Is cyber security top of mind at your business?

Assessing your organization's Cyber security capability and overall maturity

The current state of Cyber

Recent headlines continue to confirm Cyber attacks are clearly growing in scale, and Cyber incidents continue to be on the rise. Cyber security is rapidly emerging as a key risk area for enterprises around the globe with increasing frequency. This is due to many high-profile and highly disruptive security breaches that constantly threaten to cause financial and physical damage across critical national and corporate infrastructures.

Cyber security is a key area of concern in the boardrooms. There is a significant responsibility on the part of boards, audit committees, and executives to ensure to customers, stakeholders and regulators that appropriate safeguards are in place, commensurate with the risk, nature and complexity of the business.

Of most concern, organizations are increasingly vulnerable as a result of technological advances and changing working practices such as remote access, big data, cloud computing, social media and mobile technology.

How can KPMG help?

To help deal with the increased Cyber risk, KPMG have developed a highly customized, tailored Cyber maturity assessment tool. KPMG's Cyber maturity assessment (CMA) helps you take a positive approach to monitoring and managing Cyber risks, and helps enable you to turn this into a strategic advantage.

It can be used to analyze the Cyber maturity of your organization, using six key dimensions. By assessing the risks and identifying the gaps, it allows your organization to decide on your Cyber risk appetite.

How is the KPMG CMA unique?

KPMG's CMA provides an in-depth maturity assessment of an organization's capability to protect its information assets and its preparedness to respond effectively to Cyber threats. Some of the distinctive features are:

- Methodology based on leading information security frameworks such as NIST CSF, ISO 27002 and NIST 800-53
- Indicative mapping to all of the frameworks identified above to facilitate a "Perform Once, Report Multiple Times" concept
- A risk based approach to align with a sustainable risk management program

Leadership and governance: Identifies the board's and leadership's understanding of Cyber and its Cyber risk appetite, and demonstrating due diligence, ownership and effective management of risk.

Human factors: Ensure the organization's personnel are properly trained and understand the nature of Cyber security and their role in protecting the organization's assets.

Information risk management: The overall management of risk and visibility to stakeholders

Operations & technology: Technical and operational control measures implemented to address identified risks and help minimize the impact of compromise.

Business continuity: Ensuring that the role of security and its impact on business continuity is fully understood and integrated into the overall business continuity, crisis communications and mass notification processes.

Legal, compliance & audit: Ensure the organization is aware of its legal and compliance obligations and complies with them in an effective manner.

KPMG's CMA can help your business

- Assess whether the mechanisms to manage your risks are mature
- Understand whether you comply with the various regulatory requirements
- Take greater control, ensuring that your organization is prepared for the evolving Cyber security landscape
- Evaluate how your Cyber security posture compares to your competition and industry peers
- Develop or revamp your Cyber security strategy
- Build a sustainable Cyber risk management program aligned with your enterprise risk management strategy

Our approach

KPMG member firms use a three phased approach that follows a logical sequencing to help ensure that we validate findings as part of the process and seek feedback on an iterative basis. In addition to alignment, this also helps to ensure stakeholder participation through the process.

Phases		
Phase I – Information Gathering	**Phase II – Analysis**	**Phase III – Strategy & Roadmap**
Engage the business leaders, understand current, Cyber risk appetite and understand what sort of security capability is desired. Deliverables include:	Assess the current capability that exists in the business, and apply that to the inherent risk register to understand current Cyber exposure. Deliverables include:	Propose potential options to manage risk to within tolerance, and offer suggestions on a roadmap from current to desired states. Deliverables include:
– Mapping of threats and risks to Crown Jewels and enabling assets – Validation of current state technical controls	– Threat Landscape – Peer-compared current state – Inherent and net risk exposure – Risk Register with risks classified and prioritized	– Future State targeted model with roadmap and action plan – Executable project charters for improvement areas – Board Presentation

Source: KPMG in Canada

Why choose KPMG's Cyber team?

Some key differentiators for KPMG to deliver this service are:

- Industry leadership – cited as Leader in Forrester Research Inc. report, "The Forrester Wave™: Information Security Consulting Services" Q1 2016
- A distinct approach that is based on multiple frameworks and allows for cross-reference and comparison
- A specialized team with extensive Cyber security knowledge and experience
- Broad experience in emerging areas including operational technology, industrial control security, big data security, cloud technologies, etc.
- Experience in articulation of Cyber issues to board and audit committees

> "KPMG has a clear view of the relevant security issues for business executives and technicians. KPMG in Canada has been applauded for being 'doers' and easy to work with. KPMG also helps identify strategic advice, have subject matter experience, are flexible, adaptable, and deliver on commitments."

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings and comments. Forrester does not endorse any vendor, product or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Cyber Emergency?

Please contact our 24/7 Cyber response hotline

1-844-KPMG-911

1 (844) 576-4911

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