DXC Incident Response Tabletop Exercises

DXC Incident Response Tabletop Exercises aim to evaluate and bolster your team's ability to respond to cyberthreats.

As cyberthreats become more sophisticated and attacks more multifaceted, it is vital that an organization's cybersecurity posture include a tiered defense. It is no longer a matter of *if* an organization will become a victim of a cyberattack, but *when*. A quick and easy way to determine your organization's ability to respond to an attack or incident is through DXC Technology's Incident Response Tabletop Exercises. These discussion-based tabletop exercises (TTXs) simulate customized cyberattacks derived from real-world incidents. These exercises educate your teams on their incident response (IR) roles and responsibilities, validate plan efficacy and enable testing of system components.

As a leading cybersecurity services provider, DXC Technology sees ransomware attacks, other advanced persistent threats and related threat activities regularly. Through the experience of our Cyber Transformation and Operations team, which performs numerous cybersecurity remediations, DXC has crafted approaches to help organizations and their incident response teams prepare to address cyberattacks and related incidents.

The real-world scenarios in our TTX service provide hands-on learning for your teams, clarifying their IR roles before an incident happens. The exercises also evaluate how well your internal teams and external partners communicate and work together to provide a unified response to cyberthreats. These valuable insights help you improve your IR readiness and demonstrate your organization's competence in addressing incidents.

Engaging with DXC's TTX service signifies a proactive and responsible approach to incident management. It also lays the groundwork for exploring further security enhancements that can help you develop a more resilient and well-defended cybersecurity infrastructure for your organization.

Incident Response Tabletop Exercises in action

DXC Incident Response Tabletop Exercises have delivered results:

- **Successfully tested global IR process.** DXC customized a tabletop exercise for a car manufacturer to test the global IR process that we developed with the organization. We created a fictitious attack scenario triggering all steps of the new process. The exercise successfully confirmed that the new process was mature and effective.
- **Performed thorough simulation for stress testing.** We performed an offsite crisis simulation exercise for a large European bank to prepare the bank for the stress test required by the European Central Bank. We created a fictitious crisis based on a ransomware attack and related issues, including data theft, privilege escalation and Active Directory compromise. The CISO recognized

Key benefits

- Organizations simulate and train with modern, customized attack scenarios.
- IR teams improve communication and cooperation.
- Response team members receive training in their responsibilities, building their confidence in responding to an actual attack.
- Simulation provides documented actions taken, offering insights for improving crisis procedures.

the simulation as great preparation for the stress test and a successful collaboration with DXC.

- **Verified and improved IR maturity of 50+ delivery teams.** DXC conducted a tabletop exercise to educate and train delivery teams in effective crisis response. More than 250 improvement actions were verified and addressed as a result.

Key features

Key features of Incident Response Tabletop Exercises include:

- A simulated cyberattack scenario to work through as if it were real
- Participant response (detection and analysis, containment, eradication, recovery, post-event activity) using participant's knowledge, processes and tools
- Record of exercise responses and findings
- Maturity assessment based on exercise responses and findings
- Recommendation of corrective actions to address gaps and improve maturity

Why DXC?

DXC is a leading security services provider that helps thousands of organizations navigate severe security crises. Active engagement in these crises gives us insights into the requirements, challenges, questions and dependencies typical of such demanding situations. We use these insights in developing and executing tabletop exercises, making them realistic and relevant to your organization.

DXC has significant experience in all IR phases, which gives us a firm understanding of the potential impacts of different recommendations and approaches. We use this knowledge to tailor solutions to meet our customers' unique needs.

Learn more at
dxc.com/cyber-defense

Service options

Foundation (out of the box)

- 2 hours of exercise for approximately 10 participants
- Predefined scenario with limited customization
- Kickoff and wrap-up call
- Minimal resource needs
- Provides good insight into incident response readiness
- Identifies gaps and opportunities for improvement

Customized

- 4- to 5-hour exercise with approximately 20 participants in 2 to 3 breakout teams
- Scoping interviews and scenario tuning
- Kickoff and hot and cold debriefs
- Executive report with improvement recommendations
- Exercise customized for specific environment or specific security aspects

Extensive

- Multiday exercise covering multiple departments, aspects and/or locations
- Scope and approach mutually agreed upon
- Tailored for specific customer needs

Get the insights that matter.
dxc.com/optin

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission-critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services to drive new levels of performance, competitiveness, and customer experience across their IT estates. Learn more about how we deliver excellence for our customers and colleagues at **DXC.com**.