Cyber incident simulation

Your phone rings – sensitive information on your employees and your customers has been leaked – what do you do?

A cyber security breach can strike at any time, putting your entire organization at risk.

Are you ready to manage a cyber incident?

We have observed through many recent high-profile examples, the answer to this question is unfortunately not well known by organizations and the necessary reaction and response remain poorly understood.

While organizations can attempt to manage a crisis as it evolves, the likelihood of success of this approach is very low. This is often compounded by the use of untested incident response plans or poorly defined organizational responsibilities.

The challenge is that cyber threats are increasingly complex and their effects are readily amplified through social media and a 24-hour news cycle.

The frequency and severity of today's cyber incidents make them unlike any crisis your organization has likely dealt with before.

Are you ready?

What is cyber incident simulation?

KPMG's cyber incident simulation service helps your organization examine and understand its current incident response capabilities to better prepare for and manage cyber incidents.

With proven experience in incident response, crisis communications, operations and incident response planning, KPMG's cyber team will test and assess your people, plans and processes by creating custom scenarios for your organization that replicate the challenges of real cyber incidents.

This type of testing is an effective tool for your organization to assess its current and desired state of incident preparedness and forms an important part of establishing your cyber defensible position.

Our approach

To assess, test and improve your organization's ability to respond to a cyber incident, KPMG uses a three step approach which can be customized to meet the needs of your organization based on your current level of preparedness.

We will begin by working with you to obtain the necessary information on business processes and areas of concern that are essential for developing the exercises and simulation scenario.

We then employ a combination of the following methods:

- **Tabletop exercises** for the executive and/or operational team. KPMG's cyber team will guide your organization through a discussion around roles and responses to a specific incident or situation. Through this exercise we will evaluate if key personnel can effectively talk through their roles, responsibilities and planned response measures.

- **Paper testing** of your organization's incident response plan. The first time you test your plan shouldn't be during a live crisis. During a paper test, KPMG's cyber team will work with you to review all elements of your current incident response plan and provide actionable recommendations to strengthen it.

- **Interactive cyber incident simulation.** A customized scenario will be developed for your organization's executives and staff members to truly test readiness for a real world incident. As your organization manages the incident, new challenges and unexpected information will be introduced to replicate the evolution of a real world incident. The duration of the simulation will last between one and a half and three hours. The simulation is immediately followed by a 'hot' debrief and a detailed action report will be provided with recommendations for improvement and next steps.

Types of simulated incidents

The type of simulated incidents will be customized to your organization and can include:

- Data loss (crown jewels, customer info, trade secrets)
- Distributed denial of service attack (DDoS, DNS)
- Randomware (malware, viruses, trojans)
- Executive impersonation
- Rogue employee
- Telecommunications network failure
- Attacks against industrial control systems or other business specific issues.

The KPMG difference

KPMG helps you understand, prioritize and manage your cyber security risks, so you can take control of uncertainty, increase agility and turn risk into advantage.

- Cyber security threats: A new business reality
- Have confidence that you're investing appropriately.
- From strategy to implementation.
- Cyber security is about what you can do, not what you can't.
- Creating cyber resilience and self-sufficiency.

Why choose KPMG's cyber team?

KPMG brings a business context to cyber security for all levels of your organization – from the boardroom to the back office.

Using the same tools and techniques that professional hackers use for ethical hacking and offensive security, we have tested the layers of security for a large number of clients and organizations across multiple industries.

To complete our team, we include not only advisors to local, regional and federal law enforcement agencies across North America, but cyber thought leaders and authors of multiple security and forensics books that are helping to shape the industry.

KPMG Cyber Security professionals believe cyber security should be about what you can do – not what you can't

An objective, knowledgeable advisor.

As a global network of regulated member firms, we have an unwavering commitment to precision, quality and objectivity in everything we do. So you can rest assured that KPMG cyber security assessments and recommendations are based on what's best for your business – not on market hype.

Knowledge of emerging issues.

In our I-4 Forum, also known as the International Integrity Institute, we convene leading cyber security professionals from around the world to discuss emerging threats, regulatory challenges and solutions. So we can help you consider possible issues around the corner in financial services, oil and gas, pharmaceuticals, engineering and other industries.

Rated no. 1 In executive management.

In fact, in a 2016 Forrester WaveTM study on information security consulting services, companies rated KPMG No. 1 for counseling senior leadership on cyber security. KPMG member firms surpass other professional services firms and technical firms to help board members understand cyber security, make informed decisions that align to the business strategy, and feel assured in their due diligence.

Transforming security across different geographies and cultures.

KPMG member firms have deep local knowledge in nearly every market where you do business, so we understand cyber security risks, regulatory impacts, change management, forensic investigations and other factors that may change from one country to the next. We have a global network of more than 3,000 cyber security professionals, plus multi- disciplinary collaboration with 189,000 other professionals in KPMG member firms across more than 152 countries. With that global presence, we can help you drive security transformation across your operations, wherever they may be.

Contact us

Yassir Bellout
Partner, Cyber Security
T: 416-777-3416
T: 514-840-2546
E: ybellout@kpmg.ca

Jeff Thomas
Partner, Cyber Security
T: 403-691-8012
E: jwthomas@kpmg.ca

KPMG's Cyber Team works with organizations to help prevent, detect and respond to cyber threats.

We can help your organization be cyber resilient in the face of challenging conditions.

Have a cyber emergency? Contact our 24/7 Cyber response hotline

1-844-KPMG-911
1 (844) 576-4911