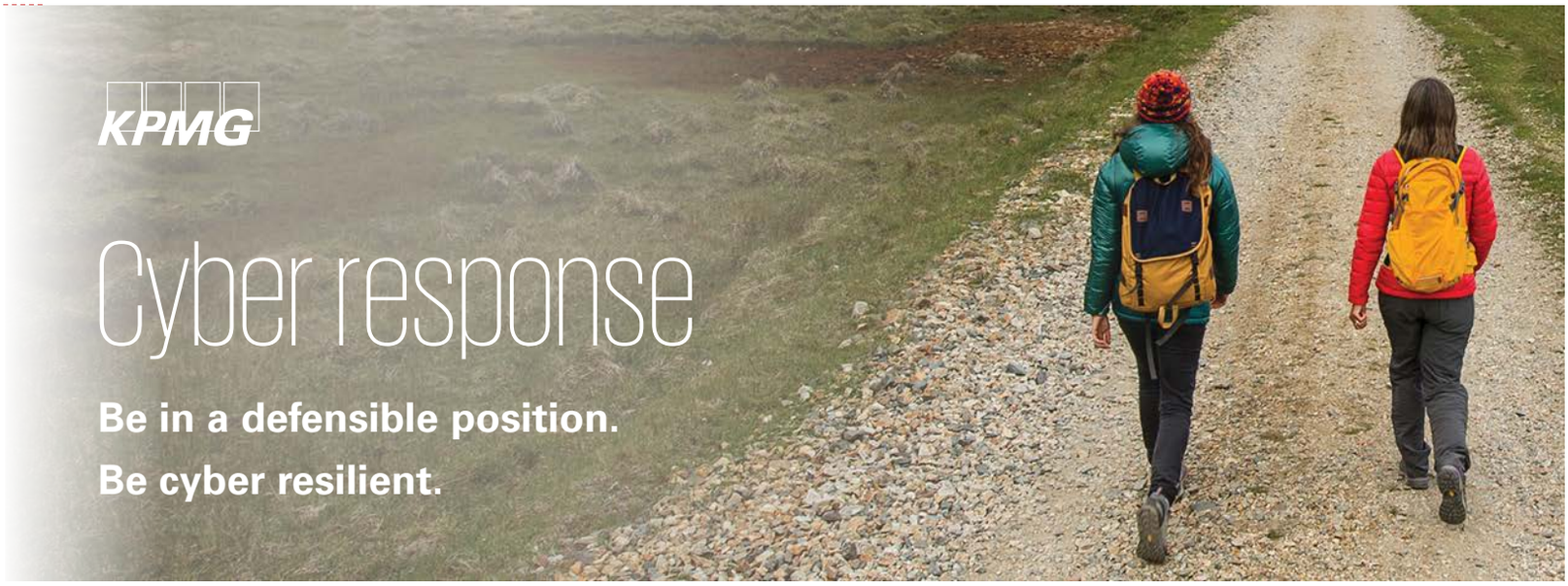

Cyber response

Be in a defensible position.

Be cyber resilient.

Cyber incidents affect more than just technology and require a holistic response encompassing people and processes to limit impact. When the inevitable happens, are you confident that you can effectively respond?

Species such as the sea urchin have adapted to ward off threats in the most challenging environments. Organizations must do the same to protect, detect and respond to ever-changing threats.

Is your organization prepared to respond to the sophisticated cyber attacks and adversaries of today?

Cyber incidents are a top concern for organizations of all sizes and across all industries. The impact can be devastating to organizations who suffer a cyber incident and struggle to effectively respond and recover:

- Loss of brand reputation and customer loyalty
- Financial fines and litigation expenses
- Loss of employee productivity
- Disruption of business services
- Loss of market competitiveness

When looking at cyber security, the stakes are high and impact is often directly associated with how well an organization can respond and recover. Response differs depending on the nature of the incident, organizational controls and adversary motivation. KPMG's Cyber Team addresses this by developing a detailed understanding of each client prior to an incident to support an effective response.

Gaining an understanding of your organization to turn risk into advantage with Cyber Incident Response

Gaining the advantage to effectively manage cyber incidents entails thorough preparation well before an event is detected. Cyber response extends beyond technical controls. Through a client on-boarding process, we gain a better understanding of your organization, culture and response processes thereby ensuring the seamless integration and execution of response activities during the management of an incident.

The professionals of KPMG's member firms have the industry leading knowledge needed to detect and monitor relevant threats inside and outside of your organization

KPMG's Cyber Team consists of industry specialists who have managed the response and recovery of some of the industry's largest and most high-profile breaches. Our team includes authors of definitive cyber security and forensics books and instructors to law enforcement across North America.

We leverage an arsenal of some of the industry's most advanced cyber response tools to help enable the rapid identification and monitoring of malicious or suspicious activity and provide the control needed to contain an incident. Dark web intelligence assists us in identifying likely adversaries, data that may have been exfiltrated from your environment and future attack plans targeting your organization.

Whether an incident involves malicious insiders, sophisticated external adversaries, malware or unintentional data exposure, we will work with your organization to help minimize the impact and effectively recover from a security incident.

Assisting you from response to resiliency

As an added benefit, incident response engagements can feed seamlessly into forensic investigations, and then cyber security enhancement to help your organization prevent the reoccurrence of a future incident as shown below:

Source: KPMG in Canada

Assisting you from response to resiliency (cont'd)

Incidents can include systems that are compromised, processes that are circumvented or people who fall victim to social engineering. Response can include technological measures, personnel interviews and process workflow analysis. Each phase in response requires communication with technical teams, business stakeholders and executives. KPMG's Cyber Team is fully experienced in leading the technological response as well as in the identification and containment of exposures within systems, processes and personnel.

Effective response to support your investigation objectives

KPMG's Cyber Team is specially trained as first responders whether the objective of an incident is to contain an exposure, recover or restore business operations or identify and take legal or other action against those involved. We will help ensure that response includes the identification and preservation of information using court-approved methods to ensure if post-incident containment, legal or other action is planned, evidence can be submitted into future proceedings.

Our incident response methodology leverages an industry recognized six-stage methodology, developed in line with NIST and SANS best practices:

Response stages

1. Prepare and detect
2. Verify
3. Assess
4. Contain
5. Eradicate
6. Review

Why choose KPMG's cyber team?

KPMG's experienced cyber team employs over 2700 cyber security, incident response and forensic technology professionals in various member firms worldwide. We are highly experienced in multi-industry and multi-jurisdictional incident response, helping to ensure an appropriate and targeted strategy tailored to the capabilities of attackers and the risk to a business. We also provide:

- 24 hour a day, 7 day a week toll-free on-call support, directly connecting you with top industry professionals
- A zero-loss retainer that allows you to apply unused retainer amounts toward proactive cyber security services
- On-boarding processes that help to identify your organization's gaps or exposures in existing response processes.

Cyber emergency?

Please contact our 24/7 Cyber response hotline

1-844-KPMG-911

1 (844) 576-4911

We believe cyber security should be about what you can do – not what you can't.

Award winning

KPMG International has been named a Leader in the Forrester Research Inc. report, The Forrester Wave™: Information Security Consulting Services, Q1 2016 achieving the highest score for current offering and strategy.

The KPMG cyber team won the SC Europe Information Security Consultancy award in 2011 and 2012. The team also won the MCA award in 2011 and 2012.

Independent

Our recommendations and technical strategies are based solely on what is fit and appropriate for your business.

KPMG in Canada is not tied to any technology or software vendor.

Collaborative

We facilitate and work with collaborative forums to bring together many of the best minds in the industry to collectively solve shared challenges and emerging threats.

KPMG's I-4 forum brings together over 50 of the world's leading organizations to talk about how to effectively deal with Cyber challenges.

Trusted

KPMG member firms have a long list of certifications and permits to work on engagements for many of the world's leading organizations.

Global, local

KPMG is a global network of member firms with over 189,000 professionals in 152 countries and 2,700 security practitioners globally. KPMG's regional practices can service your local needs from information security strategy and change programs, to low level technical assessments, forensic investigations, incident response, training and ISO27001certification.

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.

Contact us

Francis Beaudoin
National Leader,
Technology Risk Consulting
T: 514-840-2247
E: fbeaudoin@kpmg.ca

Jean-Francois Allard
Partner
T: 514 840 2645
E: jeanfrancoisallard@kpmg.ca

Yassir Bellout
Partner
T: 514-840-2546
E: ybellout@kpmg.ca

Erik Berg
Partner
T: 604-691-3245
E: erikberg@kpmg.ca

John Heaton
Partner
T: 416-476-2758
E: johnheaton@kpmg.ca

Adil Palsetia
Partner
T: 416-777-8958
E: apalsetia@kpmg.ca

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

kpmg.ca/cyber