UNISYS | Securing Your Tomorrow™

Cyber Resilience Services - Understanding potential threats, eliminating vulnerabilities, and having a trained and ready organization

Point of View

"There are no secrets to success. It is the result of preparation, hard work, and learning from failure."

- Colin Powell

Cyber Resilience wargames are conducted in realistic environments that help you understand:

- *Client/competitor action-reaction*
- *Unintended consequences*
- *Changes to the competitive landscape*
- *Preparation for and response to risk*
- *Development of strategies to rehearse, stress test, and improve strategic actions*

"Private-sector preparedness is not a luxury; it is a cost of doing business in the post-9/11 world. It is ignored at a tremendous potential cost in lives, money and national security."

- The 911 Commission Report

In today's complex cyber environment, the need for cybersecurity and ability to defeat cybercriminals continues to rise. It's estimated that by 2019, the cost of data breaches to business will increase to $2.1 trillion – four times the cost of incidents in 2015.[1] "No locale, industry, or organization is bulletproof when it comes to the compromise of data."[2]

Cyber resiliency helps the client cope with these threats through a comprehensive, in-depth cybersecurity program that's designed to anticipate, respond, and manage threats and potential impact – in essence taking the guesswork out of cyber defense. Cyber Resilience wargames are a highly successful way to prepare and ensure your organization's readiness. The resilience testing and planning team places the client in a simulated real-world threat scenario that helps assess cyber incident response proficiency, and exercises human and technological processes, resolution and decision-making capabilities, all of which are vital in defeating a potential threat. Cyber Resilience wargames can also be used to explore specific issues and conditions needed to develop procedures and processes that improve the overall resiliency posture of the client.

Conducted in stable, unthreatened environments that allow failure without repercussions to resources, fiscal assets or the brand, Cyber Resilience wargames encourage new, out-of-the-box thinking across an organization's internal and external functions. Based on the Department of Defense's time-tested procedures, the National Institute of Standards and Technology (NIST) standards, and Unisys' cyber commercial best practices, the wargames and exercises are tailored to each client's specific needs, and focus on an organization's ability to successfully detect, respond, and remediate a range of cyber threats.

[1]Juniper Research, "Cybercrime and the Internet of Things," May 12, 2015, p. 6. Accessed on August 30, 2016 at http://www.juniperresearch.com/document-library/white-papers/cybercrime-the-internet-of-threats

[2]Verizon, "Data Breach Investigations Report," 2016, p.6. Accessed August 30, 2016 at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Cyber Resilience wargames deliver a roadmap that guides improvement, development of new capabilities, allocation of resources, and signals impending change to the operating environment. Consequently, leaders are empowered to agilely and adaptively prepare their firms to deter, deflect, and if necessary, respond to emerging challenges or crises that could impact the life blood of their organization – in short, increase their resiliency proficiency.

01/17 17-0029