, and identity to enable faster, contextual, business-driven responses." He also foresees continuous threat exposure management (CTEM) becoming central, prioritising actions based on business context rather than technical alerts alone.

THE EVOLVING ROLE OF THE CISO

For Khokhani, the modern security leader is no longer a gatekeeper but a strategic business enabler embedded in organisational strategy.
"Not everything needs equal protection. Security leaders must understand what matters most to the business and articulate potential technical risks as business risk or financial impact. This shared understanding ensures alignment and support from leadership." Through his focus on trust, contextual intelligence, and resilience, Sumeet Khokhani illustrates how cybersecurity is evolving from a technical function into a strategic driver of business value in the age of AI and identity-driven threats.

> It's not just about prevention anymore - it's about resilience. AI-powered solutions enable faster triage, quicker detection, and rapid response, helping organisations stay ahead of dynamic threats

Komal Vora

CISO, Equifax Credit Information Pvt. Ltd.

DEFENDING TRUST IN A DIGITAL-FIRST ERA

Over a 25-year career, **Komal Vora** has built cybersecurity leadership through learning, collaboration, and foresight. With resilience and trust as anchors, she drives proactive strategies to protect financial enterprises in a shifting threat landscape.

By Salvi Kotian

Cybersecurity today is less about tools and more about trust, resilience, and foresight. For Komal Vora, CISO at Equifax Credit Information Pvt. Ltd., the journey to information security wasn't a single turning point but a series of deliberate choices made across a 25-year career:

"I started as a developer, moved into system administration, then governance, audits, consulting, and finally into information security. At every stage, I picked and chose areas where I could learn, upskill, and add value."

Her career has spanned Indian multinational banks, consulting giants, and now the credit bureau sector, always with the focus on strengthening organisations against evolving

cyber risks.

STRATEGIC ANCHORS: CONTINUOUS LEARNING AND COLLABORATION

In an industry where the threat landscape evolves daily, Vora emphasizes two constants - upgrading herself and building peer networks.

◆**Annual learning goal:** "Every year, I make it a point to add one new certification or technology skill. Without that discipline, we risk becoming redundant."

◆ **Peer exchange:** She actively engages with industry groups, both sharing her practices and absorbing insights from others. Her leadership approach extends to nurturing her teams. By encouraging certifications and knowledge-sharing within the workforce, she sees herself not just as a protector of systems but as a contributor to careers.

> *//*
>
> The weakest link is often the user. Centralised monitoring helps us detect anomalies before they become disasters

BUILDING ORGANISATIONAL RESILIENCE

Vora believes resilience isn't built overnight - it is cultivated through transparency, proactivity, and collaboration:

"I never wait for a regulator or internal audit to tell me where the gaps are. I proactively study the environment, identify risks, and bridge silos."

She highlights a persistent challenge in large enterprises - departments working in silos:

"This lack of collaboration is one of the biggest risks. If attackers across continents can coordinate, why can't teams within the same organisation?"

Her philosophy is to lead by example - whether it's initiating tough conversations, resolving conflicts without ego, or fostering a culture of openness.

TACKLING MODERN THREATS: IDENTITY, CLOUD, AND AI

From endpoint attacks to cloud security, Vora outlines the strategies that financial enterprises are adopting:

◆ **Identity defense:** Tools like privileged access management (e.g., CyberArk), single sign-on, and quarterly entitlement reviews are essential. She points out, "The weakest link is often the user. Centralised monitoring helps us detect anomalies before they become disasters."

◆ **Cloud adoption:** With financial services being RBI-regulated, she emphasizes a conservative and well-planned approach. "Cloud visibility is still gray, which is why configuration hardening, periodic reviews, and continuous SOC monitoring are non-negotiable."

◆ **AI in cybersecurity:** Vora sees AI as both a risk and a necessity. "Attackers are already using AI. If we don't, we fall behind. The real advantage lies in filtering out false positives and enabling real-time prioritisation. But every adoption must be preceded by impact analysis and risk assessment."

THE FUTURE: FROM OBSOLESCENCE TO RENEWAL

With decades in the field, Vora has seen countless technologies rise and fall. She believes obsolescence is inevitable - but it doesn't have to be disruptive:"Research and development must be embedded within security teams. If we continuously evaluate, assess risks, and plan alternatives, no new technology will catch us off guard."

For her, security leadership is less about chasing every trend and more about aligning technology choices with an organisation's strategic goals, while always preparing for what comes next.

SECURING CRITICAL INFRASTRUCTURE

Operational technology (OT), data centres, and disaster recovery sites are what she calls "the heart of an organisation." These must be protected with layered security, continuous

reviews, and regulatory audits. She warns, "If the heart fails, the whole organisation's reputation is at risk."

A CONTINUOUS JOURNEY

Reflecting on her career, Komal Vora frames cybersecurity not as a job, but as a journey of constant upgrading, collaboration, and responsibility:

"At the end of the day, it's about safeguarding trust. And trust is not built in a day - it's nurtured through consistency, resilience, and foresight."

Disclaimer: The views and opinions expressed in this interview are solely those of Komal Vora in her personal capacity and do not represent the views of Equifax Credit Information Pvt. Ltd.

Operational technology (OT), data centres, and disaster recovery sites are what she calls "the heart of an organisation." These must be protected with layered security, continuous reviews, and regulatory audits

Avinash Tiwari

Global CISO, Pidilite Industries Limited

NECESSITY OF HUMAN-CENTRIC, PEOPLE-FIRST CYBERSECURITY

Avinash Tiwari, Global CISO at Pidilite Industries, champions a people-first cybersecurity approach rooted in trust, empathy, and collaboration. From zero-trust adoption to AI-driven defences, he emphasizes resilience, transparency, and empowering individuals as the foundation for sustainable security leadership.

By Aaratrika Talukdar

In today's hyperconnected world, cybersecurity is no longer about merely protecting systems and data- it's about safeguarding people, operations, and trust. For Avinash Tiwari, Global CISO at Pidilite Industries Limited, security leadership is deeply personal. From steering the company's transition to a zero-trust architecture to navigating the aftermath of a spear-phishing attack, his journey reflects how empathy, transparency, and human-centricity form the backbone of modern cybersecurity.

WHEN CYBERSECURITY BECOMES PERSONAL

The turning point in Tiwari's leadership journey came during a targeted phishing attack that almost disrupted Pidilite's

supply chain operations. The incident not only threatened revenue but also created anxiety among teams on the factory floor and within warehouses.

"Witnessing firsthand how a cyberattack could affect real people-their work, their confidence, their livelihoods-changed everything for me," says Tiwari. "Cybersecurity isn't just about protecting data; it's about safeguarding trust and ensuring business continuity for those who depend on us."

That experience reshaped his philosophy: cybersecurity must be embedded into everyday culture. At Pidilite, awareness and empathy go hand in hand with technology. "When teams see security through a human lens," he adds, "they begin to understand their role in protecting not just systems, but people."

> "
>
> Witnessing firsthand how a cyberattack could affect real people - their work, their confidence, their livelihoods - changed everything for me

TRANSFORMING RISK THROUGH ZERO TRUST

One of the most transformative decisions under Tiwari's leadership was migrating Pidilite's critical workloads to a zero-trust architecture. The shift required dismantling legacy systems, enforcing continuous verification, and fostering a new level of transparency across departments.

"It wasn't just an IT project-it was an organisational mindset

shift," Tiwari explains. "We made sure everyone, from IT to HR, understood their role in maintaining secure operations."

The result was more than improved threat resilience. It empowered employees to take proactive ownership of cybersecurity, reinforcing a culture of collective responsibility and adaptability.

BUILDING RESILIENCE IN AN UNCERTAIN LANDSCAPE

In a world where perfection in cybersecurity is impossible, Tiwari's leadership centres on resilience, trust, and agility. His teams are encouraged to embrace open communication-discussing vulnerabilities, sharing lessons from setbacks, and celebrating progress.

"Resilience isn't built on fear of failure; it's built on learning and collaboration," he says. Regular incident-response simulations help teams stay prepared for unexpected scenarios, while continuous training builds confidence and competence.

"Every incident we overcome strengthens our collective resolve," Tiwari notes. "Our goal isn't to avoid uncertainty, but to be ready for it-together."

IDENTITY AND ENDPOINT SECURITY: THE NEW FRONTLINE

With the rise of identity-driven and malware-free intrusions, Tiwari views identity as the new perimeter. Pidilite's defences combine multi-factor authentication, AI-driven anomaly detection, and behaviour-based endpoint

monitoring to identify suspicious activity before it escalates.

"Each login represents a real person, and every device is a gateway to their work," he explains. "By treating identity as the core of our security framework, we ensure that every protection measure ultimately protects people."

Regular audits, strict access controls, and continuous awareness training underpin this strategy, making security a shared responsibility across the organisation.

A CLOUD BLUEPRINT BUILT ON TRUST

As cloud workloads expand, Tiwari envisions a future where automation and human intelligence coexist. Over the next two years, Pidilite's cloud security blueprint will focus on automated governance, continuous monitoring, and infrastructure-as-code for consistent, scalable protection.

"Our aim is to give teams clarity, not clutter," he says. "Automation helps us stay proactive, freeing our people to

focus on innovation rather than firefighting alerts."
Training and partnerships are equally critical. "Cloud security isn't just a compliance checklist-it's about building trust with partners, empowering teams, and ensuring that everyone can sleep peacefully at night."

BRIDGING IT AND OT SECURITY

Recognising the interconnected nature of IT and operational technology (OT) environments, Tiwari is reinforcing Identity and Access Management (IAM) and Identity Threat Detection and Response (ITDR) with role-based access, multi-factor authentication, and strict governance frameworks.

"Cross-training between IT and OT teams is crucial," he emphasises. "

AI AND AUTOMATION: REDEFINING SECURITY OPERATIONS

Addressing "SIEM fatigue"-the overwhelming flood of alerts that strain SOC teams-Tiwari's team is turning to AI, machine learning, and advanced analytics. "Automation helps us cut through the noise," he explains. "We use AI to prioritise the most critical alerts, detect subtle threat patterns, and automate triage tasks. This allows our analysts to focus on what really matters-strategic, high-impact response." Behavioural analytics and user-entity monitoring have further enhanced visibility, enabling faster and more precise threat detection.

LOOKING AHEAD: THE NEXT SECURITY FRONTIER

Tiwari believes that traditional, perimeter-based firewalls and signature-based antivirus solutions are nearing obsolescence. "Static controls simply can't keep up with adaptive, AI-powered threats," he notes. He sees the rise of AI-driven detection systems, zero-trust frameworks, adaptive authentication, and rapid response. "The future of cybersecurity," he concludes, "belongs to dynamic, integrated frameworks that balance technology with empathy. It's about protecting data, yes-but ultimately, it's about protecting people."

Srikumar Ramanathan

CSO, Mphasis

SECURITY AS A WAY OF THINKING: RISK, RESILIENCE, AND THE HUMAN FACTOR

Cybersecurity is about managing - not eliminating - risk, says **Srikumar Ramanathan**. Advocating Zero Trust, layered defenses, AI-driven monitoring, and cultural awareness, he emphasizes embedding security into every code, system, and process while preparing for inevitable incidents and ensuring business continuity.

By Salvi Kotian

For Srikumar Ramanathan, Chief Solutions Officer (CSO) at Mphasis, security is not just a professional mandate, it's been a way of thinking throughout his career. Before joining Mphasis, Ramanathan served as CIO for a leading Asian bank, overseeing operations across 14 countries. That experience, coupled with his work in Singapore's trading exchanges, ingrained in him a deep awareness that cybersecurity is not an afterthought but the foundation of trust in a digital economy. He recalls:

"As financial services moved from open-outcry trading floors to electronic trading systems, I realised the same rigor we had for physical security had to be translated into the digital world. Since then, security has been

drilled into my way of thinking from day one."

MANAGING RISK, NOT ELIMINATING IT

One of Ramanathan's core beliefs is that absolute security is a myth. "If you stop doing business, you can be 100% safe. But the moment you enable transactions, risk comes in," he explains. Instead of chasing the illusion of total protection, his focus is on risk management - ensuring resilience, layered defenses, and preparedness for inevitable incidents.
He outlines a three-fold approach:

◆ **Zero Trust from the start:** "You can't just build a moat anymore. Security has to be integrated from the ground up, starting with Zero Trust policies."

> //
>
> Cybersecurity is no longer just about enterprises. It extends to households — our parents, children, even grandparents are targets. Awareness must go beyond the workplace

◆ **Layered defence:** From identity management to monitoring, multiple security layers reduce exposure.
◆ **Incident preparedness and recovery:** "You must assume breaches will happen. What matters is how you respond and ensure business continuity."

BEYOND ANTIVIRUS: RETHINKING ENDPOINT SECURITY

With endpoints expanding in definition, Ramanathan stresses a shift from traditional tools to AI- and behaviour-

driven monitoring:

"The real challenge is alert fatigue. Too many false positives make people ignore real threats. That's where automation and machine learning play a huge role - filtering noise and surfacing only genuine alerts."

He points to advanced frameworks like EDR/XDR and emphasizes the importance of continuous updates and behavioural analysis. Yet, he cautions that technology alone is not enough:

"The human in the loop is always the weakest link. We must address that too."

EMBEDDING SECURITY INTO DEVELOPMENT

Ramanathan believes the future lies in bottom-up security integration, where every layer of infrastructure and every line of code is designed with security in mind. He cites Mphasis' own open-source tools like CSNag, which helps developers identify vulnerabilities as they code:

"Security cannot be an afterthought. It needs to be embedded into the DNA of applications, cloud architectures, and processes."

NAVIGATING IT-OT CONVERGENCE

Ramanathan observes a blurring of boundaries between IT and OT:

"Just as DevOps emerged to bridge development and operations, IT and OT are converging. We're training teams across domains to ensure tighter synergy."

IF THE BUDGET WAS NOT A CONSTRAINT

Asked what he would do with five times his current budget, Ramanathan dismisses the idea of splurging on specific tools. Instead, he would invest in organisation-wide security awareness and culture:

"Every code, every interaction with the cloud, every infrastructure decision must be security-first. If I had unlimited funds, I'd spend it ensuring security is built into the mindset of every employee, not just into systems."

THE HUMAN SIDE OF SECURITY

Despite dealing with high-stakes enterprise risk, Ramanathan never loses sight of the human impact. He points to the rise of home-based scams and phishing as a pressing concern:

"Cybersecurity is no longer just about enterprises. It extends to households - our parents, children, even grandparents are targets. Awareness must go beyond the workplace."

And when it comes to unwinding after a day of battling digital threats? Ramanathan prefers the simplicity of reading physical books:

"Unlike eBooks, a real book takes you away from notifications and alerts. It's my way of disconnecting."

As for his secret productivity hack, he admits he relies on AI and large language models:

"They're like hydraulics lifting a heavy load - if you don't use them, you're missing out."

From his early days in financial services to leading security strategy at Mphasis, Srikumar Ramanathan's philosophy is clear: Cybersecurity is not about eliminating risk but about managing it intelligently, embedding it deeply, and preparing relentlessly.

In an age where digital boundaries blur and threats multiply, his message resonates: The future of cybersecurity lies as much in mindset and culture as in technology.

Ramanathan believes the future lies in bottom-up security integration, where every layer ofinfrastructure and every line of code is designed with security in mind

Gowdhaman Jothilingam

Global CISO and Head of IT, LatentView Analytics

SPEAKING THE LANGUAGE OF BUSINESS: REDEFINING CYBERSECURITY LEADERSHIP

Gowdhaman Jothilingam champions a business-first approach to cybersecurity, where quantified risks, identity-first strategies, AI-driven defense, and continuous monitoring converge to build resilience and empower enterprises in today's evolving digital threat landscape.

By Salvi Kotian

In today's volatile threat landscape, fear-driven cybersecurity messaging is no longer enough. For Gowdhaman Jothilingam, Global CISO and Head of Information Technology at LatentView Analytics, the key to leadership lies in speaking the language business leaders understand - risk in financial terms:

"As leaders, we have to raise our hands and call out problems without hesitation. CISOs often tend to use fear as a strategy, but I encourage peers to be realistic. Don't just say if you don't do this, something bad will happen. Instead, quantify the cyber risk, correlate it to dollar value, and present that to top management. When you speak in business language, you grab their attention."

This approach, he stresses, not only makes conversations more transparent but also strengthens trust between security leaders and boards:

"If you're vocal, clear, and realistic about the impact on business, leadership will help you. That's how you secure budgets and alignment for your security roadmap."

IDENTITY FIRST: THE NEW SECURITY BLUEPRINT

As workloads shift to the cloud and attackers exploit identity as both a front door and a vulnerability, Jothilingam emphasizes the urgency of adopting an identity-first approach:

> Cybersecurity must evolve from reactive defense to a proactive, risk-based approach. Continuous benchmarking, monitoring, and alerting make that possible

"Companies that prioritize identity security will lead the way. Identity-first helps you understand who has access, what level they have, and how they're using it. But we also need to go further - incorporating identity governance, detection, and response (IGDR) and automation."

At LatentView, his team is exploring context-aware access and strengthening defenses with Zero Trust architectures:

"Adding context-aware intelligence helps detect, contain, and recover from malicious activity faster. We've already implemented top-tier Zero Trust frameworks, and the

results in identity protection have been significant."

AI-DRIVEN ENDPOINT DEFENSE

With attackers moving beyond malware to stealthy, identity-driven intrusions, traditional endpoint defense is under pressure. Jothilingam sees AI as the differentiator:

"When you look at logs, the challenge is separating the signal from the noise. The only way forward is to use AI and orchestration platforms to automate detection. This helps security teams focus on real threats instead of drowning in fatigue."

By combining AI-enabled threat hunting with orchestrated SOAR platforms, his team ensures that analysts can quickly detect, respond, and contain risks - without getting lost in endless alerts.

BUILDING FOR IMPACT: WHERE INVESTMENTS MATTER

If he had five times the budget, Jothilingam knows exactly where he would invest. His top three priorities:

◆ **Unified visibility:** "We need a single environment to monitor endpoints, cloud, and critical systems. Only with unified visibility can you measure and manage risks effectively."

◆ **People and skills:** "Technology alone can't protect us. Building skilled, talented teams that can handle critical situations is crucial."

◆ **Continuous monitoring and red-blue-purple exercises:** "Cybersecurity must evolve from reactive defense to a proactive, risk-based approach. Continuous benchmarking, monitoring, and alerting make that possible."

PARTNERSHIPS THAT MATTER

For endpoint security, Jothilingam acknowledges the role of strategic partners:

"When we want to protect critical environments, we look for strong players that can detect, contain, and eradicate threats quickly. CrowdStrike, for example, has been instrumental in monitoring and protecting our environments, not just from endpoints but across

multiple layers."

THE WAY FORWARD

For Gowdhaman Jothilingam, cybersecurity leadership isn't about instilling fear - it's about clarity, quantification, and foresight. By translating risks into business terms, championing identity-first security, harnessing AI, and investing in people, he is helping LatentView Analytics stay ahead in an era where threats evolve faster than ever:

"Ultimately, we must move from being reactive to proactive. When we quantify risk, speak in business language, and focus on resilience, we create cybersecurity strategies that not only protect but also empower the business."

As workloads shift to the cloud and attackers exploit identity as both a front door and a vulnerability, Jothilingam emphasizes the urgency of adopting an identity-first approach

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk - endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/
Follow us: Blog | X | LinkedIn | Facebook | Instagram
Start a free trial today: https://www.crowdstrike.com/free-trial-guide/