F5 regional CXO roundtable series

Bangalore edition

Building unbreakable cyber resilience

Key takeaways | December 13, 2024

Lessons from the Bangalore CXO roundtable

An actionable path for building unbreakable cyber resilience

Executive summary

The F5 regional CXO roundtable in Bangalore convened senior technology, security, and risk executives across industries to explore what it takes to operationalize cyber resilience. With threat vectors expanding across supply chains, insider access, and cloud environments, the conversation focused on shifting from reactive defence to resilient by design systems that anticipate failure and recover fast.

What stood out was a shift in focus from prevention to recovery. Most leaders accepted that breaches will happen. The real question is how fast your enterprise bounce can back and how much impact can be absorbed. Insider threats topped the list of likely attack vectors followed closely by supply chain exposures. AI was part of the conversation too but cautiously. It is being used but not blindly adopted. Trust, explainability, and value still matter more than novelty.

Live polling during the session revealed where organizations are aligned and where they are still catching up:

- **Insider threats take center stage:** Nearly half the participants identified insider threats as the most likely source of the next major breach. This marks a clear shift in perception as organizations move away from focusing solely on external actors and recognize that the real vulnerability may be within their own perimeter.
- **Operational gaps revealed by vendor failures:** The CrowdStrike outage was cited as the incident that exposed the highest level of unpreparedness. The takeaway was clear that resilience plans that do not account for third-party failure are incomplete and visibility across the extended ecosystem remains patchy.
- **Boards want financial risk not technical metrics:** What mattered most was not who had the best tech stack but who could act fast, recover faster, and knew exactly who is accountable when something goes wrong. Traditional metrics like SLAs and incident counts took a back seat highlighting the need to align security communication with business outcomes.

- **AI adoption is cautious and measured:** While there is growing interest in AI for cybersecurity, most organizations are taking a pragmatic approach deploying it selectively for detection and analytics. Concerns around cost, explainability, and oversight continue to limit broader rollout.

To support this shift, the group outlined a structured approach around five focus areas:

1. **Strategic imperatives:** Reframe cyber resilience as a core business function not a security afterthought. Key imperatives included addressing insider threats as a baseline assumption, architecting resilience into the supply chain, quantifying cyber risk for board-level decisions, preparing for failure over prevention, and applying AI only where its value is proven and measurable.

2. **Critical challenges:** Participants cited structural blockers such as fragmented accountability across security and IT, limited visibility into third-party risk, reactive budgeting, underutilized threat intelligence sharing, and board-level communication gaps as major inhibitors to resilience at scale.

3. **Implementation plan:** Build resilience into systems from the start with secure by design infrastructure, modular architecture, and layered observability. Emphasis was placed on failure simulations, tiered recovery protocols, and hardening both internal and vendor environments.

4. **Success metrics:** Track the organization's ability to detect, contain, and recover from disruption. Key metrics included time to recovery (MTTR), uptime for Tier 1 systems, simulation success rates, telemetry coverage, and vendor resilience readiness.

5. **Next steps:** Elevate resilience to a board-level priority, institutionalize a cross-functional governance model, simulate extended failure scenarios across the value chain, and build team readiness with role-specific recovery protocols not just awareness campaigns.

This session reaffirmed that leading organizations are not defined by how many controls they deploy but by how clearly they define ownership, how fast they recover, and how consistently they treat resilience as a business-critical capability.

1. Strategic imperatives for cyber resilience

Cyber threats are inevitable, but failures can be prevented. These strategic imperatives emphasize proactive planning, effective risk communication, and practical use of AI to ensure operational continuity and informed decision-making.

1.1 Treat insider threats as your most likely breach scenario

Insight: Participants unanimously recognized that the greatest vulnerabilities often come from within whether it is negligent behavior, credential misuse, or intentional sabotage. Unlike external threats, insider breaches are harder to detect and easier to underestimate. As remote work and third-party access expand, the attack surface continues to grow.

Recommendation
Reframe the security posture to assume insider compromise as the default scenario. Prevention alone is not enough as detection, deterrence, and accountability are equally critical.

Actions
- Implement real-time monitoring of user behavior and privilege escalation.
- Run simulated phishing and social engineering drills quarterly.
- Define insider risk indicators and automate escalation workflows.
- Train employees with high access privileges in breach impact scenarios.

1.2 Build supply chain resilience into your architecture

Insight: Third party vendors, open-source libraries, and cloud platforms were identified as critical but opaque risk vectors. Attacks now often enter through indirect paths such as vendors of vendors, poorly maintained APIs, or unmanaged dependencies. The group agreed that no matter how secure your perimeter is, one weak link can compromise everything.

Recommendation
Elevate supply chain security to a board-level priority, with policies that go beyond compliance paperwork and into continuous validation.

Actions
- Mandate SBOMs (software bill of materials) from all software vendors.
- Continuously scan dependencies and third-party code for vulnerabilities.
- Establish contractual SLAs (Service Level Agreements) around patch timelines and breach reporting.
- Periodically test vendor systems as part of your pen-testing routine.

1.3 Quantify risk to inform board-level decisions

Insight: Security teams are increasingly expected to justify spend and strategy in business terms. Leaders shared that qualitative assessments no longer suffice as boards want quantified risk models that highlight financial exposure, reputational damage, and recovery timelines.

Recommendation

Translate cyber risk into language executives understand such as probabilities and time to recovery. Use this to prioritize investments and drive decision making.

Actions

- Adopt frameworks like FAIR (Factor Analysis of Information Risk) or CVSS (Common Vulnerability Scoring System) to structure risk quantification.
- Present risk in terms of potential loss per business unit or system.
- Include residual risk and risk trendline in quarterly board updates.
- Use quant data to rank security investments by impact.

1.4 Build for failure, not just defense

Insight: Resilience is not about keeping threats out, it is about staying operational when systems fail. From ransomware to service outages, the group emphasized that fast recovery defines real resilience.

Recommendation

Design your infrastructure, policies, and workforce assuming breaches will happen. The goal is not zero incidents, it is zero critical downtime.

Actions

- Define RTOs (recovery time objectives) for all business-critical systems.
- Establish secondary communication channels and offline protocols.
- Deploy immutable backups and regularly test restore processes.
- Align cyber drills with actual business continuity exercises.

1.5 Anchor AI adoption in business value, not market hype

Insight: While AI shows promise for anomaly detection and access management, most participants felt that GenAI in security remains experimental. The high cost, lack of transparency, and regulatory risk make broad deployment premature.

Recommendation

Focus on proven AI use cases with measurable outcomes. Prioritize explainability, control, and integration over novelty.

Actions

- Pilot AI for user behavior analytics and log correlation, not LLM-based policy enforcement.
- Maintain human-in-the-loop oversight for all AI-driven decisions.
- Track model drift and false positive rates over time.
- Include AI components in risk assessments and vendor reviews.

2. Critical challenges

The push for cyber resilience is often slowed by organizational silos, underdeveloped operating models, and resource constraints. These challenges, while not always visible in metrics, were surfaced across industries as persistent blockers to sustained progress.

2.1 Fragmented ownership and underutilized security leadership

Mitigation: Establish a formal cyber resilience governance function to unify direction and outcomes and rebalance team structures to separate operational response from proactive resilience building.

Action

- Establish a cross-functional resilience council with clear ownership for recovery, communications, and continuity.
- Create dedicated roles to lead strategic planning and embed resilience into core operations.
- Include security architects early in transformation to build resilience from the start.

2.2 Disconnect between cyber risk and board-level dialogue

Mitigation: Translate risk into clear, business-relevant narratives that frame impact in terms of downtime, financial exposure, and regulatory consequence.

Action

- Develop executive dashboards that visualize cyber risk trends and exposure by asset or business unit.
- Train functional leaders in communicating risk in business terms.
- Incorporate risk quantification frameworks to bridge technical insights with financial implications.

2.3 Tool and data fragmentation across security operations

Mitigation: Unify observability, detection, and incident workflows across all environments and teams.

Action

- Standardize security tooling across cloud, on-prem, and hybrid environments.
- Integrate logging, alerting, and incident response into a shared platform.
- Automate routine alerts to free teams for higher-value work.

2.4 Overreliance on vendor certifications without active oversight

Mitigation: Treat third-party risk as dynamic. Build internal capacity to monitor, validate, and respond in real time.

Action

- Require telemetry, breach notifications, and audit visibility in all vendor contracts.
- Run joint resilience simulations that involve third-party platforms.
- Maintain an up-to-date inventory of critical dependencies and their security posture.

2.5 Resource constraints and misaligned budget models

Mitigation: Anchor budget decisions to risk reduction and operational continuity outcomes and allocate dedicated resources to forward-looking resilience initiatives.

Action

- Advocate for separate funding tracks for resilience initiatives distinct from operational security.
- Quantify the cost of downtime, recovery delays, or reputational damage to justify investment.
- Redesign security team structures to protect bandwidth for strategic initiatives and scenario planning.

2.6 Limited industry-level intelligence sharing

Mitigation: Accelerate cross-industry collaboration by participating in structured intelligence-sharing ecosystems and co-developing threat models.

Action

- Join industry-specific CERT and regional intelligence-sharing partnerships.
- Develop anonymized sharing frameworks for zero-day threats and breach indicators.
- Promote standardization of threat formats and response patterns across ecosystem partners.

3. Implementation plan

Building resilience is not just a policy, it is an architecture. Participants emphasized that unless resilience is designed into systems from the ground up, it remains a slide deck and not a capability. This section outlines the practical principles, architectural focus areas, and implementation steps shared by leaders across sectors.

3.1 Design principles

Resilience must be engineered into how organizations build, deploy, and manage systems. The group outlined four guiding design principles:

Modularity: Break down infrastructure into smaller, loosely coupled components to reduce blast radius and enable faster containment during incidents.

Interoperability: Ensure systems, platforms, and vendors can talk to each other, especially during a disruption. Resilience fails when critical tools are locked in silos.

Security: Build protection into every layer: infrastructure, application, user, and data. Participants stressed the need for zero-trust models, least-privilege access, and secure-by-default configurations.

Observability: End to end visibility across assets, users, APIs, and processes is essential for detection, response, and recovery.

3.2 Architecture components

Participants discussed key architectural elements that support resilience not just for today's systems but for what comes next.

Data layer

- Maintain governed, real-time data pipelines with lineage tracking and validation.
- Tag critical data assets by sensitivity and recovery priority.
- Integrate with data catalogues to enforce access control and discoverability.

Application layer

- Use microservices and containerization to isolate failures.
- Define failover logic and rate-limiting for business-critical APIs.
- Monitor service dependencies continuously to detect cascading risks.

Security layer

- Deploy identity-aware proxies, access monitoring, and behavior-based controls.
- Tokenize and encrypt sensitive assets in motion and at rest.
- Automate incident correlation across endpoints, network, and cloud.

Recovery layer

- Ensure backup systems are segregated and routinely tested.
- Define recovery point objectives (RPO) and recovery time objectives (RTO) for each system.
- Simulate failure scenarios beyond the usual (e.g., cloud provider outage, insider sabotage, API lockout).

3.3 Implementation steps

Moving from principle to execution requires deliberate, staged action. The group identified high-impact steps for embedding resilience at scale.

- Map asset criticality across infrastructure and prioritize by business impact.
- Centralize telemetry, logs, and incident signals into a unified observability platform.
- Automate routine alerts to free teams for higher-value work.
- Include security architects early in transformation to build resilience from the start.
- Run cross-functional resilience exercises simulating multi-day, multi-vendor failure scenarios.
- Define exit strategies for critical workloads, especially those in cloud or SaaS ecosystems.
- Continuously validate backup and recovery playbooks under real conditions.

4. Success metrics

Resilience must be measurable. Participants agreed that traditional security KPIs fall short. What matters is how well an organization can detect, recover, and maintain critical operations under pressure.

- **Time to detect and recover (MTTD/MTTR):** Measure how quickly incidents are identified, contained, and systems restored across zones, vendors, and environments.
- **Resilience testing frequency and outcomes:** Track how often fault simulations and recovery drills are run, and whether predefined recovery objectives are met.
- **Coverage of observability and monitoring:** Monitor the percentage of critical assets (apps, APIs, endpoints) under real-time telemetry and alerting.
- **Business-critical application uptime (Tier 1):** Assess uptime, failover success, and recovery performance specifically for high-impact systems.
- **Third-party resilience readiness:** Evaluate vendors based on telemetry sharing, breach response protocols, and alignment to your resilience standards.

5. Next steps

Resilience is not a milestone, it is a continuous loop of alignment, action, and improvement. Participants agreed it is time to move from awareness to execution.

- **Elevate resilience to a board-level business priority:** Position resilience as essential to continuity and brand trust. Ensure ownership spans beyond IT, with accountability anchored in the C-suite.
- **Institutionalize a phased resilience operating model:** Adopt a structured cycle of Plan, Discover, Execute, and Monitor. Align it to business-critical systems and enforce it through shared metrics and review cadences.
- **Create a cross-functional resilience council:** Establish a formal body with visibility across security, IT, operations, and compliance. Define ownership for detection, recovery, communications, and third-party risk.
- **Extend resilience design across the value chain:** Include vendor systems, SaaS platforms, and partner infrastructure in resilience architecture. Validate controls through exercises and not just certifications.
- **Make people the front line of recovery:** Invest in training beyond awareness, build role specific playbooks, simulate multi day disruptions, and measure team readiness.
- **Codify resilience into policy and architecture:** Use frameworks like NIST or ISO as baselines, but tailor controls to your business context. Update recovery and response policies as systems, teams, and threats evolve.

Attendees

Name	Company	Designation
Ashutosh Pathak	Manipal Global Education	Head IT
Hilal Ahmad Lone	Razorpay	CISO
Jayraj Vyas	Ola	Chief Technology Officer
Philip Varughese	DXC Technology	Global Head - Applied Intelligence, Platforms and Enginnering
Praveen Samariya	Medi Assist	Chief Technology Officer
Raghu P	Canbank Factors Limited	Chief Technology Officer
Rahul Malhotra	CSC	Senior Vice President, Global IT
Sanbir Singh Keer	TPRM, Deloitte	Executive Director | Cyber Strategy & Transformation
Srikanta Sahoo	LTIMindtree	Senior Director
Srinivas Jaggumantri	Infosys	Chief Technology Officer, Financial Services
Vasudev Puranik	Accenture	Managing Director, Global IT(CIO), Sales Excellence
Venkata Sai Kumar K.	Canara Bank	Head- (CSOC) & Divisional Manager- Information Security