F5 regional CXO roundtable series

Mumbai edition

Building unbreakable cyber resilience

Key takeaways | October 18, 2024

Lessons from the Mumbai CXO roundtable

An actionable path for building unbreakable cyber resilience

Executive summary

The Cyber resilience roundtable in Mumbai brought together senior leaders from major financial institutions and critical sectors to define a practical, outcome-driven approach to strengthening resilience in an increasingly complex digital landscape. Set against the backdrop of rising cyber threats, supply chain dependencies, and regulatory pressures, the discussion focused on translating resilience from static policy to tested execution across the enterprise.

What emerged was a collective acknowledgment that resilience is no longer about perimeter protection: it's about recovery, accountability, and visibility at every level. It is clear that security controls are necessary but not sufficient. Leading organizations are prioritizing cross-functional governance, dynamic architecture, and people readiness as core to their resilience strategy.

Insights from live polling during the session revealed clear alignment among participants:

- **Resilience gaps revealed by incidents:** CrowdStrike was identified as the event with the highest perceived unpreparedness, pointing to weaknesses in third-party risk response.
- **Budgets not adjusted post-incident:** Spending levels remained largely unchanged post-incident, suggesting limited financial realignment despite operational disruption.
- **Threat landscape remains unclear:** There was no single threat vector that stood out in the responses. This reflects the uncertainty in today's threat landscape and highlights the need to prepare for a broad range of scenarios rather than relying on past patterns.

To move from alignment to action, participants defined a structured agenda anchored in five core focus areas:

1. **Strategic imperatives**: Align resilience with business risk and regulatory context. Seven imperatives were defined, including embedding observability, simplifying tooling, and engineering for partial recovery.

2. **Critical challenges**: Addressed gaps in visibility, supply chain control, and incident preparedness. Key issues raised included untracked APIs, unclear vendor SLAs, and outdated recovery protocols.

3. **Implementation plan**: Design systems with modularity, interoperability, and observability. Architecture must support telemetry-rich detection, tested fallback, and secure-by-default design.

4. **Success metrics:** Track recovery time, fallback readiness, and decision speed, not just control coverage. Metrics should inform risk posture at both the technical and board levels.

5. **Next steps:** Elevate resilience to a board-level risk domain, operationalize business-driven playbooks, and strengthen peer knowledge exchange through trusted sharing networks.

The session reinforced a critical shift that cyber resilience is no longer about having more tools or broader coverage. It is about clarity of design, quality of execution, and confidence in recovery. The institutions leading this shift are those treating resilience not as insurance but as infrastructure.

1. Strategic imperatives for cyber resilience

The focus is on aligning resilience strategies with business priorities and regulatory obligations. Key themes include visibility, simplified architecture, proactive governance, and engineering systems for recovery rather than prevention.

1.1 Align resilience with business strategy and risk appetite

Insight: Cyber resilience must reflect the organization's specific regulatory context, customer exposure, and operational dependencies. Misaligned controls either underperform or overreach, increasing systemic risk.

Recommendation
Integrate cyber resilience into enterprise risk management frameworks with clearly defined thresholds for disruption and recovery.

Actions
- Conduct targeted risk assessments that map regulatory obligations to actual business services.
- Define recovery time objectives and risk tolerance at the board level.
- Use sector-specific scenarios to validate impact and response assumptions.

1.2 Prioritize asset intelligence across internal and external ecosystems

Insight: Many exposure points remain undocumented or invisible to internal teams. Shadow APIs, third-party integrations, and unmanaged libraries represent primary breach vectors.

Recommendation
Establish continuous visibility across infrastructure, applications, APIs, and vendor environments using telemetry and behavioral context.

Actions
- Deploy automated discovery and asset classification platforms across internal and third-party systems.
- Monitor shadow interfaces, open-source dependencies, and abandoned endpoints.
- Feed visibility data into segmentation and access control design.

1.3 Architect for recovery over prevention

Insight: Security failures are often inevitable, but prolonged downtime is not. Institutions that recover quickly maintain customer trust and operational integrity even under attack.

Recommendation
Design systems and response protocols for degraded but functional operations when core infrastructure is impacted.

Actions
- Define fallback operating states for customer-facing and internal services.
- Simulate multi-point disruptions involving infrastructure, application, and vendor breakdowns.
- Maintain role-specific crisis playbooks that are regularly updated and accessible to all teams.

1.4 Embed threat modelling into development and change management

Insight: Security blind spots often originate during development or change cycles. Reliance on unvetted third-party components introduces uncontrolled risk at scale.

Recommendation
Integrate security into design and development processes, using threat modelling to guide architecture and integration decisions.

Actions
- Mandate architecture reviews that include attack path assessments.
- Use scanning and validation tools for all third-party code before integration.
- Include threat simulation in major change reviews and CI/CD deployments.

1.5 Shift from tool accumulation to outcome-centric architecture

Insight: Tool proliferation without integration leads to fragmented alerts, delayed action, and reduced visibility. Many organizations operate more than 30 tools with overlapping functionality.

Recommendation

Consolidate and integrate security tooling based on its contribution to detection clarity, response efficiency, and business resilience.

Actions

- Evaluate tools by their role in the end-to-end response cycle rather than feature count.
- Remove platforms that do not deliver measurable operational improvement.
- Centralize telemetry to support unified threat detection and resolution.

1.6 Mature the security culture through simplified execution and shared ownership

Insight: Cultural gaps and unclear responsibility during incidents reduce the effectiveness of even the best security investments. Process complexity often causes delays during critical moments.

Recommendation

Operationalize resilience through simplified procedures, targeted training, and integration of security accountability across roles.

Actions

- Run real-time simulations that involve security, business, operations, and communications teams.
- Incorporate resilience metrics into both technical and non-technical performance frameworks.
- Foster shared accountability by clearly defining security responsibilities across all roles.

1.7 Engineer resilience into the technical architecture

Insight: High availability does not guarantee resilience. Systems must be designed to adapt, isolate failure, and support coordinated recovery without full reliance on upstream dependencies.

Recommendation

Embed resilience into architecture at the design level by focusing on isolation, recovery, and failover behavior during abnormal conditions.

Actions

- Conduct dependency mapping to identify failure propagation risks across systems and vendors.
- Adopt modular and autonomous infrastructure patterns that support localized recovery.
- Evaluate partner readiness through realistic disruption simulations and follow-up audits.

2. Critical challenges

Enterprise face issues like fragile supply chains, limited observability, unclear accountability in managed security, and emerging risks from AI systems. Compliance-driven frameworks often lack depth in real-world resilience scenarios.

2.1 Fragile supply chains and ecosystem dependencies

Mitigation: Strengthen ecosystem-level coordination through compatibility checks, risk-tiering of vendors, and resilience standards across interconnected platforms.

Action

- Conduct end-to-end dependency mapping for high-risk integrations.
- Assess third-party products for architectural weaknesses and shared vulnerabilities.
- Request security design documentation and failover protocols from vendors and partners.

2.2 Lack of secure design in development pipelines

Mitigation: Move validation and threat modeling into the initial design phase. Development workflows must internalize security as a quality metric, not a compliance requirement.

Action

- Enforce static code analysis and secure architecture reviews prior to approval.
- Launch internal developer programs that focus on application-specific threats.
- Track vulnerability age and time-to-remediate as team-level KPIs.

2.3 Expanding attack surface with limited observability

Mitigation: Replace static inventory tools with continuous, telemetry-rich asset observability that includes behavioral context and usage patterns.

Action

- Deploy asset intelligence platforms that cover APIs, IoT, and unmanaged endpoints.
- Implement network and user behavior analytics to flag deviations.
- Integrate telemetry feeds into response workflows for faster triage.

2.4 Inconsistent accountability in managed security models

Mitigation: Restructure outsourcing models with explicit expectations for threat detection, incident response, and resilience testing.

Action

- Redefine vendor KPIs around mean time to detect, escalate, and recover.
- Create shared response playbooks with clear trigger conditions and handoff points.
- Include mandatory upskilling, simulation participation, and audit-readiness in contract terms.

2.5 Misalignment between compliance and operational resilience

Mitigation: Anchor resilience programs in operational needs and threat context, using compliance only as a baseline, not a final goal.

Action

- Design tabletop simulations based on actual operating conditions and local threat models.
- Evaluate the practical usability of documented plans and test against known attack patterns.
- Establish periodic reviews to refresh resilience controls beyond certification cycles.

2.6 AI security outpaces talent and framework maturity

Mitigation: Develop in-house capability to evaluate, secure, and govern AI systems with a focus on explainability, bias management, and model safety.

Action

- Create dedicated roles or task forces for AI risk, integrating red-teaming and audit traceability.
- Introduce cross-functional training for business and technology leaders on AI control frameworks.
- Adopt risk scoring models to assess AI system readiness and operational impact.

3. Implementation plan

A robust implementation plan serves as the operational backbone for building cyber resilience. It emphasizes modularity, interoperability, and observability to ensure secure-by-design systems that can withstand, adapt to, and recover from disruptions.

3.1 Design principles

Modularity: Design systems in self-contained blocks to isolate failures, support partial recovery, and enable faster remediation across critical functions.

Interoperability: Ensure controls and telemetry work across legacy, cloud, and third-party systems. Avoid dependency on proprietary or isolated tools.

Security: Embed protection at every layer. Apply least-privilege access, encryption by default, and policy enforcement at the point of use.

Observability: Build real-time visibility into asset activity, user behavior, and system drift. Use telemetry to detect anomalies and validate recovery.

3.2 Architecture components

Data layer
Unify and classify data assets with lineage tracking, metadata standards, and access controls.

Application layer
Enable fail-safe modes and rollback features. Support alternate workflows when primary functions are degraded.

Security layer
Deploy adaptive controls including identity segmentation, behavioral monitoring, and continuous policy evaluation across the stack.

Recovery layer
Integrate fallback procedures, restoration prioritization, and tested failover paths. Ensure recovery is operational, not just technical.

3.3 Implementation steps

Building organizational resilience requires a structured, actionable approach, combining governance, operational playbooks, advanced monitoring, vendor collaboration, and continuous improvement across all business functions.

- Establish a cross-functional resilience governance council.
- Develop business-impact playbooks for common disruption scenarios.
- Upgrade telemetry to cover users, endpoints, APIs, and vendor services.
- Adopt zero-trust access based on dynamic risk and context.
- Include vendors in joint simulation and readiness testing.
- Define and report resilience KPIs at board and operational levels.

4. Success metrics

Measure the effectiveness of resilience initiatives through clear, outcome-driven indicators. Key metrics such as recovery time, decision-making speed, and fallback readiness offer critical visibility into an organization's ability to maintain continuity during disruption. These metrics enable boards and leadership teams to assess the real-world strength of their resilience posture under stress conditions.

- **Business-critical service recovery time:** Measures the time taken to restore core business functions following a disruption. Focuses on actual operational recovery rather than system uptime alone, ensuring alignment with business impact and customer expectations.
- **End-to-end visibility coverage:** Tracks the extent of real-time telemetry across infrastructure, applications, APIs, user behavior, and third-party environments. Highlights the organization's ability to detect anomalies across its full attack surface.
- **Validated fallback capabilities:** Assesses the percentage of high-impact services with documented and tested fallback procedures. Ensures continuity under degraded conditions, not just ideal failover scenarios.
- **Resilience testing frequency and integration:** Evaluates how often resilience drills are conducted and whether findings are used to update crisis playbooks, vendor protocols, and system configurations.
- **Time from detection to decision:** Captures the average duration between the identification of a threat and initiation of an appropriate response. Reflects visibility, governance clarity, and coordination efficiency.

5. Next steps

Prioritize integrating resilience into strategy, expanding offensive testing, enforcing vendor SLAs, and creating executive-led forums for knowledge-sharing to strengthen collective industry defence.

- **Integrate resilience into strategy and design:** Resilience must be treated as a foundational design input. Use AI-enabled threat modelling and scenario planning early in the technology and business strategy lifecycle to identify and mitigate risk.
- **Expand the role of offensive testing:** Red teaming and breach simulations should move from occasional checks to standard operating rhythm. Focus on identifying hidden vulnerabilities in integrations, assumptions, and open-source components.

- **Strengthen supply chain and vendor governance:** Update third-party engagement models with clearly defined resilience SLAs. Conduct joint planning exercises with key providers to validate response roles and recovery paths under real-world scenarios.
- **Simplify tooling without sacrificing coverage:** Streamline overlapping tools while preserving cross-domain functionality. Focus on intelligent bundling and interoperability rather than single-vendor dependency.
- **Establish a private knowledge-sharing network:** Support the formation of a peer-led forum where security leaders can share playbooks, analyze region-specific threats, and co-create frameworks based on collective experience and evolving risks.

Attendees

Name	Company	Designation
Abhijeet Chakravarthy	Kotak Bank	EVP - Networks & Cyber Security
Abhishek Jha	Citi Global Markets India Private Limited	Chief Information Security Officer
Amogh Zade	ECGC	Deputy Chief Technology Officer
Arif Bhatkar	Godrej Infotech	Head Information Technology Security
Diwakar Raut	BSEIndia	Head Cybersecurity
Dr. Nareshkumar Harale	ReBIT | Reserve Bank Information Technology	Former Vertical Head & CISO
Dr. Pawan K Sharma	Tata Motors	CISO
Kamlesh Jobanputra	Kotak Life	Executive VP and Head of Enterprise Apps
Kiran Belsekar	Bandhan Life	EVP CISO & IT Governance
Lalit Trivedi	FlexM	Head Information Security
Munish Blaggan	ICICI Bank	Head Technology Infrastructure Group
Nandan Gandre	IIFL Home Finance	CISO
Nehal Shah	IDBI Bank	Deputy CTO