F5 regional CXO roundtable series

Kuala Lumpur edition

Building unbreakable cyber resilience

Key takeaways | November 28, 2024

Lessons from the Kuala Lumpur CXO roundtable

A focused approach to achieving resilient, unbreakable cyber security

Executive summary

The Kuala Lumpur roundtable revealed a decisive shift in mindset from treating cybersecurity as a defensive function to positioning resilience as a business-critical capability. Leaders agreed that true resilience is defined by the ability to maintain core operations under attack, recover rapidly, and minimize business disruption. Discussions highlighted persistent gaps such as legacy infrastructure, over reliance on SaaS platforms, fragmented communication channels, and weak data controls, all of which demand outcome focused strategies rather than checklist-based compliance. AI emerged as both an opportunity and a threat, prompting a call for strict data isolation, controlled AI adoption, and workforce readiness to counter deepfake enabled fraud and AI driven attacks.

A key insight was the recognition that resilience matters more than absolute prevention. Breaches and outages are treated as unavoidable, and the true measure of preparedness lies in restoring critical operations with speed and precision. AI was discussed as both an advantage and a risk, valued for its detection and automation capabilities but implemented with strict oversight, clear governance, and a focus on proven business value rather than hype.

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

- **Reform requires leadership, not bureaucracy:** Most participants agreed government efficiency reforms succeed only with decisive leadership and accountability, not through additional bureaucratic layers or election-driven promises.
- **Vendor dependency is the Achilles' heel:** The CrowdStrike outage exposed the highest level of unpreparedness, reinforcing that resilience strategies overly reliant on third-party vendors remain dangerously fragile.
- **Insiders and organized crime pose the greatest risk:** Leaders see the next breach most likely from insiders or criminal groups, signalling a shift beyond state-centric threat assumptions.

- **Risk appetite remains fragmented:** While frameworks exist, poor communication and uneven adoption mean frontline teams often lack clarity, leaving risk management inconsistent across the organization.
- **AI adoption is measured, not mainstream:** Most organizations remain cautious, limiting AI to pilots and selective functions due to cost, oversight, and explainability concerns.

To drive this transformation, the roundtable outlined five focus areas:

1. **Strategic imperatives:** Position resilience as a business enabler with imperatives such as designing for recovery, eliminating shadow IT, securing supply chains, isolating enterprise data in AI workflows, and building workforce preparedness.
2. **Critical challenges:** Legacy systems, fragmented communication, SaaS dependency, and audit-driven compliance remain structural blockers that require proactive, outcome-focused strategies.
3. **Implementation plan:** Adopt modular architecture, Zero Trust principles, and layered observability, combined with continuous drills and hybrid recovery protocols.
4. **Success metrics:** Evaluate readiness using KPIs such as operational resilience score, uptime of Tier 1 systems, detection speed (MTTD/MTTR), and resilience drill performance.
5. **Next steps:** Elevate resilience as a board priority, enforce cross-functional accountability, test extended failure scenarios, and build role-specific response capabilities.

1. Strategic imperatives

Resilience has become a core business capability, moving beyond traditional security measures. The focus is on sustaining critical operations during disruptions, closing visibility gaps, strengthening vendor ecosystems, safeguarding data in AI environments, and elevating organizational awareness through practical adoption strategies.

1.1 Design for recovery and continuity, not just defense

Insight: Cybersecurity must extend beyond prevention. Resilience, keeping operations running with minimal disruption, is the real test during ransomware attacks or cloud failures.

Recommendation
Build infrastructure for rapid failover, zero trust validation, and operational drills that simulate real-world attacks.

Actions
- Identify the minimum set of apps required to sustain operations.
- Run quarterly drills for ransomware, isolation, and cloud outages.
- Integrate fallback systems and ensure they are fully tested.

1.2 Close visibility gaps and end shadow communication

Insight: Unauthorized tools undermine monitoring and increase exposure to AI-driven scams, such as deepfake fraud.

Recommendation
Standardize enterprise communication on auditable platforms and eliminate shadow IT tools.

Actions
- Block unapproved apps on corporate devices.
- Enforce Teams-only or approved platform usage.
- Penalize policy violations and ensure audit trails are accessible.

1.3 Fortify supply chains and vendor ecosystems

Insight: Vendors and suppliers are often weak links in security chains, with some hardware and software components compromised by malware or embedded threats.

Recommendation
Apply rigorous cyber risk frameworks to all third parties, with certifications and testing as a standard requirement.

Actions
- Classify vendors based on risk exposure and data access.
- Mandate ISO/SOC2 certifications and regular penetration tests.
- Embed cybersecurity clauses into all procurement agreements.

1.4 Isolate enterprise data from open models

Insight: Uploading sensitive data to large language models (LLMs) is a major risk. Leaders stressed that enterprise data should never be directly fine-tuned into external AI models.

Recommendation
Use AI indexing or directory-based approaches that retrieve insights without storing sensitive data in the model.

Actions

- Adopt secure AI indexing or directory-based tools for AI queries.
- Configure systems to ensure LLMs never directly access or store proprietary data.
- Create internal capability zones in the cloud dedicated to AI workloads.

1.5 Educate and demystify AI across teams

Insight: Many employees view AI as abstract or overly complex, which slows adoption. Building AI literacy and trust across all departments is essential.

Recommendation

Launch company-wide initiatives to teach practical AI applications and risks.

Actions

- Conduct workshops explaining real-world AI use cases.
- Gamify AI learning to engage teams and improve uptake.
- Train finance and security teams to identify AI-enabled scams like deepfakes.

2. Critical challenges

Cyber resilience requires going beyond conventional security measures and certifications. The discussions revealed recurring operational gaps from legacy systems and weak data controls to communication breakdowns and SaaS dependency that demand proactive, outcome-focused strategies to ensure true business continuity.

2.1 Legacy infrastructure and reactive maintenance

Mitigation: Adopt a structured tech refresh and preventive maintenance policy with enforced accountability.

Actions

- Define asset refresh cycles (e.g., every 2 years) for IT and OT systems.
- Use visibility dashboards to track aging infrastructure and obsolescence risks.
- Audit departments regularly and enforce penalties for non-compliance.

2.2 Audit-focused compliance without real effectiveness

Mitigation: Shift from policy-based audits to operational performance metrics that measure actual effectiveness.

Actions

- Define KPIs such as downtime reduction, incident recovery time, and mean time to detect (MTTD).
- Include operational drills and penetration testing in audits.
- Involve business units to validate if controls address real risks.

2.3 Data as the weakest link

Mitigation: Treat data as a strategic security asset, with robust masking, encryption, and AI-based monitoring.

Actions

- Tokenize sensitive customer and business data with split-key access control.
- Use AI indexing instead of fine-tuning LLMs with enterprise data.
- Monitor external-facing APIs and SaaS pipelines for unauthorized data access or leaks.

2.4 Fragmented communication and BCP gaps

Mitigation: Standardize enterprise communication tools and build resilient business continuity plan (BCP) workflows.

Actions

- Block unapproved messaging apps and enforce the use of Teams or approved platforms.
- Develop offline backups of critical operational plans.
- Simulate outages of communication platforms to test fallback readiness.

2.5 Ineffective awareness and behavioural gaps

Mitigation: Transition to continuous, tool-integrated awareness programs with measurable results.

Actions

- Embed threat reporting directly into email and productivity tools.
- Track employee behaviour using phishing simulation click rates and response times.
- Reward proactive reporting and quick response behaviours.

2.6 Gaps in SaaS and cloud outage preparedness

Mitigation: Build multi-cloud and internal fallback mechanisms into the business continuity framework.

Actions

- Require SaaS vendors to share their resilience plans and incident response documentation.
- Maintain minimal on-premise or multi-cloud alternatives for critical business processes.
- Test SaaS outage response scenarios as part of BCM (business continuity management) drills.

3. Implementation plan

A structured approach to resilience demands clear design principles, layered architecture, and actionable steps that ensure critical systems remain operational and recover swiftly during disruptions.

3.1 Design principles

Modularity: Structure systems into independent components to minimize disruption during failures and enable quicker upgrades, troubleshooting, and recovery.

Interoperability: Use open standards and APIs to ensure seamless integration across hybrid-cloud, on-premise, and SaaS environments..

Security: Embed Zero Trust, encryption, and least-privilege access controls into every system layer for proactive defense and data protection.

Observability: Centralize logs, metrics, and AI-based monitoring to detect anomalies, predict failures, and accelerate recovery processes.

3.2 Architecture components

Data layer
Protect sensitive data with tokenization, encryption, and replication while enabling real-time availability across on-premise and multi-cloud storage.

Application layer
Identify critical applications and containerize them with automated scaling and built-in failover mechanisms to ensure uptime.

Security layer
Deploy advanced detection tools, XDR, and continuous risk monitoring to strengthen internal and third-party security.

Recovery layer
Automate disaster recovery workflows, maintain hybrid-cloud failovers, and test response capabilities through regular drills.

3.3 Implementation steps

- **Assess and prioritize:** Conduct BIA (business imapact analysis) to identify critical applications, data, and services essential for business continuity.
- **Blueprint architecture:** Design modular, zero trust-aligned infrastructure with integrated resilience and security measures.
- **Secure data:** Apply AI indexing, tokenization, and role-based access controls to prevent unauthorized data exposure.
- **Test resilience:** Simulate ransomware attacks, cloud outages, and communication failures to validate preparedness.
- **Continuous improvement:** Refresh assets on a two-year cycle, monitor KPIs like downtime and recovery speed, and refine controls.

4. Success metrics

Measuring resilience requires more than traditional security KPIs. These metrics evaluate how well systems, data, and teams perform during real-world disruptions, ensuring alignment with business priorities and operational continuity goals.

- **Operational resilience score:** Evaluate overall resilience by tracking the percentage of critical services that remain operational during disruptions and measuring adherence to defined recovery time objectives (RTOs).
- **Threat detection and response efficiency:** Measure mean time to detect (MTTD) and mean time to respond (MTTR) for incidents, ensuring continuous improvement and faster containment of potential breaches.
- **Data protection compliance:** Track the percentage of sensitive data that is fully tokenized, encrypted, and protected, with no incidents of unauthorized access or leakage.
- **Resilience drill outcomes:** Monitor performance across simulated ransomware attacks, SaaS outages, and deepfake threats, scoring teams on readiness and recovery effectiveness.
- **Vendor and platform reliability:** Evaluate SLA compliance, uptime metrics, and resilience readiness across critical SaaS and cloud providers through structured quarterly assessments.

5. Next steps

Building true cyber resilience requires focused execution across governance, critical asset protection, testing, and continuous improvement.

- **Strengthen governance:** Form a cross-functional team with clear accountability for resilience strategy and execution.
- **Identify critical assets:** Conduct business impact analysis to map essential applications, data, and dependencies across all environments.
- **Modernize infrastructure:** Apply structured technology refresh cycles and integrate advanced security principles such as Zero Trust and encryption.
- **Validate readiness:** Run scenario-based drills for ransomware, SaaS outages, and AI-driven threats to test recovery capability.
- **Evolve continuously:** Use insights from drills, vendor reviews, and real incidents to refine and improve resilience measures.

Attendees

Name	Company	Designation
Amitabh Sharan	DHL IT Services	Head of Global Solutions (Regional IT integration Leader)
Azril Rahim	Tenaga National Berhad	Head of IT Security (direct report to CTO)
Dr. Sekar Jaganathan	Kenanga Investment Bank	Chief Business Officer, Equity Broking Business Expansion And Development
Fariz Ikhromy Rahmansyah	British American Tobacco	Regional Head of DBS Operations – Asia Pacific, Middle East, and Africa
G Saravanan	Thomson Hospital	Group Chief Information Officer
James Thang	UCSI Group Holdings	Group CIO
Lee Warner	HLAP General Insurance	CEO
Maz Mirza	KWAP	CDO
Mohd Hanapi Bin Bisni	Petra Energy Berhad	Head of Group IT (Direct report to CEO)
Sazul Samsuri	KAF Investment Bank	CTO Digital Banking, Head of Digital Innovation