Capgemini

Cyber Crisis and Incident Exercises G-Cloud 15

Table of Contents

1 Service Overview

Cybersecurity incidents are increasing and can strike without warning. When a security incident occurs, the response must be decisive and effective however, this often goes untested until a real incident happens.

Security incident response and investigation can be more complex in cloud integrated environments where multiple third party delivered services are employed, resulting in more operational security interfaces, more channels to manage, and uncertain accountabilities.

Capgemini has proven experience in designing, developing and delivering interactive simulation exercises. These exercises simulate a rapidly evolving scenario as a result of a security incident, using a variety of multimedia and subject matter expertise to test leadership teams' ability to respond effectively, navigating business, operational, technical and security risks whilst handling internal and external stakeholders including customers, senior managers, regulators and the media.

GDPR Incident management exercises can help the Buyer arrange constant data protection within their organisation and help test existing internal procedures to confirm that data protection is taken into account at all times (these can typically include policies and procedures regarding security breach preparedness, management of access or rectification requests, modification of data collected, vendor management, etc.).

This service supports cloud-based projects and services.

2 Business Need

The increasing dependency on digital services and supply chain complexity (through the adoption of integrated commodity services) has increased both the attack surface, impact of a security breach and the need for GDPR compliance within organisations. It is now widely accepted that security breaches are inevitable and that the ability to respond rapidly and confidently to a detected incident is critical to ensure the impact is contained and to facilitate a rapid recovery. The fallout from such incidents, and the associated cost when not handled effectively, is often overlooked or not tested.

Cloud and digital service adoption can provide the Buyers with new business opportunities and the ability to reach more citizens or consumers. However, as more third parties and channels may be involved in delivering services, there are more interfaces and third-party risks to manage. It is important for Buyers to ensure that their third parties and cloud service providers have incident response, business continuity (BC) and disaster recovery (DR) arrangements and that they provide the means for investigations to be conducted when needed whilst also maintaining the function, security and reputation of the business during an incident.

Capgemini surveys of industry CIOs have identified data security as one of the biggest issues that "keeps CIOs awake at night". IT, more than ever, plays a strategic role for business. Safeguarding critical information assets and business reputation is vital for organisational success. Changes in the technology landscape has increased the vulnerability of most organisations, through increasing supply chain complexity, a growing portfolio of cloud based digital services, growth in end users and devices capable of facilitating misuse of sensitive organisation data, and fraud.

Capgemini offers a comprehensive suite of Cybersecurity services enabled by Cloud technology. These include Phishing simulations, Training, Crisis Exercises, Pre-Mortem workshops, behavioural interventions, and Security Management & Assurance Reviews. All are designed to help organisations secure their business environment and build resilience against cyber threats.

3 Our Approach

Capgemini's Crisis and Incident Exercises service can be used to establish incident response readiness, or to assist with daily incident management procedures.

This can include providing resources to help the Buyers assess and deliver their incident readiness, management and investigations arrangements, and working with the Buyer's services providers including Cloud service providers. The service can test response and recovery playbooks/processes, critical decision-making, internal and external communication, clarify roles and responsibilities, and ultimately handling the fall out of an incident or crisis. These exercises are a key component of building operational resilience, ensuring that organisations can maintain essential services and recover quickly from disruptions.

Capgemini can work with the Buyer to develop authentic security incident scenarios and approaches specific to learning needs of all levels in the organisation. This ensures that preparedness is embedded across the enterprise, from technical teams to executive leadership.

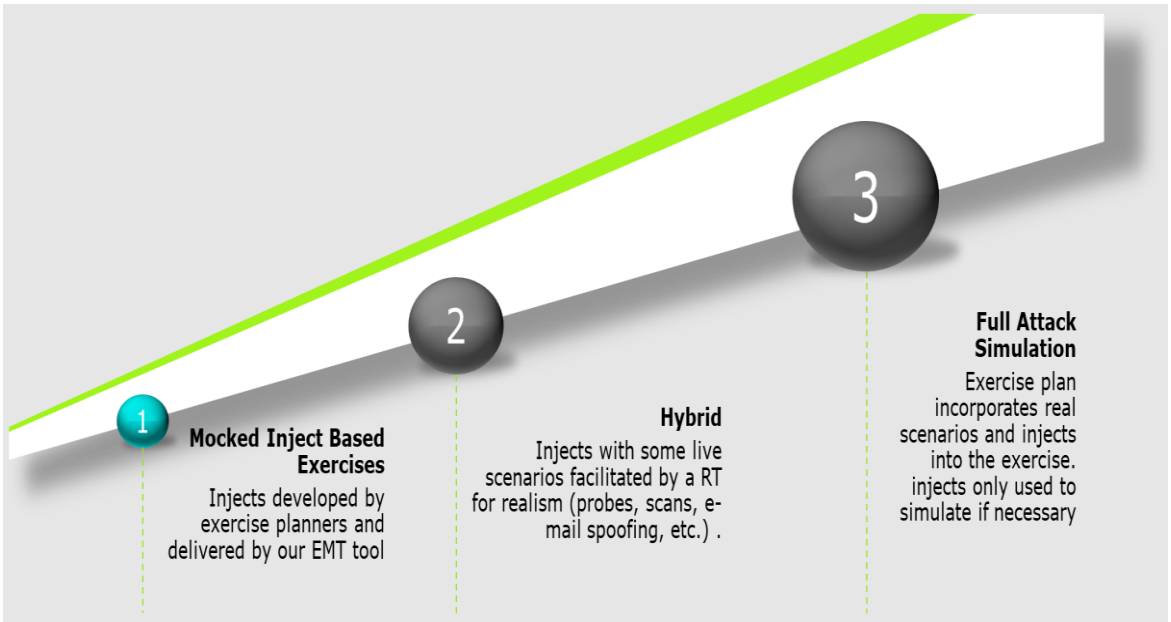
Audience	Objectives	Our Approach
Executives/Leadership	Providing Incident & Crisis Leadership	Simulated Crisis Exercise
Management	Coordinating response across teams, disciplines and departments	Pre-Mortem Workshops
Operational Staff	Ability of any single area to respond effectively and efficiently	ThreatStorming activities

Targeted to executives and by collaborating with subject matter experts in technology, business, and operations, Capgemini can identify incident scenarios that are realistic and based around the exploitation of a feasible vulnerability. Capgemini can plan the event meticulously by the minute, consider what options and recommendations would be provided by Subject Matter Experts (SMEs) in a real-life scenario, and understand the growing impact that is likely to progress as the incident develops.

For operational teams, Capgemini can also provide competencies including our 'ThreatStorming' methods and analytical techniques. ThreatStorming is an activity Capgemini use to encourage business engagement through describing threats or risks the organisation faces through a simple step-by-step process. This technique can provide value to crisis and incident exercises by accelerating the development of assets including threat scenarios, threat modelling tools, exercise designs and facilitation methodologies.

We will use our catalogue of analytical ThreatStorming techniques, including cyber-kill chain analysis, system/journey mapping, crisis injects, 5-whys, forced ranking, disruptor exercises, role-playing, affinity diagramming, and more to define and deliver an effective crisis and incident exercise. For management and team leads, we would design Pre-Mortem workshops to test response playbooks and identify what really happens during recovery from a catastrophic cyber incident. These workshops are effective in engaging team leads and management across the recovery organisation, and refining recovery processes to what actually occurs within a unique organisational culture and context.

Depending on the risk appetite, business requirements and the cyber incident management processes within an organisation, we can offer a range of exercises and approaches from the use of mocked injects on our Exercise Mastery Tool to a full-blown simulated attack.



This diagram is for illustration only and does not represent any obligation or responsibility of Capgemini.

To support the realism of the event, Capgemini can prerecord video and/or audio 'injects' that include news media reports, phone calls, online news and social media content and simulated messages from senior stakeholders to help create a pressurised environment for the tested team's decision making, alongside regular reporting of situational changes that reflects actual incident management reporting from operational teams. SMEs from inside and outside the organisation can be made available to respond to queries and direction.

The planning and delivery of an exercise will typically consist of the following steps:

No.	Step	Description
1	Objective Setting	Determine audience, learning objective, device scenario, identify key stakeholders
2	Detailed Design	Working with our combined SMEs, a detailed design is created, identifying impacted parties understanding the technical detail of the incident, culminating in a detailed flow of the day.
3	Exercise Preparation	Realistic injects are designed, ranging from emails, internal reports, system logs, newspaper articles and other media. Where applicable they are loaded onto our Exercise Mastery Tool to create cohesive script for the exercise.
4	Exercise Run	Coordinate and facilitate the exercise working together with client teams using physical facilities as well as virtual tools such as our Exercise Mastery Tool and mobilising our ThreatStorming capabilities.
5	Feedback and Evaluation	Following the exercise, a comprehensive evaluation is undertaken to identify improvements and drive an improvement plan

Events typically take a minimum of 3 hours, comprising 2-2.5 hours of active scenario delivery and further time spent in self-evaluation. However, exercises are flexible and can be tailored to suit the Buyer's specific requirements and time frame.

Where appropriate, we can use our Exercise Mastery Tool (EMT) **that has been developed to facilitate large scale incident and crisis simulation exercises**. The EMT is a flexible and accessible digital tool where **exercise content and scenarios can be** loaded into**.** The tool provides a single interactive interface to deliver injects, record responses and drive the exercise script. This tool is very useful where one or more remote team need to participate in an exercise.

Capgemini can work with the Buyer to develop skills, accreditations, certifications and training plans for personnel, so the Buyer better understands the business and technical impact of vulnerabilities and risks to their business without being dependant on a third party.

4 Buyer Responsibilities

Please refer to the Supplier Terms listed with this service on the Platform. These may contain additional Buyer obligations/costs the Buyer is subject to that are not identified anywhere else in the Supplier's Application or on the Platform.

The Buyer responsibilities as part of this service are as follows:

- The Buyer will provide a project/engagement manager to act as a single point of contact and an escalation route for the full duration of the project/engagement.
- The Buyer will be responsible for providing detailed requirements by the mutually agreed date.

If these responsibilities do not match your expectations, then please contact us in order to explore options to vary our approach.

5 Service Management

Not applicable.

6 Protection of Data

This service is based on a security classification of 'Official', however should you have a requirement for a different security classification that you would like us to consider, please contact us to discuss.

7 On-boarding and Off-boarding

Capgemini shall undertake on-boarding and off-boarding activities agreed within the Order Form (including as a minimum an exit plan in line with the Call-Off Contract terms) which will be charged for in accordance with the Pricing section for this service.

8 Skills and Knowledge Transfer

Capgemini recognises that skills and knowledge transfer is a critical element in the provision of G-Cloud services to public sector clients. Where possible and applicable, this forms part of the delivery plan for the service agreed at the start of the engagement. Our consultants and engineers are experienced in providing skills and knowledge transfer for major private and public sector clients.

Where appropriate, we may use a standard approach, tailored to topic, skills-gap and individuals, to ensure consistency and effectiveness. The approach, Capgemini's Assess-Plan-Implement framework, has been used repeatedly by our teams to structure the work involved in transferring skills and creating new teams capable of driving and sustaining change long after the end of the formal programme. The framework can be applied throughout a project to understand knowledge transfer objectives, plan training delivery methods and materials, and deliver and evaluate success.

9 Vendor Accreditations/Awards

For the 13th year in a row, Capgemini has been recognised as one of the World's Most Ethical Companies® by the Ethisphere® Institute. This is an acknowledgement of our ethical culture that makes us an employer of choice and responsible player in the eyes of our clients, shareholders, and the wider community.

ISO 9001 Quality Management for Management Consultancy and IT Implementation and services to the Public Sector

ISO 27001:2013 - Provision (Delivery) of IT services including business applications development, maintenance and Data, Digital and Cloud technologies.

NelsonHall has identified Capgemini as a Leader in its 2022 NEAT Vendor Evaluation for Learning Services due to its ability to meet future client requirements as well as its capability to deliver immediate learning benefits to them.

Capgemini is the first amongst consultancy and technology firms to be recognized six times in a row for its thought leadership reports.

2023 Ecovadis Platinum Rating: We maintained a platinum rating, recognising us as a responsible and sustainable business in the top 1% of companies assessed.

Better Society Awards: Our collaboration with Code Your Future to offer digital skills training won a Better Society Award in 2022. The awards celebrate efforts by commercial organisations to create a better society.

Inclusive Top 50 UK Employers List: We achieved second place in the Inclusive Top 50 UK Employers List 2022/23 – a list that assesses companies for best practice on diversity, equality and inclusion

UK Best Workplaces for Women: We were listed as a Best Workplace for Women by Great Place to Work®. This listing is based on responses from our team to an anonymous survey about their employee experience.

UK Best Workplaces for Wellbeing: We are listed by Great Place to Work® as a Best Workplace for Wellbeing

Great Place to Work: We were certified as a Great Place to Work® in 2023, reflecting our employees' experience of working at Capgemini in the UK.

10 Sub-contractors

Capgemini UK may use the following subcontractors to deliver this service:

- Capgemini Technology Services India Limited.

11 Business Continuity and Disaster Recovery

No disaster recovery plan is provided as part of these Services.

12 Pricing

This service is priced in accordance with the SFIA Rate Card attached. Capgemini can also provide offshore resources at reduced rates where appropriate. Projects can be priced either on a Time & Materials or Fixed Price basis.

13 Ordering and Invoicing

Please refer to the Supplier Terms for this service.

We would be pleased to arrange a call or meeting to discuss your requirements of our service in more detail.

14 Termination Terms

Please refer to the Supplier Terms for this service.

15 Further Information

In addition to Cybersecurity crisis and incident exercises, Capgemini can provide a range of cybersecurity services such as – cybersecurity awareness, behaviour and culture, cybersecurity maturity, strategy and transformation, security management, governance risk and compliance, architecture design & implementation, identity and access management, cyber analytics & protective monitoring, digital forensics and testing.

Capgemini has over 500 security professionals based in the UK whose expertise can be leveraged to provide Buyers with cybersecurity services.

For more information about this or any of Capgemini's G-Cloud services, please contact our Public Sector Team.

Phone: 0370 904 4858

Email: publicsector.opps.uk@capgemini.com including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.

About Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Make it real. | www.capgemini.com