Improve your team's cyber risk readiness with digital tabletop simulations customized for your organization.
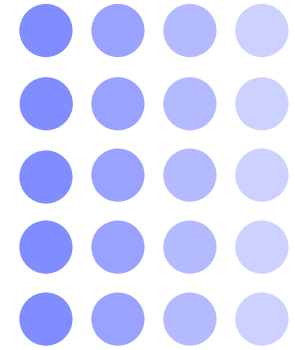
Engage your cross-functional teams in a live, interactive, and realistic cyberattack situation to improve rapid decision training and cyber risk readiness:

- Customize a virtual, hybrid, or in-person format to fit your organization's infrastructure and needs.

- Empower front-line individuals to handle high-consequence cyber incidents with the highest degree of preparedness, data, and speed.

- Identify gaps in your current incident response plan and consult with breach response experts to implement improvements.

Features

Engage cross-functional teams including executive leadership, IT, Legal, Finance, Forensics, HR, key vendor partners and Communications.

'Training By Gaming' approach lets players see, hear, touch, and feel emotion as they navigate various cyber incident situations.

'Heads Up Display' provides a dynamic view of the essential parameters that help players assess ramifications prior to making decisions.

Management levels can assess usage and performance at a macro level.

Why Epiq Legal Solutions?

Experience the advantage of solutions from a partner specializing in legal and compliance.

Drive decisions with AI-enabled solutions that combine people, process, technology, and data.

Epiq Differentiators

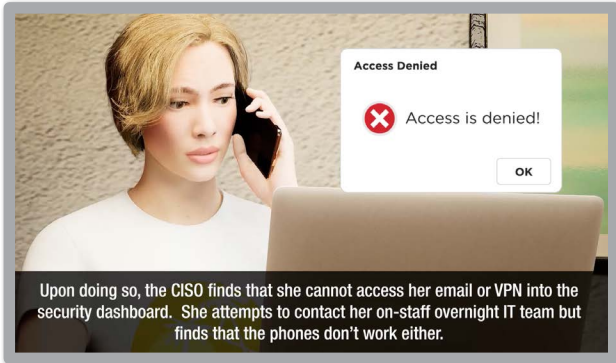— Gamify your tabletop simulation exercise through an interactive and engaging digital platform.

— Partner with the only full-service breach response provider offering breach preparation consulting and a digital tabletop simulation platform.

— Apply learnings on the go with access to Epiq breach response experts throughout your training.

Interactive and Engaging Digital Platform
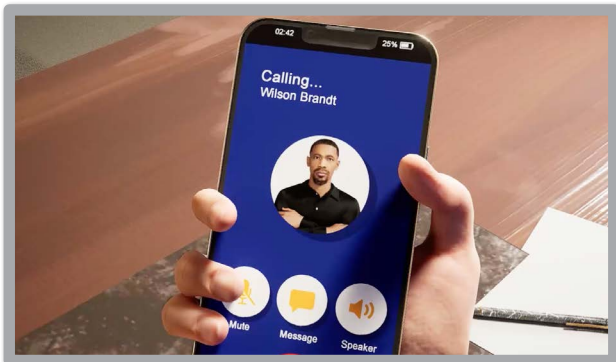

epiqglobal.com

©Epiq 2024 Sep 03

Improve your team's cyber risk readiness with digital tabletop simulations customized for your organization.

Gamify your tabletop simulation exercise through an interactive platform.

Upon doing so, the CISO finds that she cannot access her email or VPN into the security dashboard. She attempts to contact her on-staff overnight IT team but finds that the phones don't work either.

"Training by gaming" approach with interactive scenarios.

Set up team avatars, voice overs, branded content, and more.

Calling...
Wilson Brandt

Dynamic views of scenarios and performance for rapid decision making.

Customize a storyline to fit the needs of your organization.

Single selection Question
How should you respond to this breach?

A — Notify all necessary team members, including IT, security, legal, communications, and relevant business units, to activate the incident response team.

B — Contact IT personnel only. Involving representatives from other departments or external specialists is unnecessary and could slow down the response process.

C — Wait until the end of the business day to declare the breach as a security incident. It is important to take time to gather more information before making any declarations.

D — Avoid communicating with employees, customers, partners, or the public about the breach. It is better to keep the breach confidential to prevent any potential reputation damage.

SUBMIT

Develop customized training questions and cyber attack scenarios for team response readiness.

Click for Video Demo