Deloitte.

Deloitte's Cyber Threat War-Gaming Services Help C-Suite, Technical Staff Prepare, Respond and be Resilient to Cyber Attacks

New York, August 1, 2014 — Deloitte's Cyber Risk Services practice today announced the commercial availability of its cyber war-gaming and simulation services, bringing together the broad spectrum of people required for concerted response to cyber-attacks. Deloitte's cyber war-gaming and simulation services are part of a broader portfolio of resilient services that help organizations minimize the impact of cyber incidents.

"Business leaders are coming to accept that even with the best security defenses in place, cyber incidents will occur," explains **Ed Powers**, national managing principal of Deloitte's Cyber Risk Services. "Although a well-constructed incident response manual is necessary, this alone does not create the reflexive judgment capability that organizations may need if a security incident becomes a true business crisis. War-gaming trains diverse teams of responders to act rapidly to reduce the business disruption and costs often associated with cyber incidents, as well as to minimize brand and reputation damage."

Deloitte's cyber threat war-gaming approach draws on the strengths of its broader Risk Advisory capabilities, relies on leading thinking from the military and academia, and incorporates lessons learned from war-game simulations conducted for multi-national companies, government entities, regulatory bodies and industry groups. Deloitte served as objective observer and co-authored the "**After Action**" report for Quantum Dawn 2, a simulated systemic cyber attack on the U.S. financial system sponsored in June 2013 by the Securities Industry and Financial Markets Association.

Many organizations conduct technical rehearsals of their incident response plans, but Deloitte's cyber threat war-gaming services involve CEOs, CFOs, risk officers, talent (human relations) officers, legal counsel, and corporate communications teams, as well as technical responders.

"When a cyber attack threatens critical operations," said Mary Galligan, a director in Deloitte's Cyber Risk Services, "business leaders may need to make quick decisions to off-line core systems or applications. Executives may need to guide communications with media, customers, investors and regulators. Collaboration with law enforcement and industry peers may also be essential in limiting the exposure of critical infrastructure." Galligan was formerly the FBI Special Agent in Charge of Cyber and Special Operations for the FBI's New York office.

Deloitte's approach raises understanding and awareness of cyber threats among this wide range of responders, many of whom have typically had little exposure to IT security functions. Through simulated scenarios, they gain a greater sense of ownership of their role in cyber defense and help establish a broad culture of cyber resilience.

"Resilience," notes Emily Mossburg, principal in charge of resilient services for Deloitte, "doesn't start when an incident occurs. Preparedness for cyber attacks is a multi-layered challenge. It includes the design of infrastructure and applications, the building of necessary support relationships, and a broad, ongoing program to build a cyber-aware culture throughout the organization."

Deloitte's cyber threat war-gaming services leverage a wide range of pre-packaged exercises and an inventory of threat scenarios and action components that can be customized to each organization's risk profile, drawing on Deloitte's extensive experience across a wide range of industry sectors.

Deloitte is recognized by Forrester Research, Inc. as a leader in information security consulting services[1], named by Kennedy Consulting Research and Advisory as a global leader in cyber security consulting[2], and ranked No. 1 globally in security consulting, based on revenue, by Gartner.[3] [4]Please visit **www.deloitte.com/us/resilientservices** for more information.

[1]"The Forrester Wave™: Information Security Consulting Services, Q1 2013", Forrester Research, February 1, 2013

[2]"Cyber Security Consulting, 2013," Kennedy Consulting Research and Advisory, October 2013.

[3]Source: Gartner, Market Share Analysis: Security Consulting, Worldwide, 2013, Lawrence Pingree, 16 May, 2014.

[4]References by Forrester Research, Inc., Kennedy and Gartner are to the Cyber Risk Services practices of the member firms of Deloitte Touche Tohmatsu Limited, including those member firms outside the U.S., in the aggregate.

About Deloitte's Cyber Risk Services

Deloitte's Cyber Risk Services help complex organizations more confidently leverage advanced technologies to achieve their strategic growth, innovation and performance objectives through proactive management of the associated cyber risks. With deep experience across a broad range of industries, Deloitte's more than 1600 practitioners provide advisory and implementation services, spanning executive and technical functions, to help transform legacy IT security programs into proactive *Secure.Vigilant.Resilient.* cyber risk programs that better align security investments with risk priorities, establish improved threat awareness and visibility, and strengthen the ability of organizations to thrive in the face of cyber incidents.

About Deloitte's Risk Advisory practice

Deloitte's market-leading Risk Advisory Practice helps organizations build value by taking a strategic risk approach to managing financial, technology and business risks. This approach helps our clients focus on their areas of increased risk, bridge silos to effectively manage risk across organizational boundaries and seek not only risk mitigation, but also pursue intelligent risk taking as a means to value creation.