“...No organisation is too large or too small to fall victim to a data breach. No industry vertical is immune to attack. Regardless of the type or amount of your organisation’s data, there is someone out there who is trying to steal it...” 2019 Verizon Data Breach Investigations Report

A Cyber Security Exercise tests and evaluates your organisation’s ability to detect, investigate and respond to cyber attacks in a timely and secure manner. Yet according to recent ISF research many leading, global organisations have not run a cyber attack simulation, leaving response plans untested and so vulnerable to failure in the event of a breach. How prepared is your organisation?

WHAT DOES RUNNING A CYBER SECURITY EXERCISE MEAN FOR YOUR ORGANISATION?

ISF Consultants bring a wealth of experience and expertise to the preparation and design of your Cyber Security Exercise. Leveraging ISF tools such as the annual Threat Horizon forecast as well as hands-on experience with diverse global organisations, ISF Consultants increase your ability to deliver and gain maximum benefit from a Cyber Security Exercise.

Working with ISF Consultancy enables you to:

- Identify vulnerabilities in your attack response plans across people, processes, and technology.
- Develop procedures for agile and structured cyber attack response.
- Increase awareness among key stakeholders about the nature and scale of cyber attacks
- Effectively stress test your organisation e.g. following a re-structure, merger or acquisition

Adversarial threat events are often initiated in a particular sequence, forming a five-stage cyber attack chain

- ISF Cyber Security Exercise report, 2019
THE ISF APPROACH TO DELIVERING AN EFFECTIVE CYBERSECURITY EXERCISE

Our consultants will follow three key steps with selected members of your organisation:

A: PREPARE

ISF consultants’ thorough approach at this stage ensure that the exercise meets objectives, runs smoothly, and delivers value to your organisation. The team interview key stakeholders to understand your critical business functions, select appropriate ‘targets’ (such as technical infrastructure, physical devices, specific locations), and assess any constraints to ensure the exercise is both realistic and achievable. Working with you and your team we design scenarios to best fit your organisation, considering; types of exercise, such as table top or digital simulations, phishing exercises and red and blue teaming, and relevant threats drawn from Threat Horizon reports or mimicking real-life reported incidents. The team then confirm scope, agree success metrics, and develop a playbook for running the exercise.

B: RUN

ISF consultants will immerse your participants in customised and realistic attack scenarios where they must handle a range of physical and cyber attacks, collaborating to achieve an effective response. Participants typically include members of the following groups: Security, Security Operation Centre, IT, HR/Communications, senior Business Executives, and Legal. The exercise(s) can usually be completed in one day and our team both observe and provide feedback immediately after the exercise.

C: FOLLOW-UP

ISF Consultants produce a detailed report that reviews the cyber security exercise, evaluating effectiveness (i.e. your preparedness for a cyber attack) and detailing learnings for your organisation. The report also includes prioritised recommendations for improvement and key findings to share with your wider stakeholder group. Our team can assist with communicating results and actions to the business as well as with implementing recommendations for remediation and enhanced protection.

KEY DELIVERABLES

- Cyber security Exercise playbook
- A detailed report highlighting areas of strength and weakness
- Prioritised recommendations for improvement
- ISF Consultancy can also support your implementation of this plan across the wider organisation.

“Scenario-based testing of your cybersecurity incident response capability is a high-impact way of engaging your response teams (which includes executive leadership and not just the IT team).”

- ISF Member, Financial Services

For more information, contact:
Steve Durbin, Managing Director
US: +1 (347) 767 6772
UK: +44 (0) 7785 953800
steve.durbin@securityforum.org