Prepare for the unexpected
Cyber threat war-gaming can help decrease the business impact of cyber incidents

Overview

Gaining the upper hand in the face of cyber incidents

As society has become increasingly transformed through Internet-based communication and data exchange, cyber threats have increased in both sophistication and frequency. In many organizations, executives know that cyber incidents can lead to high-profile losses, rampant media exposure, and damage to client, customer, or investor confidence. Business leaders have begun to acknowledge that, despite strong security controls, cyber incidents will occur. How heavily they impact an organization's reputation, bottom line, and market standing depends, in part, on how well-prepared the organization is to analyze and contain an incident as it unfolds, respond decisively, and manage the aftermath. *Deloitte's cyber threat war-gaming services help organizations establish "muscle memory" and multi-function coordination to better manage the business crises that cyber incidents can cause.*

Incident response: more than a technical function

A response playbook is not enough

In many organizations, security incidents may occur daily, and are routinely handled by security and technology teams. But some incidents will escalate into significant business crises. Even with well-documented response plans, few organizations are sufficiently prepared. Because the threat landscape changes rapidly, responses cannot be perfectly scripted.

Cyber incidents will occur that require agility and sound judgment in the face of the unknown. These events call for concerted engagement by many organizational functions, including risk management, legal, public affairs, talent management, and technology. Interaction may be required with a wide range of external third parties, including industry peers, regulators, law enforcement, and vendors providing support functions. To reduce damage and impact, organizations need the ability to:

- efficiently assess and determine the scope of the event;
- act decisively to contain the impact and preserve forensic information;
- determine when to engage or report to law enforcement and/or regulatory bodies;
- manage communications to control public and investor perception; and
- activate business continuity and recovery mechanisms.

A fresh approach

Building resilience through practice

Deloitte's cyber simulation and war-gaming exercises immerse participants in a simulated and interactive cyber-attack scenario, allowing organizations to test their response reflexes, identify capability gaps, and train on and develop advanced preparedness techniques. Engagements are led by specialists with deep knowledge of applicable regulations, law enforcement and cyber intelligence, informed by Deloitte's broad experience across many industry sectors. Incorporating methods from military and academic research, our approach has been refined through engagements with multi-national companies, government entities, regulatory bodies, and industry groups. The exercises utilize gamification techniques that appeal to natural human tendencies, and leverage a toolkit of accelerators, such as a repository of scenarios and inject templates, to enhance and expedite war game development and delivery.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Our Cyber Threat War Gaming services

Deloitte's war gaming delivery methods include:

	Option 1 Static simulation	Option 2 Dynamic simulation	Option 3 Live-response simulation
Description/ Approach	A fixed-path war game that leverages predetermined attack vectors and injects that are relevant to the organization's cyber threat landscape	A flexible multi-path war game that leverages an inventory of potential attack vectors and injects that is deployed based upon player decisions, actions, and reactions	An open-ended war game, typically aligned with a baseline threat vector, where players engage a "live" cyber attacker that reacts directly to participant decisions, actions, and reactions
Purpose	Increases cyber awareness and introduces cyber threat concepts to operations/ management	Enables organizations to evaluate their preparedness against a potential and/or likely cyber threat	Stress tests an organization's ability to react to emerging threats and/or simultaneous attacks from persistent/advanced cyber threat actors
Format	1–2 hour single-room war game	3–4 hour multi-room war game	4+ hour "in place" war game
No. of participants	~ 10–15	~ 25	*Varies*

Our Cyber Threat War Gaming toolbox

Deloitte's tools to accelerate the delivery of its cyber threat war gaming services include:

Scenario inventory	Inject inventory	Logistics templates	Educational materials	Delivery templates
An inventory of cyber-attack scenarios — ranging from basic to complex — which include legacy, current and emerging cyber threat vectors.	An inventory of content injects to support various scenario and content delivery needs, including: security alerts, news articles, social media feeds, internal correspondence, automated workflow notifications, mock websites, etc.	Templates to support exercise logistics management, including: task lists, participant lists, exercise room layouts, technology diagrams, inject organizers, etc.	Materials to train cyber war game facilitators, participants, and observers on how to participate effectively in a cyber-war game.	Templates to support war game delivery, including step-by-step facilitation guides, player placemats, kick-off presentations, and debrief surveys

Don't wait for the real thing

It takes practice to hone the organizational reflexes and collaborative judgment capabilities needed to avert or reduce a cyber incident crisis. Deloitte's cyber simulation and war-gaming services can help you…

Build group readiness. Cyber incident response may be unfamiliar terrain for some team members, and requires orchestration among groups that may normally have little direct interaction. War-gaming establishes a response foundation by promoting familiarity with both the people and the tasks that arise.

Strengthen your plans and your people. Enacting response processes simulates the stress of a real incident. It can uncover surprising gaps and weaknesses that need to be addressed, and stimulates the "what if…?" thinking that can improve preparedness.

Develop a common language. Simulation-based learning can demystify security jargon and empower non-technical professionals, and also help technical participants communicate more effectively with business colleagues — interaction that enhances the broader cyber risk program.

Express conviction about cyber threat awareness. Internal news about the cyber war-gaming exercise may be an appropriate way to demonstrate executive commitment to cyber defense, and help reinforce risk-aware organizational behavior.

Secure.Vigilant.Resilient.
To grow, streamline and innovate, many organizations have difficulty keeping pace with the evolution of cyber threats. The traditional discipline of IT security, isolated from a more comprehensive risk-based approach, may no longer be enough to protect you. Through the lens of what's most important to your organization, you must invest in cost-justified security controls to protect your most important assets, and focus equal or greater effort on gaining more insight into threats, and responding more effectively to reduce their impact. A *Secure.Vigilant. Resilient.* cyber risk program can help you become more confident in your ability to reap the value of your strategic investments.

- **BEING SECURE** means having risk-focused defenses around what matters most to your mission.
- **BEING VIGILANT** means having threat awareness to know when a compromise has occurred, or may be imminent.
- **BEING RESILIENT** means having the ability to regain ground when an incident does occur.

Contact us

To discuss your business challenges and solution options, please contact:

Edward Powers
National Managing Partner
Cyber Risk Services
Deloitte & Touche LLP
+1 212 436 5599
epowers@deloitte.com

Emily Mossburg
Principal
Cyber Risk Services
Deloitte & Touche LLP
+1 571 858 1607
emossburg@deloitte.com

Vikram Bhat
Principal
Cyber Risk Services
Deloitte & Touche LLP
+1 973 602 4270
vbhat@deloitte.com

Daniel Soo
Principal
Cyber Risk Services
Deloitte & Touche LLP
+1 212 436 5588
dsoo@deloitte.com

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Copyright © 2014 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited