Deloitte.

Cyber Simulation-in-a-box

Are you ready?

Attackers are increasingly motivated to target an organisation's digital infrastructure for financial, personal and political gain. Our increasing dependency on these systems means the impact of an attack can spread across the business as a whole.

Understanding the Threats

The Cyber Simulation scenario and injects have been designed to be used with Board/Senior level participants where they are given Board level roles during the simulation. Through this role-play the participants experience the business impacts and consequences of a major cyber-attack on a mocked-up organisation.

The simulation is split into two moves.
Move 1: Participants focus on crisis management and strategic decision making. The focus is on assessing information being fed to them from their Crisis Management Support Team (CMST).
Move 2: Participants focus on consequence management, in particular with regard to internal and external communications.

Realistic injects have been developed to convey the scenario to the participants. The injects take a number of different formats including media, emails, social media and phone calls.

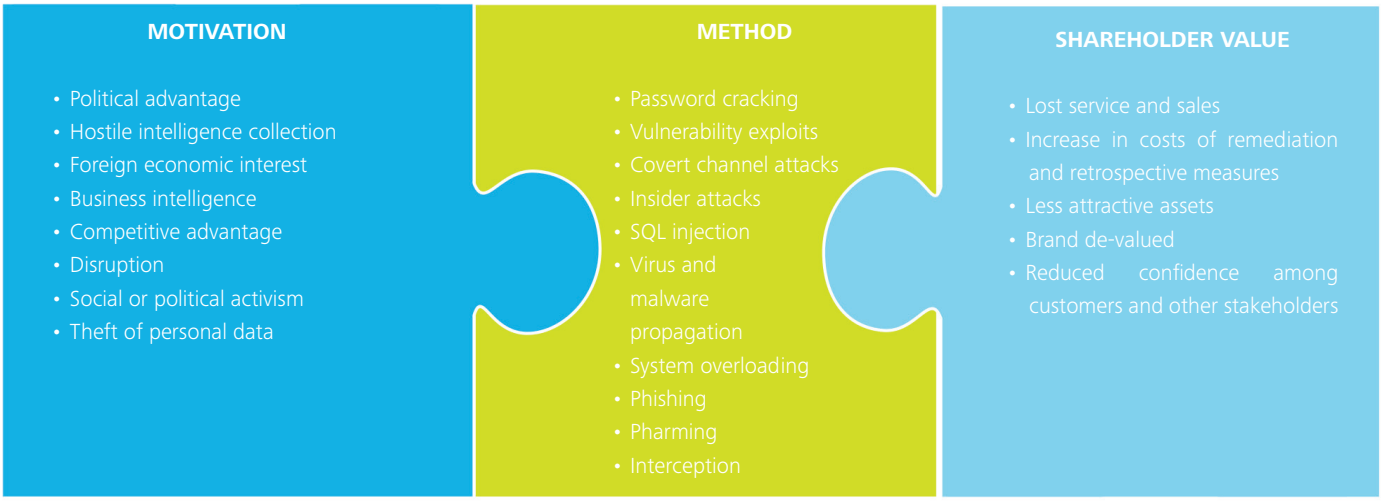
"History has taught us: never underestimate the amount of money, time, and effort someone will expend to thwart a security system. It's always better to assume the worst. Assume your adversaries are better than they are. Assume science and technology will soon be able to do things they cannot yet. Give yourself a margin for error. Give yourself more security than you need today. When the unexpected happens, you'll be glad you did".

Bruce Schneieregal

Why is a cyber attack so impactful?

Many motives and multiple routes of attack which can directly impact shareholders. The following illustration provides examples of cyber attack motivation and method. Preparedness will minimise erosion of value if/ when a significant cyber attack takes place. Motivation, Method and Value relate directly to the way a simulation is designed; developing the scenario, examining the mechanism/response and managing the consequences.

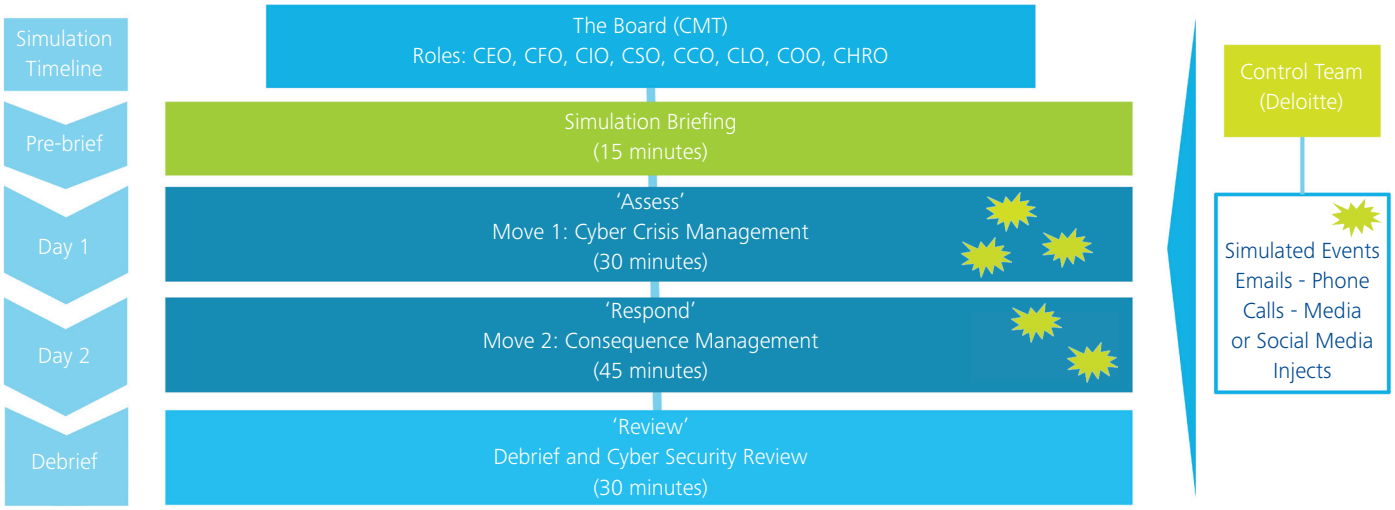
How cyber attacks can affect you:



Cyber Simulation-in-a-box Objectives

- Explore as the Board the business impact of a major cyber-attack during a two hour interactive and engaging role-play session using a fictitious organization.
- Experience strategic decisaion-making during a crisis management period and during a consequence management period.
- Increase your cyber awareness, highlight potential weaknesses and support consensus building at Board level.

Cyber Simulation-in-a-box Objectives



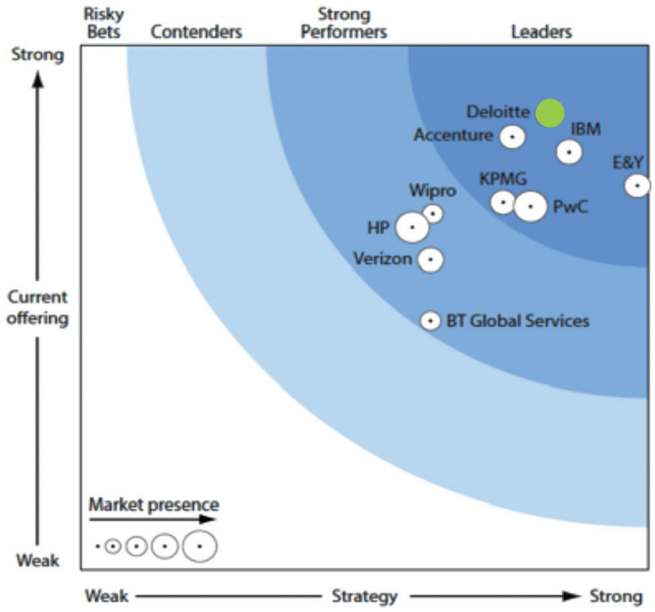
Benefits

By considering what to do prior to a Cyber Attack, organizations can prepare suitable responses based on the inherent capabilities within the organization. This may lead to efficiency and cost savings before an organization attempts to procure external products and services that duplicate existing capabilities. However, when developing such Cyber Attack mitigation strategy, gaps in an organization's existing cyber defences may be identified, which require specialist services to be procured. An in-depth analysis of the gaps exposed will provide an effective scope for procuring specific Cyber Attack mitigation defences and implement them pre-emptively rather than in the midst of an attack.

Monitoring the conditions that would identify a distressed critical business service, having pre-defined, tested stages within a graceful degradation plan, and having criteria for moving between each state allows an organization to respond quickly to detrimental external stimulus during an attack for detailed assessment and robust corrective measures to be implemented.

World Class Services

- Our security experts have the same skills and methods hackers use, but can also translate technical issues into business risks.
- Deloitte has a global reach, with a presence in over 150 countries worldwide.
- We can support you in solving security issues as a trusted advisor in a vendor-agnostic, but knowledgeable way.
- Deloitte has been named a leader by Forrester Research, Inc. in Information Security Consulting in a new report, The Forrester Wave™: Information Security Consulting Services, Q1 2013.



Cybercrime.
Be ready.

Deloitte.

For more information on Deloitte's Cyber Risk Services, please contact:

Panicos Papamichael
Partner, Enterprise Risk Services
Tel.: +357 22 360805
E-mail: ppapamichael@deloitte.com