



UPDATING YOUR OPERATIONAL RESILIENCE PLANS

How Investment Advisers and Funds
Should Respond to Evolving UK Regulations.

CONTENTS

- 03 NEW CYBERSECURITY RULES FOR A CHANGING THREAT LANDSCAPE**
- 04 ACTION 1: ESTABLISH WRITTEN CYBERSECURITY AND CYBERSECURITY PLANS, POLICIES, AND PROCEDURES**
- 06 ACTION 2: REVIEW, DOCUMENT, AND ENFORCE ACCESS MANAGEMENT BEST PRACTICES**
- 07 ACTION 3: DEPLOY DATA PROTECTION POLICIES AND TECHNOLOGIES**
- 08 ACTION 4: REPORT AND DISCLOSE CYBERSECURITY INCIDENTS AND FORMALISE RESPONSIBILITY AND ACCOUNTABILITY**
- 09 TAKING ACTION TO MANAGE CYBER RISK**



NEW OPERATIONAL RESILIENCE REQUIREMENTS FOR A CHANGING THREAT LANDSCAPE

Initially updated as a response to the pandemic, the FCA's Operational Resilience policy provides a framework for advisers and funds to strengthen the way the financial sector can prevent, adapt, respond to, recover, and learn from operational disruptions.

Leading firms across the industry are putting in place frameworks to understand their operational resilience capabilities, resources, and preparedness to answer critical questions for the FCA, including (as written):

- Does your firm have a board-approved cyber security strategy?
- How does it identify and protect its critical assets?
- How does it detect and respond to an incident, recover the business, and learn from the experience?

The FCA's Operational Resilience policy itself focuses on five key areas that firms must be able to demonstrate:

1. To develop internal and external communication plans when services are disrupted and prepare self-assessment documentation.
2. To identify the important business services that would cause intolerable damage to consumers or the market if they were disrupted.
3. To establish impact tolerances for these services – the maximum level of disruption that can be endured while still able to deliver.
4. To carry out mapping and testing to identify vulnerabilities and assess whether services can remain within impact tolerances under different harmful scenarios.
5. To identify, prioritise, and invest in your ability to respond and recover from disruptions effectively.

We've created a series of four action points aligning with these key areas – intended to support your existing efforts to achieve compliance, secure your business against disruption, and help build trust with regulators and clients.



ACTION 1

ESTABLISH WRITTEN RESILIENCE AND CYBERSECURITY PLANS, POLICIES, AND PROCEDURES

Already, most firms maintain guidelines that govern their resilience with a specific focus on cybersecurity. However, formalising your operational resilience plans, policies, and procedures is a best practice, and forms the basis of all your resilience efforts.

THIS SHOULD INCLUDE:



Assessing, categorising, and prioritising your unique cyber risks and aligning cybersecurity with your specific business model.



Identifying and classifying your business-critical information architecture and data assets.



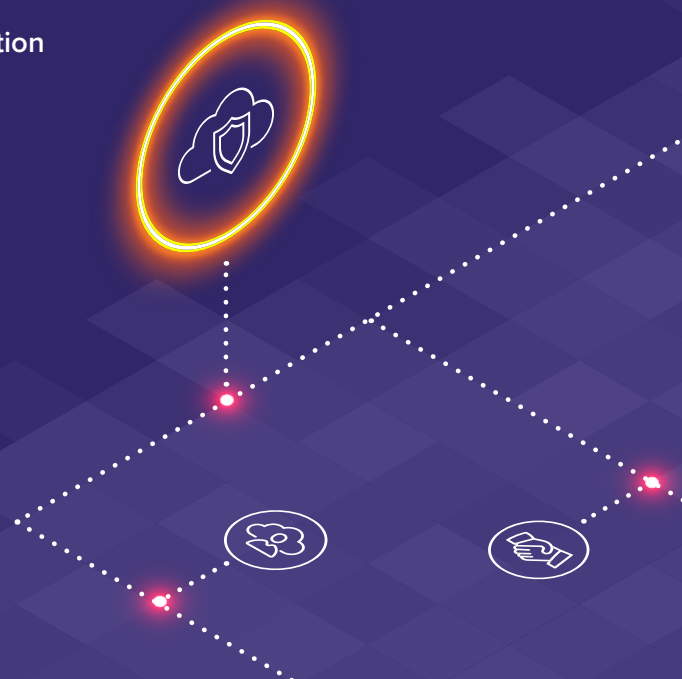
Identifying critical service providers that have access to your data – you're still responsible for protecting the data you outsource to an IT platform or service.



Ensuring policies and procedures are kept up to date, especially after substantial changes to your environment. Review them at least annually.



Making sure documentation is easily retrievable.



WHEN UPDATING YOUR OPERATIONAL RESILIENCE PLANS, RE-EXAMINE YOUR APPROACHES TO:



DETECTION

You can no longer rely on piecemeal solutions for threat detection. Extended detection and response (XDR) platforms, for example, combine the statistical analysis of security information and event management (SIEM) with complete visibility across environments and endpoints. XDRs enable proactive threat responses through automation and by providing increased levels of intelligence to SOC teams.



RESPONSE

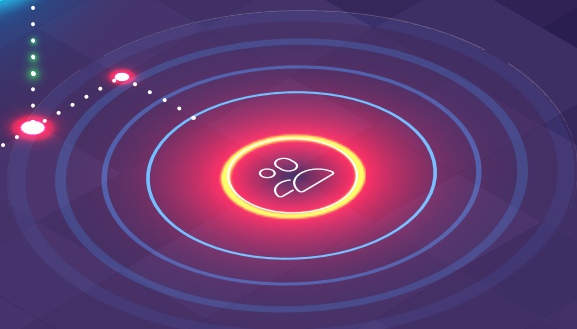
Your response plan will differ depending on your unique risks and business requirements. A playbook for responding to common cyber events will help avoid the shortcomings of ad hoc response. Conduct tabletop exercises, with clear response metrics, to fine-tune your playbook.



RECOVERY

Rapid and complete recovery is essential for business continuity and maintaining regulator and client confidence. Consulting a trusted cybersecurity partner with fine-tuned recovery processes through real-world experiences can help.

Finally, if you outsource IT platforms or data services to a vendor, you should be able to continue operations even if their systems are interrupted by a cyber event. Make sure you have procedures for handling data on an alternative system or briefly sustaining processes manually.



ACTION 2

REVIEW, DOCUMENT, AND ENFORCE ACCESS MANAGEMENT BEST PRACTICES

Where previously there have been suggestions for how to manage data access, there are now best practice rules for access management. This includes Acceptable Use Policy (AUP), Principle of Least Privilege (PoLP), and multi-factor authentication (MFA).



AUP

This stipulates behaviours and constraints users agree to in order to access data, including the management of credentials during onboarding, offboarding, and the start and end of projects. In short, terminating credentials when they're no longer needed.



MFA

True MFA combines what you know (a password), what you have (a device), and what you are (a biometric such as a fingerprint). This will also require an understanding of your network perimeter. Where before this was the four walls of your office, with cloud computing, software-as-a-service, and remote workforces, your perimeter is in constant flux.



PoLP

Where users only have permission to use the information resources, they need to do their job. This calls for a clear understanding of your systems, SaaS platforms, and your data.



REMOTE ACCESS

This doesn't only apply to employees. Contractors, partners, vendors, and other third parties also require MFA.



ACTION 3

DEPLOY DATA PROTECTION POLICIES AND TECHNOLOGIES

As you know, safeguarding your data requires a deep understanding of your data landscape. Not only to keep data secure based on its sensitivity level and importance to operations, but also allow you to communicate to regulators and clients whether data has remained protected.

Technologies and methodologies to support you to protect data include:

SEGMENTATION

Segregate datacentres, cloud environments, and networks to keep data separate based on sensitivity level or value to business continuity.

ACCESS CONTROLS

Employ tools and best-practice methodologies to manage data access.

THREAT DETECTION AND PREVENTION

Deploy automated tools and services (including SIEM/XDR) to detect and prevent threats.

VULNERABILITY MANAGEMENT

Leverage vulnerability assessments and remediation to uncover malware, backdoors, hosts communicating with botnet-infected systems, and webservices linking to malicious content.

MOBILE DEVICE MANAGEMENT

Avail yourself of tools or services to ensure proper device configuration, restrict sensitive data from devices, and remotely wipe devices when necessary.

DATA ENCRYPTION

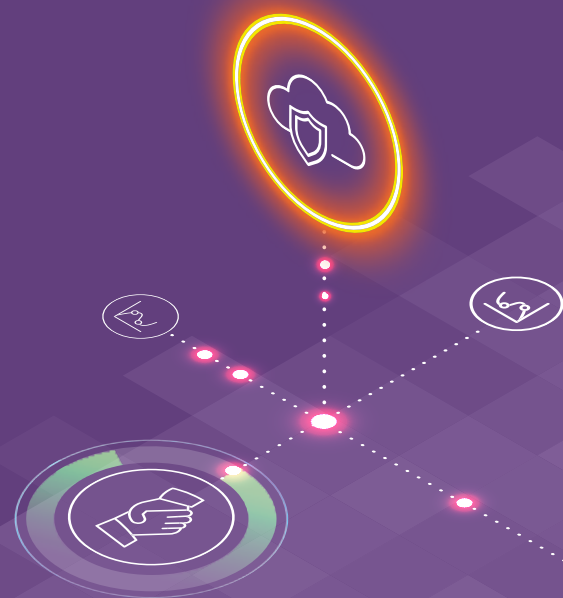
Encrypt data while at rest on hard drives and while in motion over networks.

VULNERABILITY SCANS AND PENETRATION TESTS

Identify cyber risks and update applications with security patches (and hardware and software configurations) to protect against zero-day threats. You also need to demonstrate to regulators and clients that prescribed processes are being followed.

USER TRAINING

Make sure employees are well-versed in managing passwords, recognising and responding to phishing attacks, and other basics of cyber hygiene. Contractually require vendors to meet minimum cybersecurity standards and to promptly report cyber incidents.



ACTION 4

REPORT AND DISCLOSE CYBERSECURITY INCIDENTS AND FORMALISE RESPONSIBILITY AND ACCOUNTABILITY

With firms having to notify the FCA immediately after they become aware of an incident – or have information which suggests an incident has occurred or may occur – operational resilience plans require a detailed and tested process.

When looking at your existing incident response plan, have you established clear roles and responsibilities that enable you to report promptly and accurately? Take the opportunity to document who will lead the response and which team members will perform which response actions.

We would also recommend that you:



ESTABLISH THE RIGHT TONE AT THE TOP

This is the best way to create accountability throughout an organisation, with your board reviewing and approving all cyber-related policies and procedures. It should also accept ultimate responsibility for the health of your cyber program. However, this is a new level of engagement that not all boards will be prepared for. Work with your board members to bring them up to speed.



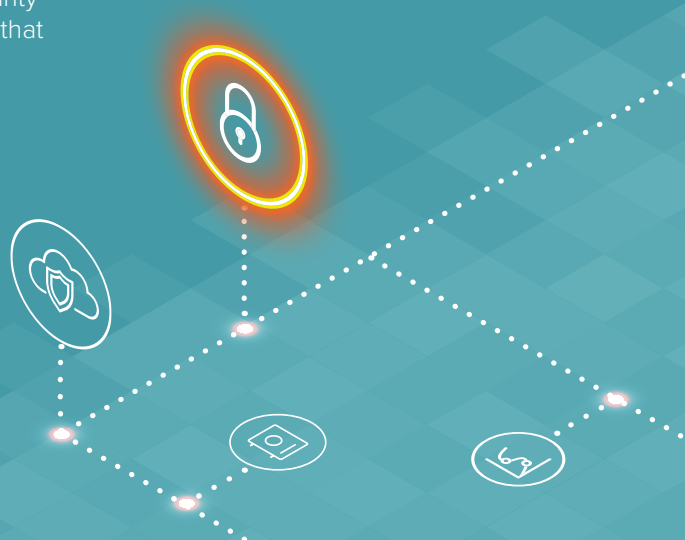
PROMPTLY INFORM THE BOARD OF CYBER INCIDENTS

This is a key enabler of board accountability. Equally important is a process to keep the board apprised of your cybersecurity posture, including vendors that handle firm data.



ESTABLISH METRICS FOR CYBER RISK MANAGEMENT

Measure against them, and report to the board in a clear, consumable manner on a monthly, quarterly, and annual basis.



TAKING ACTION TO MANAGE CYBER RISK AND ENSURE OPERATIONAL RESILIENCY

As operational resiliency and cybersecurity best practices become policy, investment advisers and funds must establish clear requirements to mitigate against cyberattacks and report cyber incidents as they occur.

It will become imperative for you to identify, protect against, and mitigate cyber risk in a more focused and formal way. You'll need to identify your information assets both inside and outside your network, understand your workflows and vulnerabilities, and deploy effective technologies and methodologies to reinforce your cybersecurity posture.

Firms will no longer be able to relegate responsibility or delay adoption. Taking action to comply with the new rules, strengthen cyber programs, and reinforce client trust will take time, focus and effort. The time to begin is now.

Ready to take your cybersecurity beyond lights on?

Contact ECI today for assured business acceleration through technology.

800.752.1382. | eci.com

ABOUT ECI

ECI is the leading provider of managed services, cybersecurity and digital transformation for alternative financial services organisations across the globe. With its unmatched platform of solutions, ECI provides assured business acceleration through technology, partnering with clients to drive innovation. More than 1,000 customers worldwide with over \$3 trillion of assets under management put their trust in ECI.

US: +1 800 752 1382

UK: +44 207 071 6802

Singapore: +65 6622 2345

Hong Kong: +852 3189 0101

For more information visit: **www.eci.com**