Grant Thornton

Building cyber resilience in a changing risk landscape

Wednesday, 26 November 2025 | 10:00am – 11:15am

Agenda

1 Cybersecurity

2 Incidence response

3 The evolving regulatory landscape

4 Resilience and Third Parties

5 Q&A

Industry experts speaking today

Vijay Rathour

Partner, Head of Cyber and Digital Investigations
Grant Thornton UK

Charlotte Devlin

Director,
Grant Thornton UK

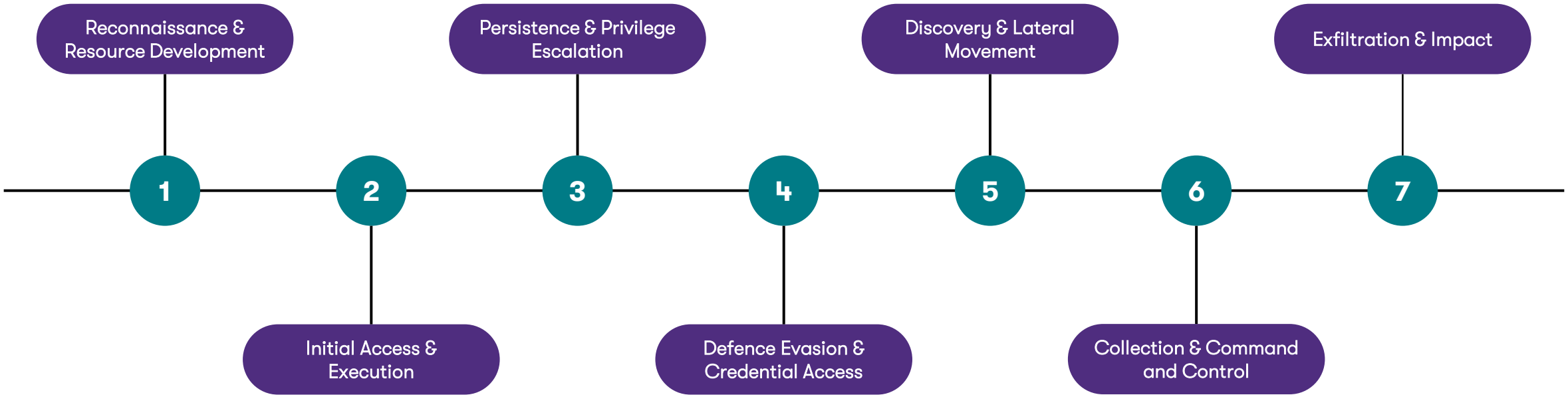
Priya Prakash

Associate Director,
Grant Thornton UK

1 Cybersecurity

Grant Thornton

Cyber Attack Phases



Cyber Controls Framework (key elements)

Identify

Establish a clear understanding of your organization's systems, assets, data, and capabilities. This includes asset management, understanding the business environment, threat analysis, governance, and conducting thorough risk assessments.

Protect

Implement safeguards to ensure the delivery of critical infrastructure services. Key areas include access control, security awareness and training, robust data security measures, and the deployment of protective technology.

Detect

Develop capabilities to identify the occurrence of a cybersecurity event. This involves monitoring for anomalies and events, continuous security monitoring, and establishing efficient detection processes.

Respond

Take appropriate actions regarding a detected cybersecurity incident. This category focuses on incident response planning, effective communications, thorough analysis and mitigation strategies, and continuous improvements to the response process.

Recover

Activities to restore and validate system functionality and services that were impaired due to a cybersecurity incident. Key elements include: trusted backups, data reconciliation, Operational resilience, communication with stakeholders, and lessons learnt.

Case Study: M&S Cyber Attack

Attack timeline

Threat actors infiltrated systems weeks in advance, deploying ransomware.

Operational Impact

M&S suspended online orders and digital services, losing £4M/day.

Financial Fallout

Share price dropped 18%, wiping out over £1 billion in market value.

M&S: Security Lessons

The M&S incident underscores critical areas for bolstering credential security, especially regarding Active Directory.

Service Desk Protocols

Implement stringent verification to prevent social engineering attacks.

Secure AD Backups

Encrypt and store AD database backups offline, test regularly.

Limit Privileged Accounts

Restrict Domain Admins and enforce MFA for all administrative accounts.

Robust Password Policies

Adopt length-based policies (15+ chars for users, 30+ for service accounts).

Monitor Lateral Movement

Detect unusual AD activities and privilege escalations.

Enhanced MFA & JIT Access

Require MFA for all accounts and consider Just-In-Time provisioning.

Final Takeaways for Leadership

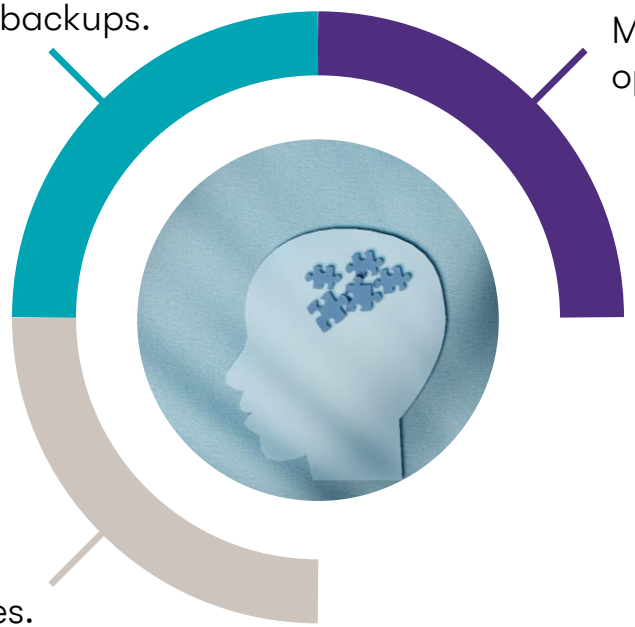
Cybersecurity is a Board-level resilience imperative. The ability to anticipate, withstand, and recover from disruption defines corporate strength and customer trust.

Recovery Readiness

Validate recovery plans and ensure offline backups.

Control Discipline

Maintain rigorous security controls across all operations.



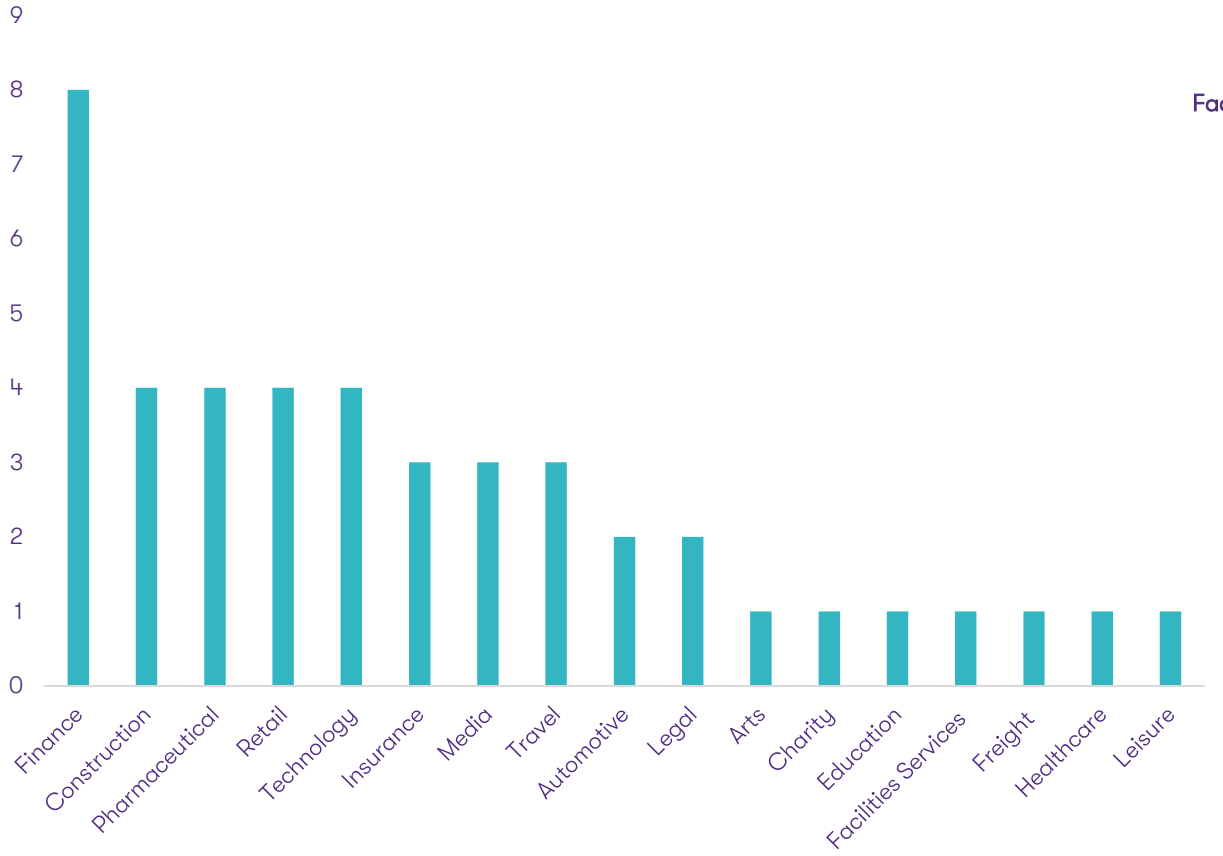
Cultural Awareness

Embed security into culture and processes.

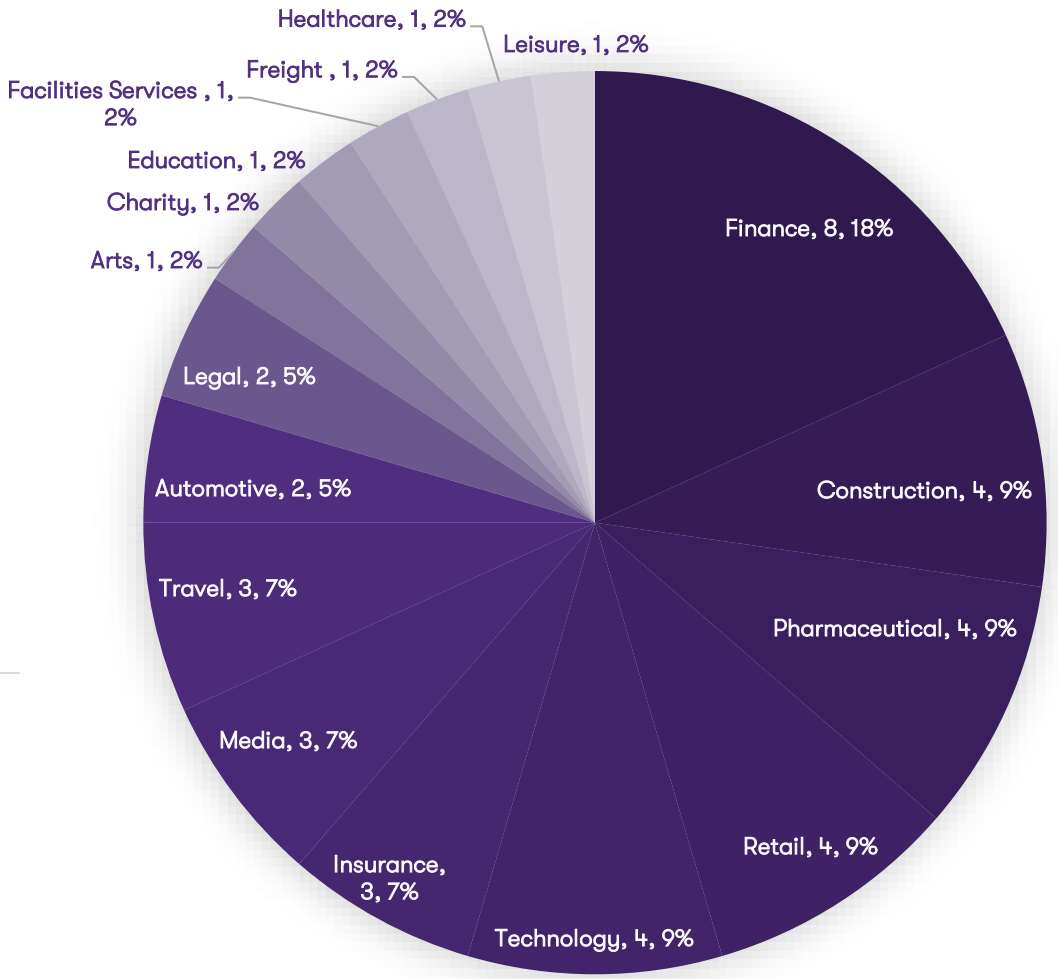
3 Incident Response

Market Sector Analysis

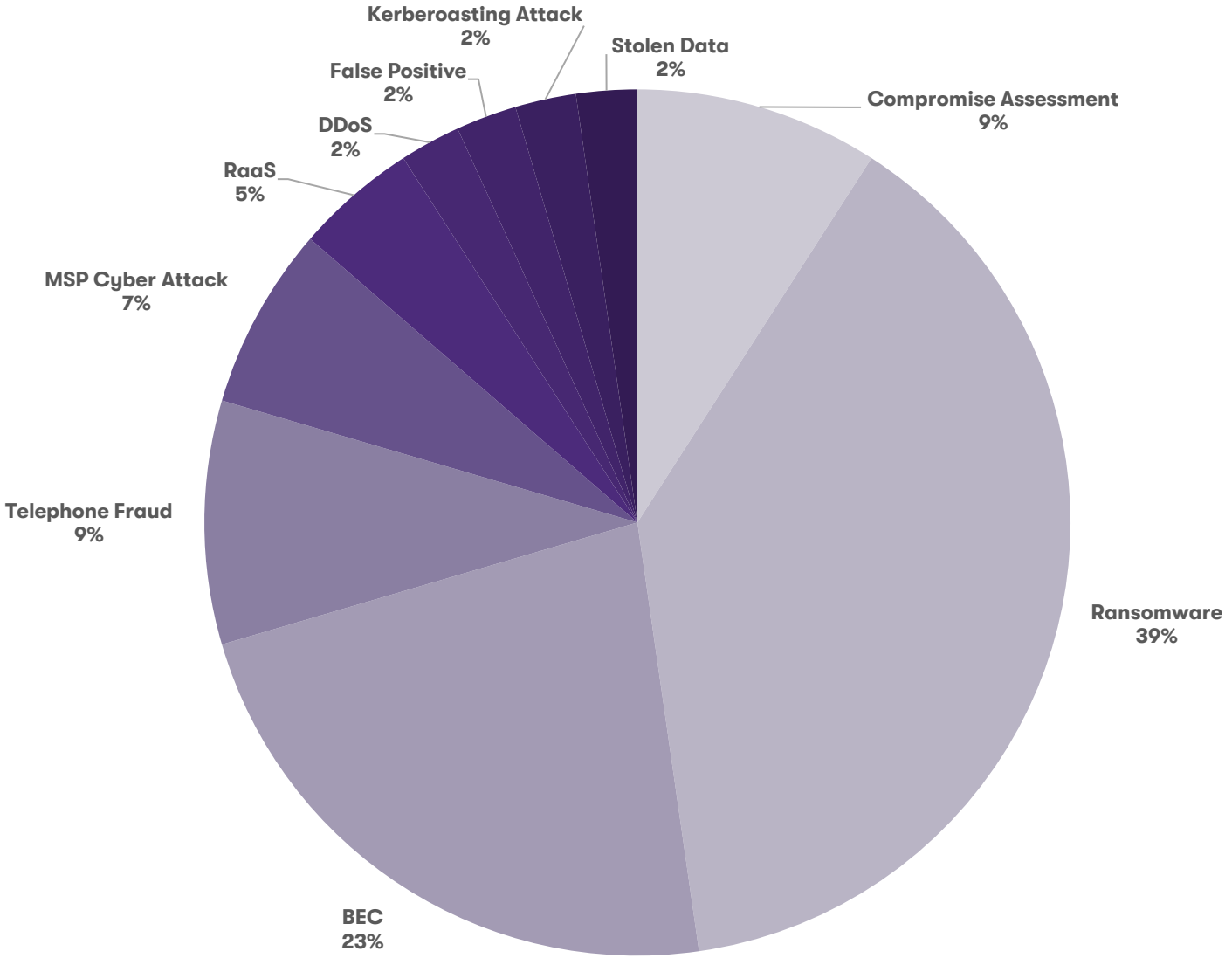
Incidents by Market Sector



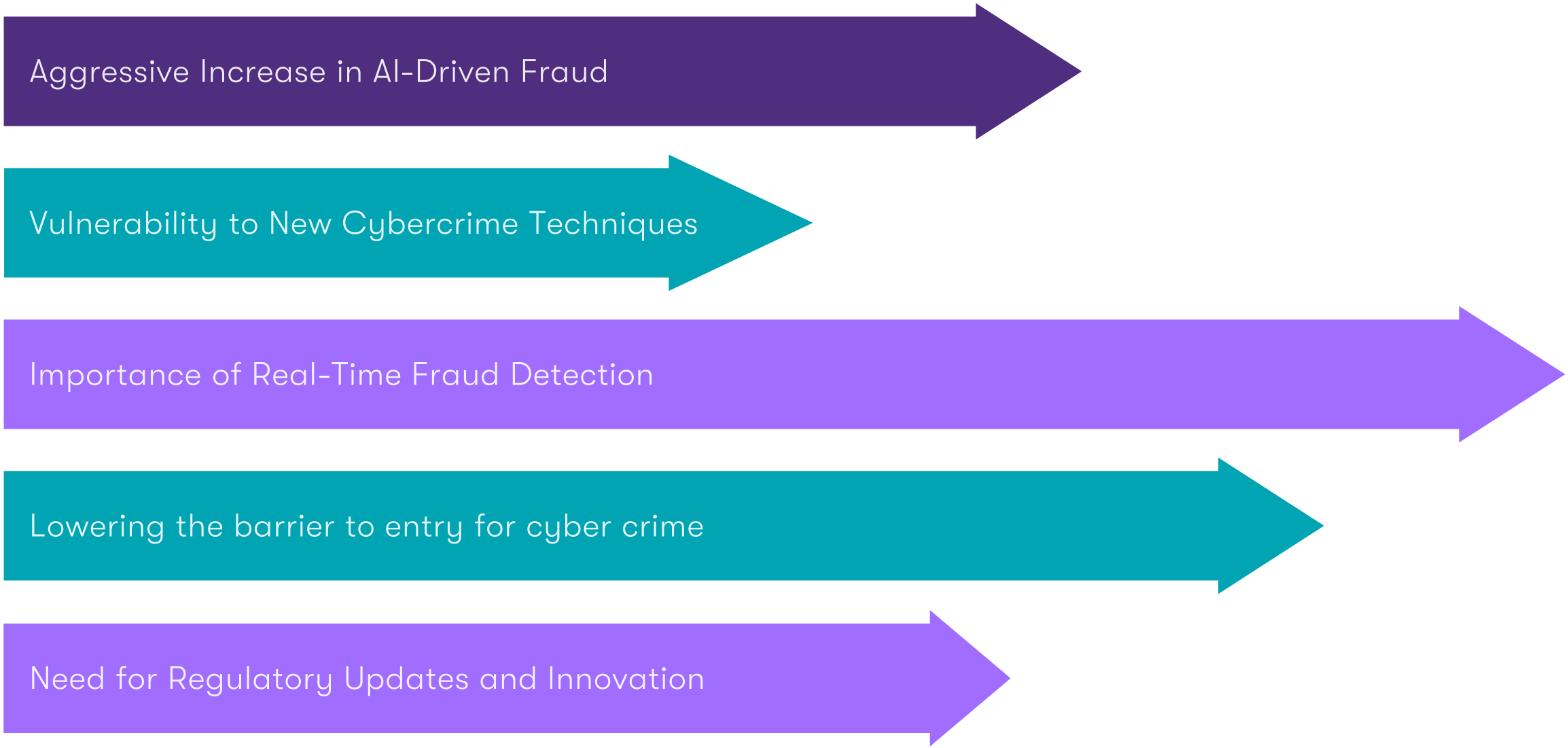
Market Sector Distribution



Type of Attack Analysis

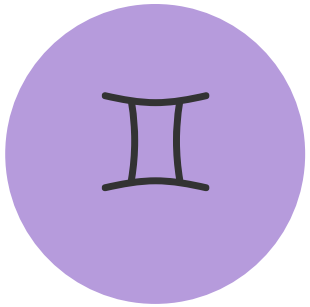


Evolving Attack Strategies



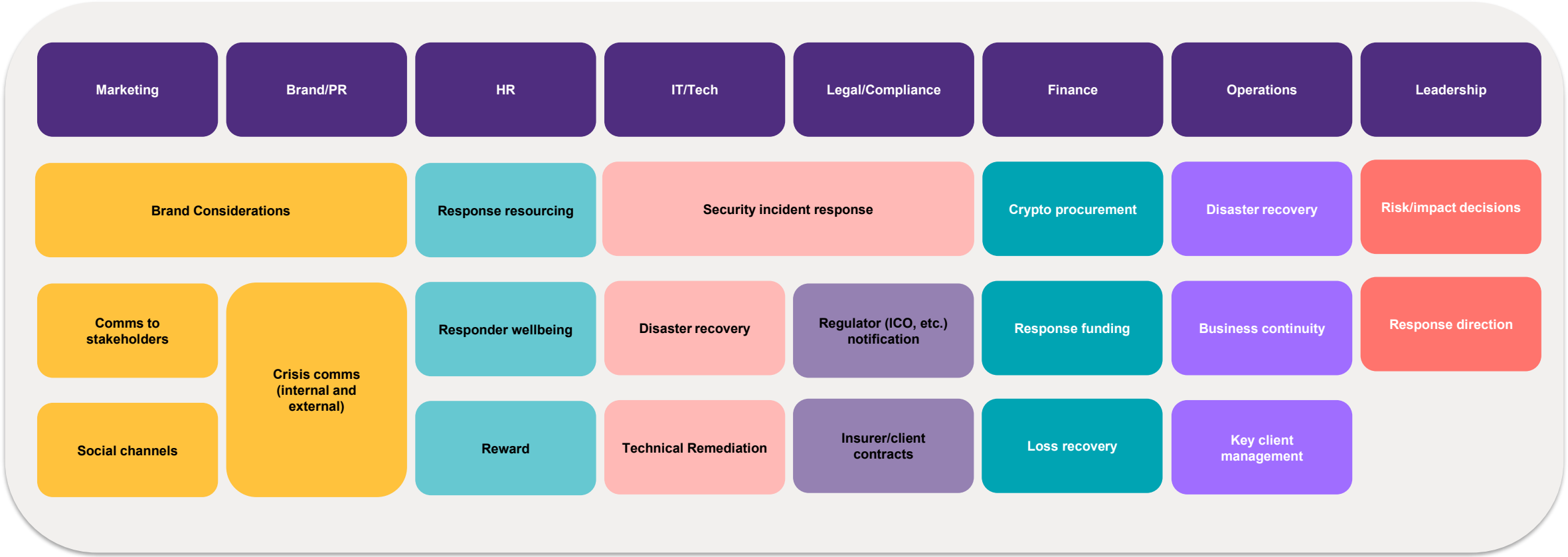
Agentic AI and Evolving Attack Strategies

- AI-powered tools, especially deepfakes, are now the second most common cyber security threat for businesses.
- They power convincing business email compromise (BEC), CEO fraud, and social engineering attacks that can trick executives, such as CFOs, into authorising fraudulent payments or disclosing sensitive information.



AI-powered attacks, such as deepfakes and automated reconnaissance, are reshaping the cybersecurity landscape

Functional impact of a major cyber incident



3 Resilience and Third Parties

Grant Thornton

Global resilience landscape

The evolving global regulatory landscape highlights the ongoing requirements for Financial Services firms to prioritise resilience measures and have a clear underlying framework for compliance, integrating resilience into their operations and organisational culture.

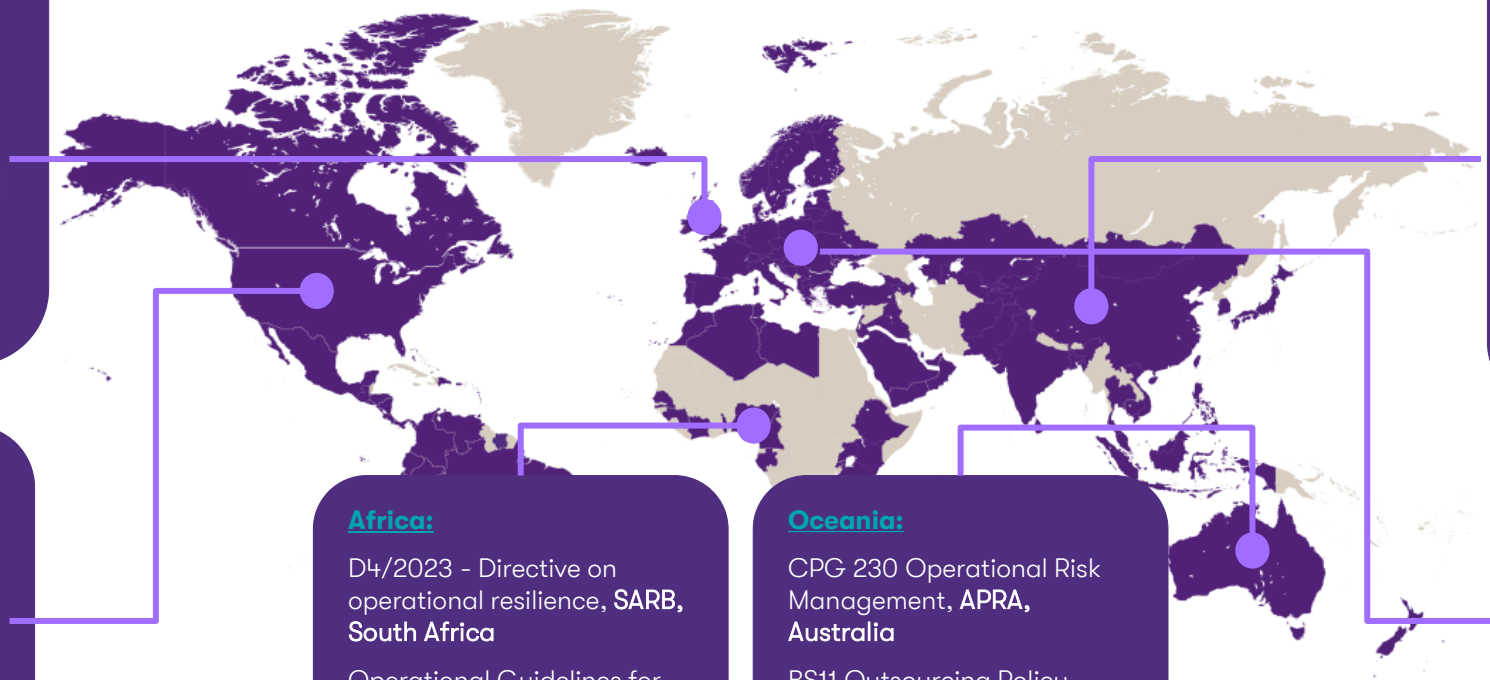
UK:

Operational Resilience, **FCA/PRA**

CP17/24 – Operational resilience: Operational incident and outsourcing and third-party reporting, **PRA**

CP24/28: Operational Incident and Third-Party Reporting, **FCA**

PS16/24 – Operational resilience: Critical third parties to the UK financial sector, **PRA**



Asia:

Operational Risk Management and Operational Resilience, **Reserve Bank of India, India**

Guidelines on Outsourcing, **Monetary Authority of Singapore's (MAS), Singapore**

Supervisory Policy Manual module, OR-2, on Operational Resilience, **HKMA, Hong Kong**

North America:

Sound Practices to Strengthen Operational Resilience, **Federal Reserve System, USA**

Guideline E-21: Operational Risk Management and Resilience, **Superintendent of Financial Institutions (OSFI), Canada**

Africa:

D4/2023 - Directive on operational resilience, **SARB, South Africa**

Operational Guidelines for Open Banking, **CBN, Nigeria**

Oceania:

CPG 230 Operational Risk Management, **APRA, Australia**

BS11 Outsourcing Policy, **RBNZ, New Zealand**

Europe:

Digital Operational Resilience Act (DORA), **European Supervisory Authorities (ESAs), EU**

Cyber Resilience Act (CRA), **ESAs, EU**

Preventative measures to ensure resilience

Organisations need to maintain resilience to survive and thrive in an increasingly complex threat landscape or during internal changes – this is not just a regulatory requirement.

External threats

- Ransomware attack
- Third party data loss incident
- Payment disruption
- Cloud provider disruption
- Outsource provider failure

Internal Changes

- System platforming
- Technology changes
- Organisational and location restructuring
- New service introduction
- Change in service provision

Proactive risk management and resilience protects the business and minimises the impact of incidents/ internal changes

Key focus areas

- Third party risk management
- Operational resilience
- Cyber resilience

Essential protective capabilities

Whilst these capabilities are defined by regulatory requirements, developing an overall coordinated approach is much more efficient and maximises the combined protective capability.

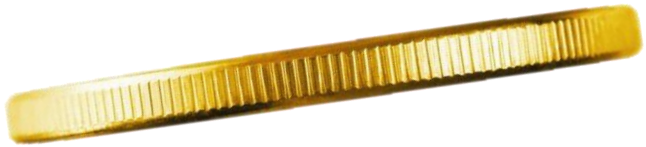
Operational Resilience in practice

"Operational resilience is the ability of firms, financial market infrastructures and the financial sector as a whole to prevent, adapt and respond to, recover and learn from operational disruption"

Flip Sides of the Same Operational Resilience Coin

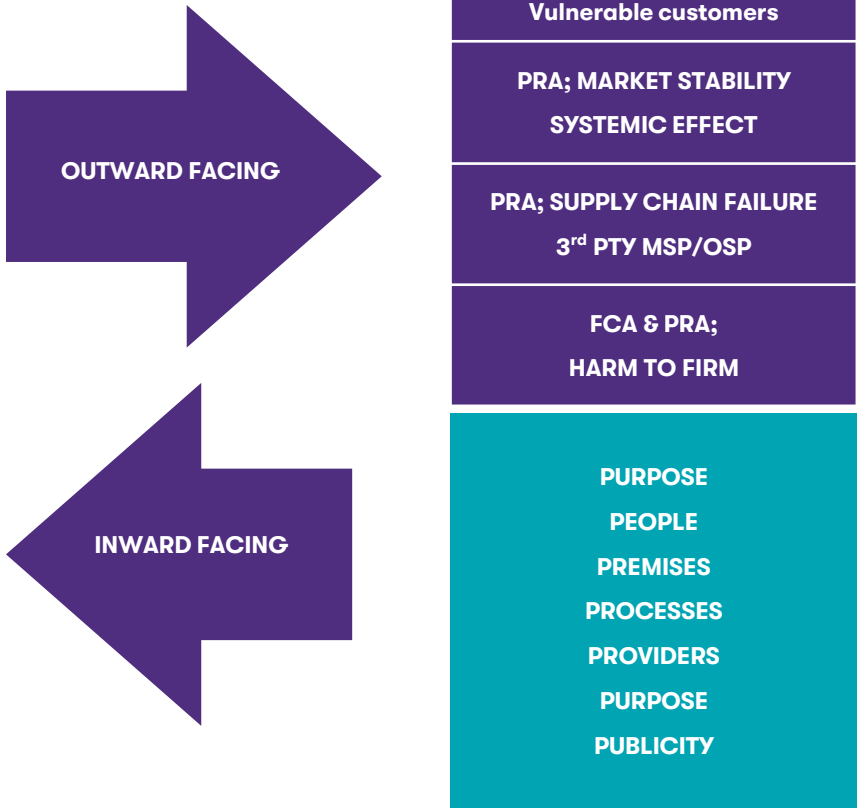
Risk Management

Treat Inherent risks (likelihood and impact) but always left with residual risks



Response

(Emergency Response, Crisis Management, Business Continuity and IT Disaster Recovery, Business Resumption to BAU) Mitigates residual risks



Operational Resilience in practice

"Operational resilience is the ability of firms, financial market infrastructures and the financial sector as a whole to prevent, adapt and respond to, recover and learn from operational disruption"

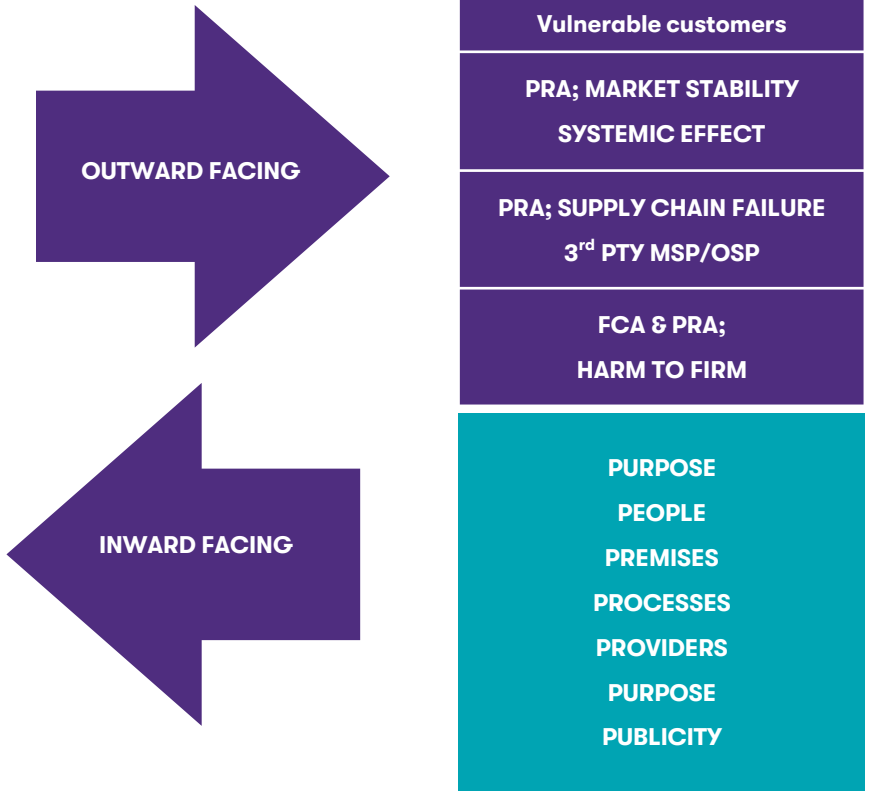
Flip Sides of the Same Operational Resilience Coin

Risk Management

Treat Inherent risks (likelihood and impact) but always left with residual risks

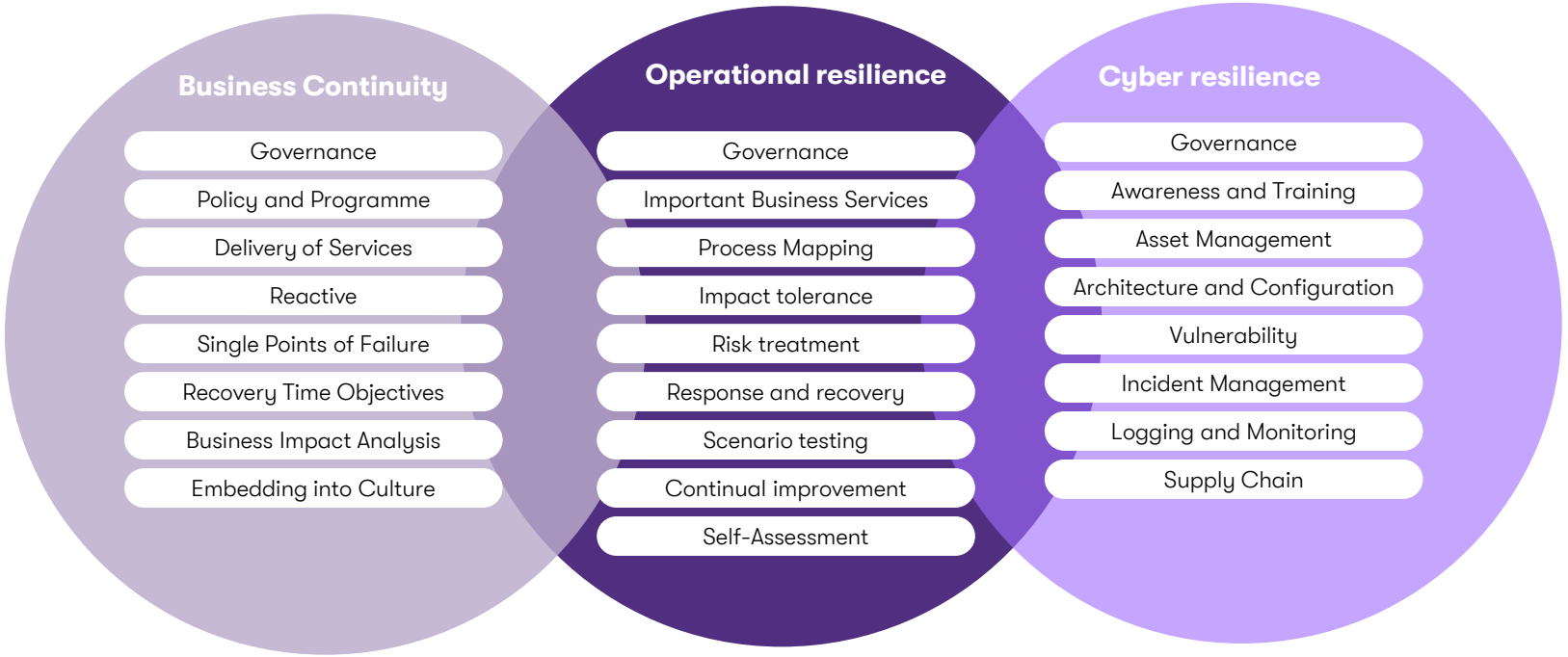
Response

(Emergency Response, Crisis Management, Business Continuity and IT Disaster Recovery, Business Resumption to BAU) Mitigates residual risks



An integrated approach– What we need to do to be resilient and why?

Firms need to comply with various regulations and good practices, it is important to take an integrated approach



Common areas

- Governance
- Incident Management
- Vulnerabilities and Risk Treatment
- Awareness and training
- Rehearsals, scenario tests and exercises
- Third Party/Vendors

DORA | **Payment Resilience** | **Disaster Recovery** | **Consumer Duty**

Third Party Resilience | **Cloud Resilience** | **Data Resilience** | **GDPR**

Our view of the resilience world

Ten steps toward Operational Resilience

Step	Processes
1 Governance	Scope, policy, programme, manual, governance, oversight and RACI (Responsible, Accountable, Consulted and Informed). Annual attestation, OR Framework and Target Operating Model
2 Important Business Services	Identify Important business Services by mapping services that could cause external harm to customers, markets and the supply chain
3 Mapping	End to end process mapping and dependency modelling of business processes supported by resources and technology
4 Impact Tolerance	Setting impact tolerances and metrics to measure relative criticality from the end to end of each important business service
5 Vulnerabilities	Implementation of a risk control to protect against vulnerability or prevent a risk to an important business service
6 Third Party Suppliers, OSP, MSP	Ranking, monitoring and exit strategies for key suppliers, outsourced service partners and managed service providers
7 Communication, Response and Recovery	Reactive plans for emergency response, incident management crisis management business continuity and disaster recovery
8 Stress Testing	Plausible but severe scenarios rehearsed in a simulation leading to risk reduction, improved capability and better plans
9 Continual Improvement	Plan-do-check-act spiral of discovery, investigation, root cause analysis, remediation, re-testing and close
10 Self Assessment	Provide Board level assurance on the status of compliance to the Operational Resilience Regulations

The FCA/PRA implementation deadline for UK Operational Resilience was 31st March 2025. Firms should now prioritise embedding resilience into BAU activities.

Industry insights

As organisations continue to develop their operational resilience programmes beyond the 2025 regulatory deadlines, there are recurring challenges to a successful transition to business-as-usual (BAU) operations.

Common challenges faced by industry peers:

1. Governance structures

Many financial services firms do not have a robust governance structure to support operational resilience implementation. Others lack sufficient oversight from key committees and fail to maintain well-documented governance frameworks – both of which are critical for informed decision-making and accountability.

2. Effective scenario testing

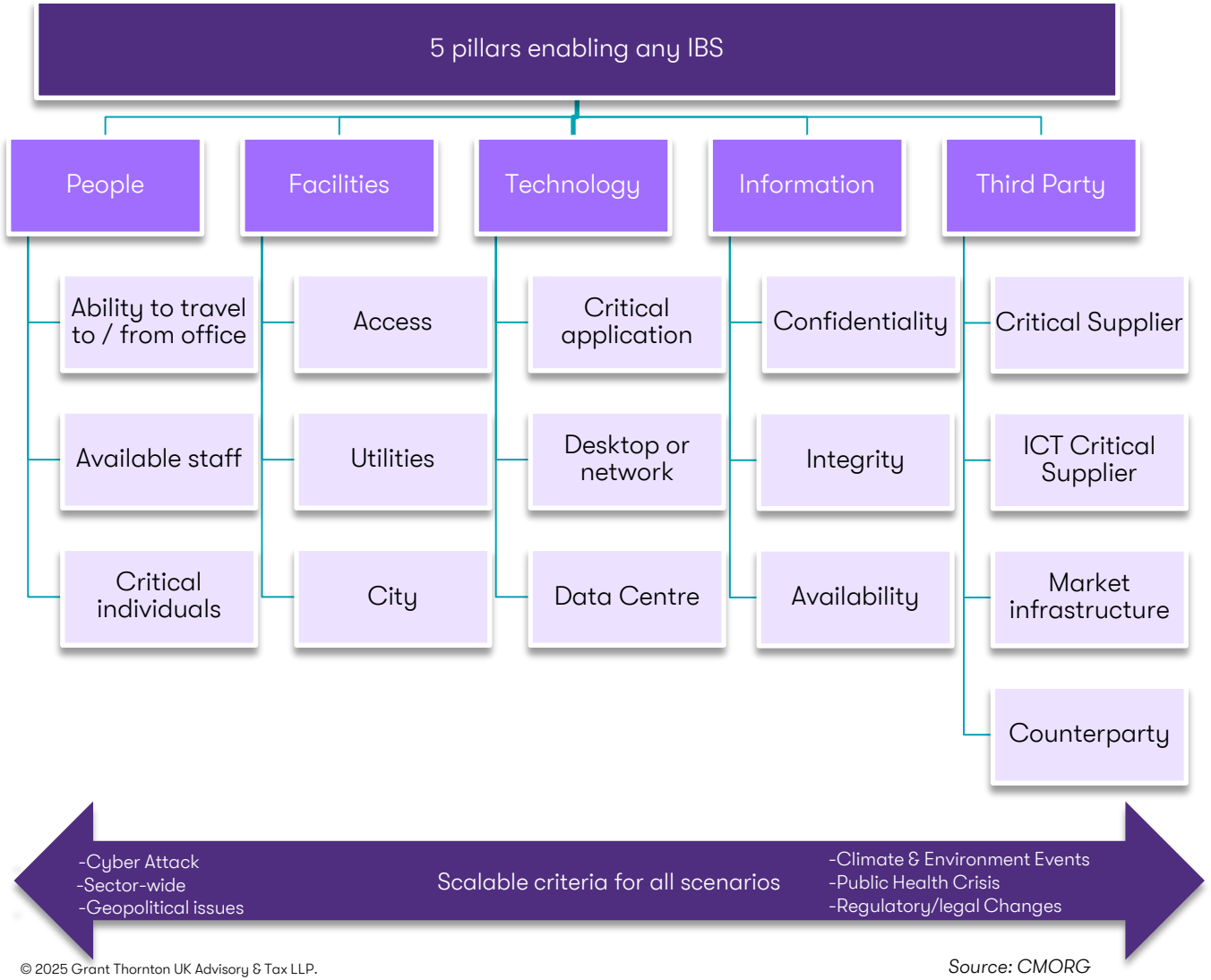
Despite the significant regulatory focus, scenario testing is often limited to basic tabletop exercises, with minimal use of sophisticated simulations or stress testing. Scenario libraries also frequently lack clear risk prioritisation and structured testing methodologies.

3. Third-party risk frameworks

There are significant gaps in integration between operational resilience and third-party risk management. For example, outsourcing dependencies and vulnerabilities related to important business services (IBS) are often overlooked. Furthermore, many third-party contracts don't include formal exit strategies, leaving organisations exposed in the event of supplier failure.

Defining the right scenario for you

Firms should define disruption scenarios clearly, covering causes, risk types (e.g., data integrity, availability), and potential scale, from localised to systemic impacts. This helps assess response effectiveness and ensures preparedness for complex, multi-layered events.



Plausibility in Scenario Design

Scenarios must be realistic, based on known risks and past events, assuming disruptions will impact all critical services. They should reflect vulnerabilities like cyber threats and be supported by well-documented, unbiased assumptions.

Assumptions

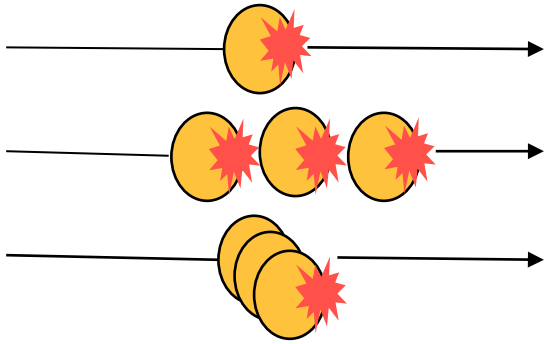
Scenario assumptions should be well-justified and documented, drawing on internal and external incidents to maintain plausibility. Care must be taken to avoid bias and over-reliance on recent events. Key impact drivers to consider include affected customer accounts, timing of outages, physical damage causes, and sector-wide effects.

Compounding impacts of an event

One event at massive scale

Multiple events occurring in succession that has cascading affects

Multiple events at small scale simultaneously



Source: CMORG

Supply Chain Risk: One of the Threat to Operational Resilience

- There is a wealth of information and technical examples on supply chain and third-party risk
- It's essential to frame these within the broader context of operational resilience
- Ensure all relevant risks—especially from critical third parties—are addressed proportionately
- Align activities and assurance with regulatory expectations from the outset
- Many assessments are technical and complex, but your thought process can remain simple and structured
- Avoid diving too deep into technical detail before understanding the overall resilience picture

Understand your supply chain

- Identify key suppliers
- Understand how they support your business
- Don't forget the extended supply chain (4th and 5th parties) for

Supplier risk assessment

- Work out the relative criticality of each supplier to your business
- Understand what risk they pose, were they to exploit vulnerabilities in your defences (accidentally or deliberately) or suffer exploits themselves

Determine security requirements

- Work out what would count as proportionate security requirements for a given supplier based on your assessment of the criticality and potential risk that they represent to your business

Validation and ongoing assurance

- Proportionate approach to confirm that required supplier security requirements are operational and effective
- Use tools and technology to gain efficiencies

What do you need to consider?

Incorporating resilience measures within your firm is a continuing journey, and requires ongoing attention and action

- Is Operational Resilience embedded into your firm's governance and risk management frameworks?
- How confident are you that you will not breach impact tolerances during a disruption?
- How is your Board receiving assurance that resilience capabilities are effective and evolving?
- Are you conducting regular, sophisticated scenario tests that reflect emerging risks (e.g., cyber, geopolitical, third-party failures)?
- Are your internal and external communication plans tested and ready for activation during disruptions?
- Have you reviewed and adjusted your impact tolerances in light of business changes or new threats?
- How are you using scenario testing outcomes to inform remediation and strategic planning?
- How are you managing resilience risks associated with critical third parties (CTPs)?
- Are resilience requirements embedded in third-party contracts and monitored through assurance reviews?
- Is your resilience programme aligned with broader regulatory themes such as Consumer Duty, AI risk, and financial crime?

Questions

Get in touch

Vijay Rathour

Partner, Head of Cyber and Digital Investigations
E: Vijay.Rathour@uk.gt.com
M: +442071844684

Priya Prakash

Associate Director,
E: Priya.Prakash@uk.gt.com
M: +442078652997

Charlotte Devlin

Director,
E: Charlotte.H.Devlin@uk.gt.com
M: +442078652336