Crisil
Integral IQ

Thriving through cyber resilience

Why cyber resilience matters

Threats are escalating
- Rise of ransomware, AI-driven phishing and deepfakes
- Increasing reliance on third-party ecosystems and rise in hybrid working models
- Emergence of critical disruptors such as quantum computing and data sovereignty

Regulatory pressure is intensifying
- Global regulations—DORA (EU), SEC (US), FCA/PRA (UK), APRA CPS 234 (Australia)—demanding demonstrable resilience
- Heightened expectations of Board level accountability and operational readiness
- Addressing fragmented compliance, talent shortage and budget constraints

Requirement becoming strategic imperative
- Move beyond compliance to a strategic business capability
- Embed resilience into governance, risk management and culture
- Emphasise proactive testing, red teaming and continuous monitoring

Ensures advantageous positioning
- Early focus on governance, talent, third-party oversight and quantum-ready strategies ensure system robustness
- Cross-industry collaboration enhances collective defence and agility

The new differentiator
- Not just protection—it builds trust and credibility, and provides a competitive edge
- Institutions with resilient frameworks inspire confidence in regulators, investors and customers
- Can be positioned as a strategic advantage in a volatile digital economy

Cyber threats rapidly evolving with new attack vectors

Rise in ransomware
- Ransomware becoming a major systematic risk—now a core resilience and business continuity threat
- Also, rising ransomware attacks disrupting operations

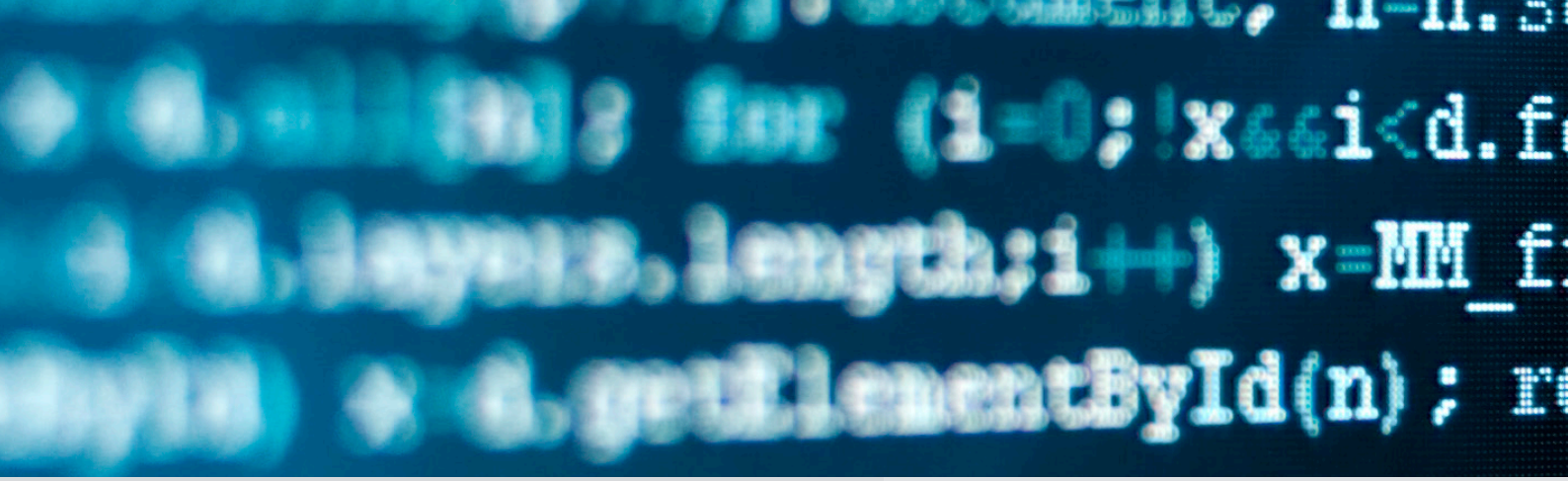
AI-driven phishing campaigns
- AI-enhanced phishing eroding traditional security controls
- AI automation also enabling large-scale, highly targeted attacks
- Phishing emerging as a top credential compromise vector

Deepfakes and synthetic media
- Deepfakes present growing cyber risk, with unprecedented levels of manifestation
- Fraudsters leveraging manipulated images, videos/ audio to impersonate executives, mislead customers and spread misinformation
- Increases the potential to trigger fraudulent financial transactions, reputational crises or regulatory breaches

Hybrid working model
- Hybrid work increases digital exposure across devices, networks and geographies
- Weak home network security and poor authentication elevate cyber risks
- Organisations must strengthen endpoint, security, zero trust and employee awareness

Moon shadowing
- Attackers mimic normal system behaviour, staying undetected for long periods
- These stealth attacks enable data exfiltration or preparation for larger breachers
- Hence, advanced monitoring, anomaly detection and threat intel needed

DORA – Digital Operational Resilience Act; SEC – Securities and Exchange Commission; FCA - Financial Conduct Authority; PRA – Prudential Regulation Authority; APRA CPS - Australian Prudential Regulation Authority Comprehensive Service Provider



Multiple security layers needed to address emerging risks

Cloud misconfigurations

- Misconfigured cloud assets are a top cause of data breaches globally
- Lack of visibility, encryption, and access governance exposes sensitive data
- Attackers exploit storage buckets, APIs and IAM gaps at scale
- Requires secure by design architecture and continuous posture monitoring

Third-party risk management

- Expanding digital ecosystems increase supply-chain exposure
- Breaches at vendors can cause systemic operational and data compromise
- Boards must ensure TPRM frameworks include real-time monitoring and escalation
- Shift from compliance- based to resilience-based vendor risk models

Data sovereignty

- Rising cross-border data flows challenge compliance with local privacy laws
- Non-compliance risks regulatory penalties and reputational damage
- Firms must embed data residency controls into architecture and operations
- Align data strategy with jurisdiction and cloud-localisation mandates

Quantum computing threats

- Rapid quantum progress poses an existential threat to modern encryption
- Future quantum attacks could break RSA and ECC encryption in seconds
- Urgent need to adopt quantum-resistant algorithm (PQC)
- Develop a quantum readiness roadmap for long-term data protectio

APIs – Application Programming Interfaces; IAM – Identity and Access Management; TPRM – Third-Party Risk Management; ECC – Elliptic Curve Cryptography; PQC – Post-Quantum Cryptography

Regulatory pressures building globally

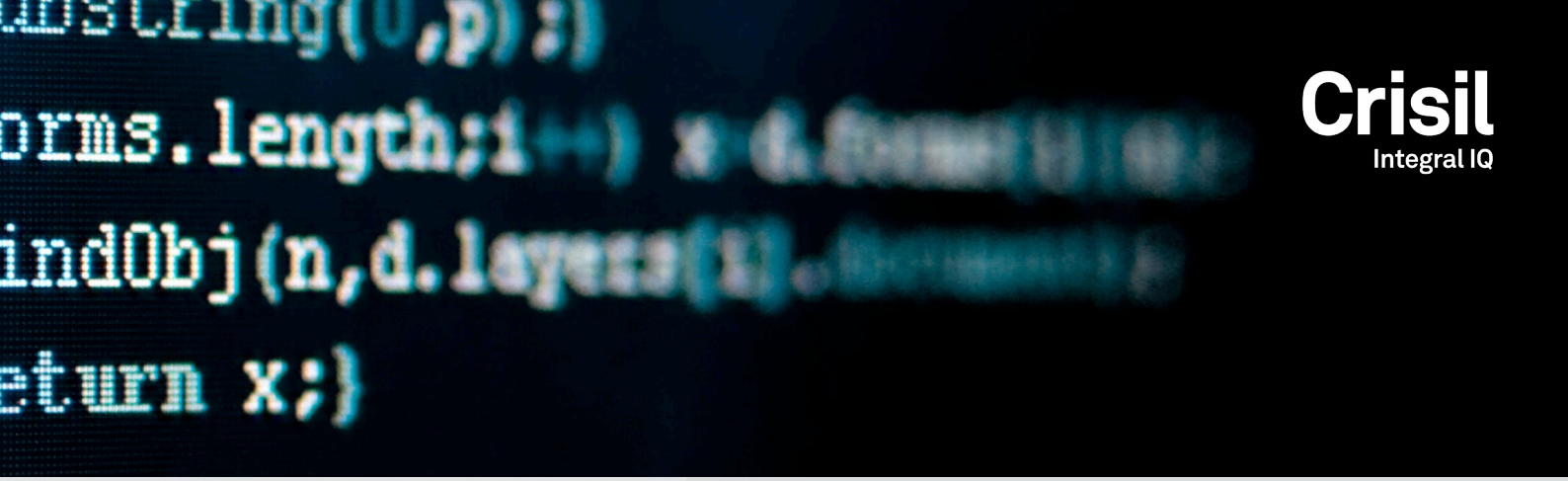
Digital operational resilience act (EU)

- Enforces unified ICT risk and resilience standards across the EU
- Mandates TLPT, incident reporting and third-party oversight
- Embeds governance, accountability and continuous resilience testing
- Creates an EU-wide compliance baseline for financial firms

SEC cybersecurity rules (US)

- Requires rapid disclosure of material cyber incidents
- Mandates Board level governance and risk oversight reporting
- Has elevated executive accountability for cybersecurity posture and response
- Aligns cyber transparency with investor protection and market integrity

FCA - Financial Conduct Authority; PRA – Prudential Regulation Authority; APRA CPS - Australian Prudential Regulation Authority Comprehensive Service Provider; ICT - Information and Communication Technology; TLPT – Threat-Led Penetration Testing



Crisil
Integral IQ

FCA / PRA (UK)

- Enforces operational resilience for critical business services
- Requires impact tolerances and severe disruption testing
- Focuses on real-world resilience over procedural compliance
- Strengthens management accountability and governance clarity

APRA CPS 234 (Australia)

- Mandates Board ownership of cybersecurity risk and oversight
- Defines minimum information security control standards
- Requires timely breach reporting and continuous control validation
- Promotes cyber maturity and supply-chain resilience across sectors

Challenges for institutions and building operational resilience

Challenges for institutions

Institutions face several systemic hurdles that undermine their ability to respond effectively to cyber threats, such as:

- Fragmented regulatory landscape: Institution face overlapping and evolving compliance mandates across jurisdictions
- Lack of talent: Acute shortage of cyber resilience professionals limits response capability
- Budget pressures: Competing priorities force trade-offs between compliance and resilience investments
- Operational strain: Balancing day-to-day performance with strengthening resilience capabilities

Interconnectivity with operational resilience

Cyber resilience cannot be addressed in isolation. Growing interconnectivity within the financial system, supply chains and digital ecosystems means that a single failure can have systemic consequences. Key to circumvent these are:

- Scenario testing: Simulate real-world crises to expose weak links and sharpen response readiness
- Tolerance statements: Define clear risk limits to know when to act before resilience is tested
- Continuous monitoring: Implement real-time insights to detect, respond and adapt before the risk escalate
- Assess third-party dependencies: Vendor disruptions can cascade across critical financial services

These measures, together, will foster a system-wide resilience, ensuring that institutions can absorb shocks while protecting critical services.

Our outlook and recommendations

Outlook

The cyber resilience landscape is evolving rapidly, becoming increasingly complex and demanding. Threat actors are leveraging advanced technologies such as AI, automation and quantum computing to exploit vulnerabilities at unprecedented scale. Simultaneously, increasing digital interconnectivity is amplifying systematic risks and potential disruptions.

Regulators globally are intensifying scrutiny, expecting not only compliance but clear evidence of operational resilience and Board-level accountability.

In this environment, reactive approaches will no longer suffice. The future belongs to organisations that position cyber resilience as a strategic enabler, integrating it into enterprise planning, innovation and the trust agenda

Strengthen governance
Establish robust governance frameworks that embed cyber resilience into enterprise risk management

Advance testing and monitoring
Move beyond compliance-driven assessments to implement continuous scenario testing, red teaming and real-time threat monitoring to validate operational readiness

Invest in talent and capability building
Develop a sustainable pipeline of cybersecurity professionals while enhancing organisation-wide awareness and digital hygiene

Enhance third-party risk management
Implement structured, data-driven oversight of third-party ecosystems with continuous risk monitoring and performance evaluation

Foster cross-industry collaboration
Share intelligence, insights and best practices across sectors to strengthen collective defense and accelerate threat response

Prepare for the quantum era
Proactively explore quantum-resistant cryptographic solutions to safeguard future digital assets and maintain cryptographic agility

Our core team

Suprabha AD
President

Maninder (Mandy) Singh
Global Head of Sales and Business Development

Nageswara Ganduri
Global Head of Quantitative Solutions and Operational Risk

Bhawaney Kumar Karnam
Head – ORM UK

Dhriti Gupta
Cyber Security Specialist

Argentina | Australia | China | Colombia | Hong Kong | India | Japan | Poland | Singapore | Switzerland | UAE | UK | USA
Crisil Limited: Lightbridge IT Park, Saki Vihar Road, Andheri East, Mumbai 400 072, India
Phone: +91 22 6137 3000 | www.integraliq.crisil.com/

/company/Crisil @CrisilLimited /CrisilLimited /user/CrisilLimited /lifeatcrisil

Crisil
a company of S&P Global