


Justin

One of the
RSM team



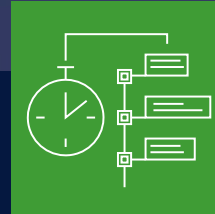
Cyber incident response exercise

Cyber incident response exercise (table-top and live-play)



Cybercrime shows no signs of slowing down

The UK National Cyber Security Centre (NCSC) claims that **over 70%** of medium and large businesses experienced cyber-attacks in the **last 12-months**. These attacks are taking place on an almost **continuous basis**, with victims likely to suffer significant financial impact, data loss, reputational damage, and operational disruption.



Businesses need to do more in order to be ready

To effectively counter a cyber-attack, it's imperative for businesses to go beyond merely having a response plan; they must ensure plans are both robust and thoroughly tested to confirm their efficacy. This requirement is heightened given most businesses are reliant on their 3rd party service providers, hence knowing they can react effectively in the event of a cyber-attack is key to a cyber incident response.



Partnering with RSM to support you with all things Cyber

By working with our dedicated specialist Cyber team to design and facilitate a cyber incident response exercise you will:

- understand **potential ramifications** of your response actions to a cyber-attack;
- learn about different threat actors that may **target your business**, and their strategies; and
- identify **strengths** and **areas of improvement** in your response plan

Value of performing cyber incident response exercises

Businesses that exercise their cyber incident response plans can significantly reduce the damage caused by a cyber-attack. Accordingly, it is crucial that exercises are tailored with well-considered cyber-attack scenarios. This enables you to learn and continually improve your preparedness and business response as part of operational resilience efforts.

Based on our experience cyber incident response exercises should:



Support preparedness

Test your capability to detect and respond to cyber-attacks by proactively exercising your response plans. Exercises should be tailored to your operational context and consider parties you are dependent on.



Be scenario driven

Exercises should be relevant, realistic and consider the likely cyber threats your business faces. Cyber-attack scenarios should include a focus on attacks that have taken place in your industry or sector.



Improve business resilience

There is an increasing expectation by customers, suppliers and regulators that regular exercises are performed, with the output used to generate learnings to improve your risk position and prepare you to withstand a cyber-attack.

How RSM can help

We work with businesses to design and facilitate tailored cyber incident response exercises that simulate a real-world cyber-attack, creating a realistic experience where your response team are required to make quick, high-impact and critical decisions.

Our approach to delivering a cyber exercise includes:

01

Understanding your business and threats

Creation of scenario and tailoring including:

- working with you to understand your systems, threats, past cyber events and critical impacts; and
- performing threat research to establish relevant cyber-attack scenarios appropriate to your business.

02

Crafting real-world exercises

Create an incident response exercise and live-play script considering existing response plans and attendees:

- Our tailored material allows you to experience communication styles and tactics used by threat actors in real attacks; and
- simulates the speed and complexity of a real-world cyber-attack to force high impact response and decision making.

03

Facilitated exercise

A highly immersive and engaging test of your response capability with a simulation of how an actual cyber-attack unfolds:

- experience a critical cyber-attack in a safe environment, testing your decision making, containment, eradication, recovery and communication strategies.

04

Debrief & 'lessons learnt' report

Recommendations to capture learnings, opportunities for improvement and evidence to satisfy regulators, customers and suppliers:

- end of exercise debrief to capture immediate learnings and provide feedback; and
- final report with findings from the exercise and recommendations to improve your response processes.

For further information contact:



Stuart Leach

Partner

Technology & Cyber Risk
Assurance

stuart.leach@rsmuk.com



Sheila Pancholi

Partner

Technology & Cyber Risk
Assurance

sheila.pancholi@rsmuk.com



Richard Curtis

Director

Technology & Cyber Risk
Assurance

richard.curtis@rsmuk.com



The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction.

The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM UK Corporate Finance LLP, RSM UK Legal LLP, RSM UK Restructuring Advisory LLP, RSM UK Risk Assurance Services LLP, RSM UK Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP and RSM UK Creditor Solutions LLP are limited liability partnerships registered in England and Wales, with registered numbers OC325347, OC402439, OC325349, OC389499, OC325348, OC325350, OC397475 and OC390886 respectively. RSM UK Employer Services Limited, RSM UK Tax and Accounting Limited and RSM UK Management Limited are registered in England and Wales with numbers 6463594, 6677561 and 3077999 respectively. RSM Northern Ireland (UK) Limited is registered in Northern Ireland at Number One Lanyon Quay, Belfast, BT1 3LG with number NI642821. All other limited companies and limited liability partnerships are registered at 6th Floor, 25 Farringdon Street, London, EC4A 4AB. The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm which practises in its own right. The RSM network is not itself a separate legal entity in any jurisdiction.