KPMG

Governance: Are we ready for cybercrime?

Internet Governance Forum

—

23 June 2017

ISSA
Information Systems Security Association
Barbados Chapter

KPMG

2017 Cyber Security and CIO Surveys' Snapshots

Internet Governance Forum

EMEA Cyber Security Benchmark Survey 2017

During our assessment of the annual reports, different elements of cyber security reporting were reviewed:

1. The depth and extent of addressing cyber security;
2. Cyber security topics that were mentioned;
3. Whether the board explicitly accepts ultimate responsibility for cyber security risks.

Key Result Areas	Researched companies that still don't mention Cyber Security risks in their annual report	Researched companies which spend at least a paragraph on Cyber Security in their annual report	Researched companies that consider Cyber Security risks a boardroom responsibility	Research Population
EMEA	56%	26%	18%	800 companies
Barbados	89%	11%	0%	Sample of listed companies
Caribbean	84%	5%	11%	Sample of listed companies

** Note that we have not reviewed whether a company has actually devoted attention to threats, risks, countermeasures and risk appetite.

KPMG

Harvey Nash/KPMG CIO Survey 2017

Question	Answer	Global	Caribbean
Do you believe your Board is doing enough about the risks posed by cyber attack?	Yes	55.7%	42.2%
	No	44.3%	57.8%
Has your organization been subjected to any major IT security or cyber attacks in the last 2 years	Yes	32.5%	27.3%
	No	67.5%	72.7%

Internet Governance Forum

Harvey Nash/KPMG CIO Survey 2017

Which type of threat give you most cause for concern in terms of cyber attack?	Area	Foreign Power	Competitors	Organized Cyber Crime	Amateur Cyber Criminals	Insiders	Spammers	Other
	Global	27.8%	19.1%	70.7%	51.8%	47.3%	38.9%	1.5%
	Caribbean	22.7%	18.2%	65.2%	59.1%	65.2%	54.5%	1.6%

KPMG

Board/Business Leaders Oversight

Internet Governance Forum

Board engagement and oversight framework
Information risk management

Information risk management

The approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners

How should Boards engage?

- Understand risk management approach and linkage to enterprise risk
- Be able to understand and contextualize risk
- Review and approve risk tolerance
- Understand third-party supplier program
- Review and question program metrics

Communication **Direction**

What should management do?

- Develop risk management approach and policies
- Identify risk tolerance and communicate
- Link risks to sensitive data assets
- Perform risk assessment and measures
- Perform third-party supplier accreditation
- Report relevant metrics

KPMG

KPMG

Thank you

Mariette Simmons-Browne
Manager, Risk and Management Consulting

Tel: +1 (246) 434-3942
mariettesimmons@kpmg.bb

Mariette Simmons-Browne
Manager, Risk and Management Consulting

Tel: +1 (246) 434-3942
mariettesimmons@kpmg.bb