Anticipating the unexpected
Be ready with simulated cyber threat war games

A proactive approach to combating cyber threats

Cyber threats have continued to increase in both sophistication and frequency, and are increasingly supported by coordinated and well-funded external sponsors with multiple aims and strategies to achieve their objectives. Many of these threats often lead to high-profile losses, rampant media commentary, and client or customer uneasiness regarding the security and privacy of the digital economy.

To prepare for a cyber-attack, many organizations have traditionally taken a monolithic, compliance-oriented approach to security that is focused on evaluating technology controls. With a global marketplace that has been built on sharing, rather than protecting information, a new mindset is required. Organizations should seek to understand where threats are coming from and foster a resilient environment that is able to operate "business as usual" in the event a security incident occurs. Those who recognize the need for vigilance and resilience with security are investing in emerging areas, such as cyber threat war gaming. The objective is to immerse potential cyber-attack responders in a simulated and interactive cyber-attack scenario — allowing organizations to test their cyber incident response, identify capability gaps, and train on advanced preparedness techniques.

The problem

Challenges organizations face in mitigating risk

Malware, virus, network/application Distributed Denial of Service (DDOS), spear- or mass-phishing, code injection, cyber presence vandalism, loss of confidential data, passive wiretapping, and spoofing — all of these attacks can leave organizations at risk of exposure, data corruption, keystroke logging, contact spamming, website defacement, and more. The cascading effect of cyber-attacks like these could ruin a company's reputation and literally put it out of business.

Well-resourced, persistent actors are executing coordinated attacks that become a common mechanism to exert influence and acquire wealth or control. To defend against this, the precision and breadth of organizations' abilities to respond to cyber attacks should continuously evolve beyond what has traditionally been sufficient. Smart organizations realize they need to be vigilant by gaining a better understanding of the cyber risks — seen and unseen — facing their particular business or industry. They are striving to be more resilient by building the capability to continue to operate despite these risks and minimize the business impact at the onset of an attack.

But, even the smartest organizations face several obstacles: a fading perimeter of what an organization must protect; an expanding universe of cyber threats and attacks; traditional viewpoints around the management of cyber risks; dedicated attackers that target high-value assets; and organizational complacency.

As mobile and cloud-based computing become increasingly commonplace, an organization's ability to manage its operating environment decreases while the need to control the same environment continues to grow. Meanwhile, enterprises need to continue to protect themselves from "legacy" threats, which still present real and meaningful risk. Continued and accelerated growth in the set of cyber threats and attacks is another challenge, especially in the context of budget freezes and/or cutbacks.

In today's cyber ecosystem, cross-functional engagement (i.e., with legal, public affairs, human resources, etc.) is necessary for effective command and control during a cyber incident — and many enterprises may not be sufficiently prepared. Organizations should strive to match or exceed the diligence of cyber attackers that prey on their targets' weaknesses and patiently wait for the right circumstances to launch attacks. Even for companies where there is a lack of "an event," there is a need to reenergize their awareness and attention to prevent devastating repercussions.

A fresh approach

An arsenal for successful war games

By extending research from the military and academia, Deloitte's cyber threat war gaming approach incorporates demonstrated methodologies and strategies. We have designed and executed war games at varying levels of depth and breadth for multinational companies, government entities, regulatory bodies, industry groups, and niche organizations.

Deloitte's cyber threat war gaming methodology leverages gamification techniques that appeal to people's natural tendencies — competition, achievement, status, self-expression, altruism, and closure — to drive simulation flow and effectiveness, and a toolkit of cyber threat war game accelerators to enhance and expedite war game delivery.

Our Cyber Threat War Gaming services

Deloitte's war gaming delivery methods include:

	Prepackaged Cyber Exercise	Customized Cyber Exercise	Dynamic Cyber Simulation
Description/ Approach	A packaged exercise with a predefined, single-path war game scenario using attack vectors and injects relevant to the client's industry and/or areas of concern	A single-path or multi-path war game scenario with customized attack vectors and customized injects to address client goals	A flexible, interactive war game where participants engage a "live" cyber attacker who reacts directly to participant actions and decisions
Purpose	Increase cyber awareness and introduce threat concepts and associated risks to management seeking to enhance their cyber threat experience/knowledge	Enable organizations to evaluate their preparedness against a potential and/or likely cyber threat	Stress test the organization's ability to react to emerging threats and/or simultaneous attacks from persistent/ advanced cyber threat actors
Format	1-2 hour, prepackaged war game	3+ hour war game	4+ hour war game
No. of participants	~10-15	~25	Up to 50

Our Cyber Threat War Gaming toolbox

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

PrePackaged Exercises	Scenario Inventory	Inject Inventory	Logistics Templates	Educational Materials
Complete cyber exercises — including a predefined scenario and supporting injects — tailored to introduce and highlight critical cyber threats and issues applicable to various industries.	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 Operations Center (SOC) 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.

The Deloitte difference

Our differentiated services include:

- **Robust simulation design.** Deloitte leverages a specialized combination of military and academic rigor, gamification techniques, and prior global experience to design and execute war games in an efficient and expedited manner.

- **Depth and breadth of cyber experience.** Deloitte's dedicated network of cyber security professionals supports our clients to design cyber security strategies, execute capability enhancement programs, configure and operate systems/infrastructure, interpret and prioritize intelligence, etc. — enabling our practitioners to understand critical risk areas, common pitfalls, and active and emerging cyber threats.

- **Industry knowledge.** Deloitte practitioners support organizations in every global market segment, which promotes an understanding of the unique cyber issues and challenges organizations face in each industry and sector.

- **Risk-based approach.** Deloitte's methodologies focus on maximizing risk impact at minimal effort and cost — supporting our clients' efforts to meaningfully manage risk exposure while being conscious of business operations.

Contact us

To discuss your business challenges, please contact:

Edward Powers
National Managing Principal
Deloitte & Touche LLP
+1 212 436 5599
epowers@deloitte.com

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

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