The inevitability of cyber attacks, whether small, isolated events or large-scale network compromises, presents a strong business case for investing in effective defence and response testing capabilities.

The problem
Recent cyber break-ins at high profile entities have highlighted the reputational and business impacts of failing to properly safeguard information assets. Additionally, regulatory requirements mean that companies can expect restrictions on their business operations or, more severely, monetary fines should they fail to properly protect their customer data.

The KPMG approach
Over the years, the demand for penetration testing has increased substantially as businesses have recognized the need to provide assurance that they are protected from internal or external threats.

We base our approach on the preposition that an information asset’s value, threats, and vulnerabilities represent the level of risk associated with that asset. As the significance of any of these factors increases, the relevant risk also increases. Conversely, reducing any of these factors reduces the risk. All these factors must be understood before it is possible to assess risk in a reliable manner. Our penetration studies assess and quantify threats and vulnerabilities associated with specific target environments.

The KPMG in Canada penetration testing services strive to provide you with an independent and objective security assessment of your IT systems, clearly highlighting the security risk to corporate and customer data from both external and internal threats.

How can we help?
KPMG in Canada can provide the following services to help you understand the risks you face with regard to technical vulnerabilities, as well as support the creation and delivery of appropriate strategies to mitigate those risks:

- An independent and objective insight into the business risks of technical security vulnerabilities (and associated people/process aspects) by showing whether and how an attacker can compromise networks and systems or socially engineer valuable information.
- A clear statement of the security risks and priorities to allow you to focus on fixing the most important issues.
- Tracking your common IT security technical shortfalls and failings, such that common issues in your development and deployment processes can be identified and remedied to facilitate improved security on future-deployed systems.

KPMG’s security testing model

© 2018 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.
A wealth of testing scenarios
Our penetration testing service scenarios include:

- White, grey and black box testing: Through defined methodologies which cover the attack paths taken by real-world hackers, we can perform infrastructure and web application penetration testing across all technology types.

- Open source data reconnaissance: How much information is leaked about your organization which can be used by attackers in further attacks against your systems?

- Social engineering: We can simulate scenarios such as e-mailing Trojans to specific e-mail accounts to investigate whether perimeter defences can be breached via such mechanisms and persistent back-door access planted in your organization.

- Physical security: Many organizations rely on the physical security of their building to a greater extent than their firewalls, yet do not test the physical security controls in place.

- Resilience testing: If you have a requirement to operate 24x7, you may have invested in resilient hardware and software, yet may not have tested how well the configuration works.

- Performance testing: In conjunction with our testing group we can provide a performance profile for your hardware to establish if it meets your requirements. We can also perform application stress testing to ensure it can handle the anticipated load.

Potential benefits to you

- Only by emulating real-life threat agents, such as disgruntled employees, external hackers and cyber attackers, can the true technical risks inherent in IT systems be identified to then facilitate identification of the necessary mitigating controls to be implemented.

- Teams of KPMG professionals have performed a variety of scenario based tests against global financial institutions, retail giants and international media companies. These have included posing as cleaning staff in order to gain access to company buildings, setting up fake wireless access points to capture employee credentials and simulating a rogue employee in order to test incident response teams.

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 Wave™ 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.

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

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

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

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

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

Have a cyber emergency? Contact our 24/7 Cyber response hotline.
1-844-KPMG-911
1 (844) 576-4911

© 2018 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. 17915

The KPMG name and logo are registered trademarks or trademarks of KPMG International.