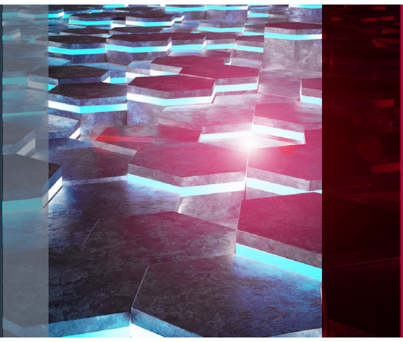
Information
Security
Forum

DELIVERING AN EFFECTIVE CYBER SECURITY EXERCISE



Cyber attacks are steadily increasing year on year.[1] Organisations are constantly under threat with over two-thirds experiencing data breaches in 2017.[2] Consequently, cyber security preparedness and resiliency are becoming increasingly important to the protection of an organisation's information. One way of improving the ability to handle cyber attacks is by running cyber security exercises.

Cyber security exercises are simulations or tests of some nature, based on a cyber attack scenario. They test the organisation's ability to detect, investigate and respond to cyber attacks in a timely, effective and secure manner. The results of a cyber security exercise should help the organisation identify areas of improvement in people, processes and technology, reducing the impact should a real cyber attack occur.

EVOLUTION OF EXERCISES

Scenario planning, simulations and exercises are not new concepts. Armed forces have found tangible benefits in running 'war-gaming' exercises for thousands of years.[3] They learn from their experience in a safe manner so that in the event of conflict they know how to react and what to do.

The same preparatory concepts have evolved over time and can be adapted to the information age in the form of cyber security exercises. These exercises help to train participants, improve processes (e.g. cyber attack handling and incident response) and highlight technology that needs updating or replacing.

THE BUSINESS PROBLEM

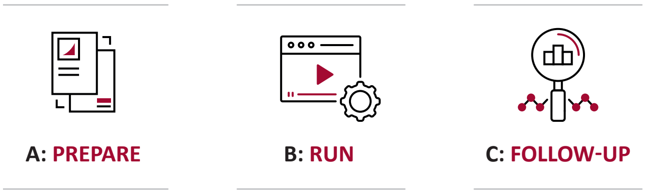
ISF Members may struggle to deliver effective cyber security exercises, with many concerned about how to:

- define tangible benefits of performing a cyber exercise
- select the most appropriate types of cyber exercise to perform
- evaluate their level of ability to handle cyber attacks
- understand and apply best practice when performing a cyber security exercise.

PURPOSE OF THE REPORT

This report provides a structured approach for exercise controllers and facilitators to prepare, run and follow-up cyber security exercises.

Figure 1: The ISF Approach for Delivering an Effective Cyber Security Exercise



The report highlights reasons why organisations choose to run cyber security exercises and the benefits of running them.

It helps Members to design cyber attack scenarios and is supported by sample cyber security exercise playbooks that organisations can tailor to create their own.

The main focus of the report is on table-top and digital simulations, but the content also applies to other types of exercises, including red and blue teaming, penetration testing and phishing exercises.

[1] T. Seals, "Cyberattacks Doubled in 2017", *InfoSecurity Magazine*, 26 Jan 2018, https:/www.infosecurity-magazine.com/news/cyberattacks-doubled-in-2017/

[2] R. Klahr, J. Navin Shah, P. Sheriffs, T. Rossington, G. Pestell, "Cyber security breaches survey 2017", *Ipsos Mori Social Research Institute*, 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

[3] Manuela de Landa, ''War in the Age of Intelligent Machines'', *Swerve Editions*, December 1991, https://mitpress.mit.edu/books/war-age-intelligent-machines

Conclusion

Cyber attacks are commonplace in the modern world; they receive significant media attention and cause real damage to organisations. Performing cyber security exercises can help organisations improve their ability to detect, investigate and respond to cyber attacks in a timely and effective manner.

Cyber security exercises can test a range of targets, such as critical business applications, supporting technical infrastructure or all systems in a particular location. Organisations can run these exercises for a variety of reasons, such as testing if newly restructured business operations can withstand a cyber attack, reacting to a newsworthy cyber incident, or complying with legal, regulatory or contractual requirements.

Merely running a cyber security exercise is not enough. It needs to be based on thorough preparation, including designing cyber attack scenarios, assessing operational constraints and building rigorous playbooks. If the results of the exercise are not used to create and implement comprehensive, achievable action plans, then it will only deliver limited value.

Performing cyber security exercises should be an integral part of any cyber security testing programme. Organisations should investigate how running an effective cyber security exercise can significantly reduce the impact of cyber attacks.

WHERE NEXT?

The ISF encourages collaboration on its research and tools. ISF Members are invited to join the **Process** community on ***ISF Live*** to share experiences and discuss practical and innovative approaches for delivering an effective cyber security exercise.

This is an excerpt from the ISF briefing paper ***Delivering an Effective Cyber Security Exercise***. To purchase the full paper contact:

Steve Durbin, Managing Director
US: +1 (347) 767 6772
UK: +44 (0)20 3289 5884
UK Mobile: +44 (0)7785 953 800
steve.durbin@securityforum.org
securityforum.org

Delivering an Effective Cyber Security Exercise
September 2018

ABOUT THE ISF

Founded in 1989, the Information Security Forum (ISF) is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in cyber, information security and risk management and developing best practice methodologies, processes and solutions that meet the business needs of its Members.

WARNING

This document is confidential and is intended for the attention of and use by either organisations that are Members of the Information Security Forum (ISF) or by persons who have purchased it from the ISF direct. If you are not a Member of the ISF or have received this document in error, please destroy it or contact the ISF on info@securityforum.org. Any storage or use of this document by organisations which are not Members of the ISF or who have not validly acquired the report directly from the ISF is not permitted and strictly prohibited. This document has been produced with care and to the best of our ability. However, both the Information Security Forum and the Information Security Forum Limited accept no responsibility for any problems or incidents arising from its use.

CLASSIFICATION

Restricted to ISF Members, ISF Service Providers and non-Members who have acquired the report from the ISF.

Information
Security
Forum

REFERENCE: ISF 18 09 02