4Di Incident Responsive Exercising

Threat-led cyberattack simulations Immersive experience through a cloud-based platform

Data-driven output for robust improvements

Why should you run IR exercises?

A cybersecurity breach can strike at any time, putting your entire organization at risk.

As many organisations are recognizing and experiencing first -hand, cyberattacks are no longer a matter of if, but when. Recent cyber breaches at housing associations highlight the increasing sophistication, stealth, and persistence of cyberattacks that organisations are facing today.

These breaches result in increased regulatory oversight and often have a negative business impact. The loss of intellectual property, customer data, and other sensitive information can cause severe financial and reputational damage.

KPMG conduct threat-led cyber incident response exercises – tailored to your organisation – that will enable you to take proactive measures to improve your resilience and respond confidently to future cybersecurity incidents.

KPMG's Approach to Incident Response Exercising

Preparation

KPMG will discuss with you what you want to get from the exercise, which areas and levels of the organisation will be involved, and agree exercise objectives. We will outline our methodology, including data collection and analysis, and begin our review of key documentation.

Development

We will use threat modelling and cyber intelligence to develop a realistic simulated attack on your organisation, following workshops with key personnel including the CISO, Head of IT, CIO, COO and more. We engage with representatives of business areas as well as system and service owners – to tailor the exercise and ensure it is targeted, impactful, and asks the rights questions of the right people.

Execution

We will configure the simulation in our cloud-based tool, 4Di, and hold a dry run with you to ensure it meets your requirements. Our experienced security consultants will deliver a pre-exercise briefing to confirm scope, objectives, key roles and rules of engagement before facilitating a fully immersive exercise, tailored to suit the maturity level of your teams and intricacies of your organisation.

Analysis and Recommendations

Immediately after the exercise we hold a hot debrief to reflect on performance and lessons learned. We will then analyse all data collected through 4Di and develop a detailed report with insights, strengths, weaknesses and remediation actions. This is evidence -based and aligned to industry best practice, and will enable you to take immediate action to improve your cyber resilience.

¾ Nearly ¾ of organisations have had at least one cyber attack in the last year[1]

£3.2m Total average organisational cost of data breach in 2021[2]

KPMG combines advisory capability and experience in IR along with leading edge technology – to ensure you are prepared.

4Di insight

KPMG's 4Di platform enables detailed exercise data analytics and robust enhancements in cyber resilience. Other benefits include:

Versatile and adaptable to any scenario

- Built within a web and cloud-based environment for exceptional flexibility
- Tool can be used for any scenario and can be tailored easily to the association and all roles within
- Enterprise grade feature set with multiple inject media types (e.g. Google maps, Facebook, Twitter, audio and video)
- Fully customizable injects, even during an exercise, that can be tailored to the business, any process or system

Immersive training platform to continuously develop staff professionally

- Easy to use, intuitive platform that replicates the pressures of live incidents
- Suitable for team and individual development, with the ability to generate individual, participant participant-level metrics instantly
- Staff can access full CPD records and have their own personalized learning log

Data capture into single platform

- All data from exercises is captured into 4Di platform contemporaneously
- Enables comprehensive data collection, robust analysis of results, and evidenced and auditable improvement actions
- All participants have access to the platform, enabling everyone's viewpoints to be heard

Cost and time efficient

- Bespoke exercises can be developed rapidly, reducing lead times
- Reduced costs from BYOD and no need for fixed premises
- Increased efficiency due to accessibility of tool. No fixed premises are required, and tool can be accessed on any device via the internet.

How it works

- Traditionally, PowerPoint and paper feeds have been used to deploy injects. This has worked well for single room exercises, but is limited in terms of participant interaction and data collection. There is also limited ability to control and adjust the simulation in real real-time, which prohibits truly dynamic and immersive exercising.
- With 4Di, participants log in to a web web-based portal in which all exercise injects are delivered. From a user perspective, it is simple to register and engage with the platform, which presents the scenario in an intuitive and immersive interface. Users can log in from any device, from any location. The platform integrates with Teams, Zoom and other communication channels.
- 4Di simulations can be run across multiple locations, incorporating supply chains/third party providers, and with 100+ participants. Its success is built upon considering cyber incidents in the context of your organisation's overall incident response strategy to exercise and train your approach within a positive learning environment.

> KPMG led a well well-structured and challenging major incident scenario event bringing to the table practical experience from the industry as well as thought leadership of major incident management. Delivered at the right time and right way to our senior leadership team.
>
> **Major UK Bank**

For more information, please contact:

Mike Nelsey
Director, Risk Consulting, KPMG in the UK
mike.nelsey@kpmg.co.uk

kpmg.com/uk

1BCI Cyber Resilience Report 2021 2IBM Cost of a Data Breach Report 2021