RESTRICTED
ACCESS

Resilience is key

www.restrictedaccessltd.co.uk

Table of contents

Crisis and Resilience

Collaborate in preparation to improve resilience in a crisis.

It is with increasing importance that business leaders prepare and respond well in a crisis. We will help you prepare and respond to direct pressures as a result of the crisis enabling the growth of your business.

No crisis is the same; each can have diverse impacts that can advance rapidly or build as the fog lifts through time. We support our clients through the challenging situations involved in the crisis while understanding that business leaders can feel the effects of a crisis for a prolonged period.

Our multi-skilled subject experts will dovetail with you and your team to provide professional advice to help reduce risk.

To achieve the 'cyber muscle memory', which will enable you to respond successfully, it is essential that the crisis planning is a fundamental part of the preparation and integrated into business plans. When a crisis does occur, you will have exercised and tested your plan to ensure your business is resilient. We will work together with you to build trust, understand business risks, and develop strategies so that you are prepared when the inevitable happens.

Our methodology follows the National Institute of Standards and Technology (NIST) guidance on contingency planning along with the NIST Computer Security Incident Handling Guide.

About Us

We are an organisation that believes that you need to be prepared by having the correct bespoke documentation and exercise using your documents. The NCSC states, “Organisations must test and practice their response to crisis, including cyber-attacks”.

We have credible experience working in the MOD, British Military, RAF, Military Intelligence, Military Cyber, Government Signals Intelligence (GCHQ), and Big 4 Cyber Resilience inside all verticals.

We will provide you with the tools and training to help lift the fog when the inevitable happens. We use the OODA loop (Observe, Orient, Decide, Act) approach to help you prepare, respond, and recover to Incidents and Crisis. Our training and documents will help you move quickly to the most appropriate decision, while also understanding that changes are inevitable as further data becomes available.

What we offer

1. Cyber Incident Response document suite
2. Cyber Crisis exercising
3. Targeted Attack Discovery (Threat Hunting)

Cyber Incident Response Documentation

Cyber Incident Response Documentation

We will provide you with the full suite of documents, bespoke to your organisation, which will be practical and useful during an incident or crisis. If you already have these documents, we are skilled at making sure that the documents are appropriate for your organisation and industry.

Policy

We know that the Policy governing incident response is highly individualised to the organisation. However, most policies will include the same essential elements:

- Statement of management commitment
- Purpose and objectives of the policy
- Scope of the policy (to whom and what it applies and under what circumstances)
- Definition of computer security incidents and related terms
- Organisational structure and purpose of roles, responsibilities, and levels of authority. This should include the authority of the incident response team to confiscate or disconnect equipment and to monitor suspicious activity, the requirements for reporting certain types of incidents, the requirements and guidelines for external communications and information sharing and the handoff and escalation points in the incident management process
- Prioritisation or severity ratings of incidents
- Performance measures
- Reporting and contact forms
- How will the incident be managed, and are there any requirements for specialists joining the incident team?
- What third party support required? This could include forensic IT specialists
- Risks, decisions, and issues to consider
- Guidance on communications and lines to take – this should be debated and exercised so that there is a structure in place already
- Relevant Business Continuity Plans and Disaster Recovery strategies
- What actions can be taken to support those affected, and what support are you going to give the victims of the incident?
- What matrices should be used and monitored to check the effect on the organisation?
- Priorities and predetermined objectives for this type of incident
- Other – under this heading, an example would be, ‘what data do we hold’, if this playbook were for a breach of the staff database, we would already know what data we hold

Plan

Organisations should have a formal, focused, and coordinated approach to responding to incidents, including an incident response plan that provides the roadmap for implementing the incident response capability. Each organisation needs a plan that meets its unique requirements, which relates to the organisation’s mission, size, structure, and functions. The plan should lay out the necessary resources and management support. The incident response plan should include the following elements:

- Mission
- Strategies and goals
- Senior management approval
- An organisational approach to incident response
- How the incident response team will communicate with the rest of the organisation and with other organisations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organisation documentation

The organisation's mission, strategies, and goals for an incident response should help in determining the structure of its incident response capability. The incident response program structure should also be discussed within the plan. Once an organisation develops a plan and acquires management approval, the organisation should implement the plan and review it at least once a year to ensure that the organisation is following the roadmap for maturing the capability and fulfilling their goals for incident response.

Procedures

Procedures should be based on the incident response policy and plan. Standard operating procedures (SOPs) are a delineation of the specific technical processes, techniques, checklists, and forms used by the incident response team. SOPs should be reasonably comprehensive and detailed to ensure that the priorities of the organisation are reflected in response operations. In addition, standardised responses should minimise errors, particularly those which might be caused by stressful incident handling situations. SOPs should be tested \ exercised to validate their accuracy and usefulness, then distributed to all team members. Training should be provided for SOP users; the SOP documents can be used as the instructional and statutory notifications required, including time frames and what information is needed? For example, reporting to regulators, including Information Commissioners Office (if in the UK) and the stock market.

Playbooks

We will provide you with playbooks to guide you through incidents and crisis, which have been proven to be prevalent within your organisation and industry. It is highly recommended that these playbooks are exercised along with the rest of your document suite to build your team's cyber muscle memory. The playbooks will include, where necessary the following elements:

- Type of incident – Denial-of-service attack, Ransomeware, Insider Threat, Phishing Attack, Malware Attack etc.
- Likely means of detection – This will include the main ways the incident could be detected
- Likely impacts – which part of the organisation might be affected? E.g. ransomware could stop all company systems, but data loss may not affect actual systems
- IT plans in place for dealing with it and their strategy for recovery – we will cross-reference the relevant IT plans
- Who needs to be informed of the incident, internally and externally? This is a crucial part so that you can quickly identify all those who might be affected. There should be information on how to contact your staff if the IT systems are down
- What are regulatory and statutory notifications required, including time frames and what information is needed? For example, reporting to regulators, Information Commissioners Office (if in the UK) and the stock market

- How will the incident be managed, and are there any requirements for specialists joining the incident team? Which team will handle the incident, and do you need specialists, such as external public relations help, plus legal and compliance people on the team?
- What third party support is required? This could include forensic IT specialists
- Risks, decisions and issues to consider
- Guidance on communications and lines to take – this should be debated and exercised so that there is a structure in place already
- Relevant Business Continuity Plans and Disaster Recovery strategies – are there manual workarounds which can help the response?
- What actions can be taken to support those affected, and what support are you going to give the victims of the incident?
- What matrices should be used and monitored to check the effect on the organisation? How do you tell if your response plans are successful?
- Priorities and predetermined objectives for this type of incident
- Other – under this heading, an example would be, 'what data do we hold', if this playbook were for a breach of the staff database, we will already know what data we hold on staff

Cyber Crisis Exercises

Cyber Incident Response
Cyber Crisis Exercises

We offer bespoke crisis exercises specialising in cyber incidents. We have had practice over the last two years of running our exercises fully remote. Our method has successfully been tried and tested during the recent pandemic. Our remote exercises have all the benefits of our face to face offering. Whether your staff are still in the office or working from home, your whole team will be able to rehearse and improve cyber incident response plans.

The exercise will either be in person or remote. They will include:

- Workshops including business and technology to ensure realism
- Exercise delivery face to face or via interactive video conferencing
- Simulated media, stakeholder and public interaction
- Post-exercise reporting which will include a Hot-debrief after the exercise

Stage 1: Workshop

Our workshops are designed to not only educate but to exercise the cyber muscle memory required in an incident or crisis. Bespoke to your organisation, we will lift the fog which exists in non-exercised teams.

Workshops are a great start to building a more complex exercise, or as an introduction to less mature teams. Typically lasting for a couple of hours, they are intended for both business and the technical audience, who are both involved in incidents or crisis.

Stage 2: Desktop

Desktop exercises are intended to build awareness by exploring credible cyber incident scenarios in a safe, secure and passive environment.

Facilitated by an experienced Subject Matter Expert (SME), our desktop exercises are based around scenarios that are relevant to your organisation and industry. They are for installing that muscle memory into all levels of the organisation involved in the crisis, from the Cyber Security Incident Response Team (CSIRT) to the C-suite. These exercises are on average, 3 - 4 hours in duration.

Stage 3: Simulation

Only for those with a higher cyber maturity, who have exercised previously; simulations are a great way to rehearse your incident response processes with realism, safely.

Our SMEs construct a credible scenario, using role-players to simulate media, regulators and client interest, as your incident unfolds. Simulations often have a duration of one or two days, which provides the time to explore strategies and practice making difficult decisions while under realistic pressure.

Stage 4: Wargaming

Our most advanced offering and only for the mature audience, our wargaming package ensures that your organisation has the tools, for when the inevitable happens.

A wargame provides the ideal opportunity to practice cross-function involvement, stress-testing your teams against the worst-case scenarios. Players will be fully immersed within a realistic, multi-day exercise where they will need to make decisions and then defend them. Business members and technical teams will be wargamed; detecting, analysing and mitigating realistic threats, which closely represent the latest Tactics, Techniques and Procedures seen in the wild, attacking organisations like you.

Restricted Access Targeted Attack Discovery (Threat Hunting)

Restricted Access Targeted Attack Discovery (Threat Hunting)

Restricted Access Targeted Attack Discovery will be valuable if you are concerned about attacks directed towards your organisation and your industry. If you have noticed suspicious behaviour in your systems, or if your organisation recognises the benefits of regular preventative inspections, this is worth consideration.

The service helps to discover:

- Ongoing attacks
- Attacks that occurred in the past
- Compromised systems

Your report will include recommendations on how to remediate attacks and prevent similar incidents in the future.

How our service works

Our experts detect, identify and analyse your infrastructure, providing expanded visibility. We aim to uncover malicious activities, identify the possible sources and provide you with for the most effective remediation. We do this by:

- Analysing the specific threat landscape of your organisation
- Conducting in-depth inspections of your IT infrastructure and data (such as log files) to identify possible signs of compromise
- Analysing your outgoing and incoming network connections for suspicious activity
- Using hypotheses to uncover probable sources of an attack and other potentially compromised systems

Results

Our findings are delivered in a detailed report covering:

- General information confirming your network is compromised or signs that it is
- Analysis of the intelligence gathered including relevant threats and indicators of compromise (IOC)
- Description of possible attack sources and compromised network components
- Remediation recommendations to mitigate the impact of an incident and protect your resources from similar attacks in future
-

Threat Hunting in Detail

Restricted Access Targeted Attack Discovery stages

Gathering and analysing data on attacks from external sources. The aim at this stage is to obtain a snapshot of the attack surface of a company whose assets are, or were, being targeted by intruders. We tap into a variety of intelligence sources, including underground cybercriminal communities, as well as internal monitoring systems. Analysing this intelligence allows us to identify weaknesses in a company's infrastructure that are of interest to cybercriminals including compromised accounts, stolen data and much more.

Onsite or remote data collection and early incident response. This stage sees data collected from workstations, servers, SIEM systems and other equipment in your infrastructure. Data can be assembled onsite or remotely using software provided to the customer within the framework of the service. In case of suspicious activity, experts collect evidence related to the incident, which may include: log files, applications and network equipment, web traffic logs, network traffic dumps, HDD images, memory and any other information which could be used in an investigation. If required, Interviews with your representatives and third parties can also be included.

Evidence analysis. Restricted Access performs analysis of all available information (including malware analysis if required) to recreate the picture of the incident. The customer may be asked to provide additional data (via email or various network resources, depending on the type and amount of data requested).

Report preparation. The work carried out within the framework of the service concludes in a final report. It contains the results of data analysis from external sources, as well as descriptions of detected attacks based on analysis of the data collected in your organisation's infrastructure. The report also contains best practice and remediation recommendations for the detected attacks.

Contact us for further information and Pro bono engagements

About Restricted Access

Restricted Access LTD is a company registered in
England and Wales with company number 12716144

VAT Registration Number: 355 0919 90

Contact us

Registered Office: 71-75 Shelton St, West End, London WC2H 9JQ

Telephone: +44 (0)7735 928594

Email: info@restrictedaccessltd.co.uk

RESTRICTED
ACCESS