KPMG

Cyber security: the changing role of Internal Auditors

Survey of Internal Audit professionals in Bahrain

December 2017

kpmg.com/bh

A new unknown

In recent history in Bahrain and around the world, we have seen drastic changes in the ways we live and work as a result of unprecedented developments in technology. Whilst this change has brought unimaginable benefits, it also brings unknown threats. It is not surprising to hear then, that in a recent survey of Internal Audit professionals in Bahrain, KPMG discovered that the impact of this change, and in particular the threat to the security of businesses' digital operations and assets, is the most important priority for them in the coming year.

What is your main Internal Audit priority for 2018?

1. **Cyber security**
2. **Taxation**
3. **Digital risk**
4. **Data analytics**
5. **Accounting standards**

In today's digital world, businesses can't afford to be held back by cyber risks. They need to make bold decisions and feel confident that their cyber strategy, defenses and recovery capabilities will protect their business and support their growth ambitions. Although it is everyone's responsibility to adopt good practices to protect against cyber attacks, Internal Auditors play a key role and are increasingly expanding their focus to include not only core operational and external risks, but also emerging risks, such as robotics, cyber and internet of things.

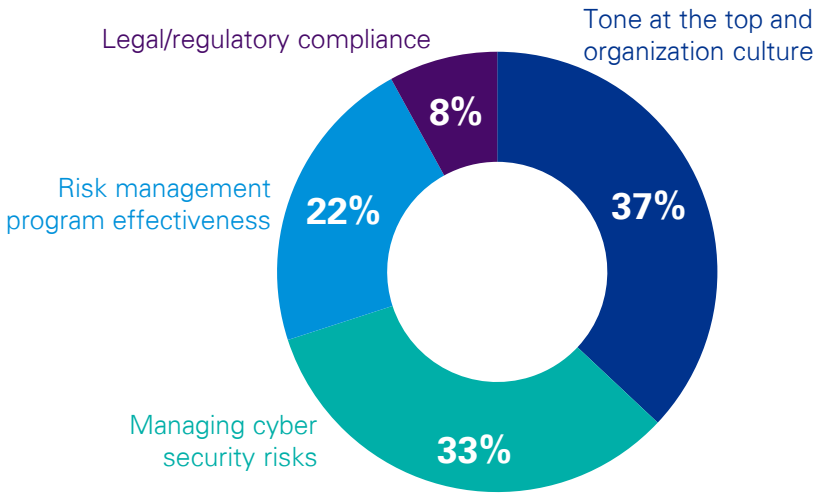
And the focus should not only be inward looking. Stakeholders and regulators are expecting organizations to protect digital assets and maintain efficient systems that are resilient to deliberate attacks. Loss of intellectual property, such as clients' information and commercially sensitive data, can lead to significant penalties and reputational damage. Therefore, it is important that organizations invest in developing and implementing overarching strategies to detect, respond to, and recover from cyber-attacks and related activities.

In this publication, we analyze the results of a short survey of 55 Bahrain-based Internal Auditors, conducted at a KPMG event on cyber security, held in November 2017. The survey aimed to assess the profession's current perspective on cyber security and how ready businesses are to respond to this.

"Cyber security is a serious threat facing organizations and businesses, and it is no longer the sole responsibility of IT security. Boards, management teams and all departments and functions that use digital assets in their business processes, have a role to play in ensuring the business is prepared for and protected against cyber threats."

Jeyapriya Partiban
Head of Risk Consulting
KPMG in Bahrain

From an Internal Audit perspective, what poses the greatest challenge to your company?



KPMG's view

Building maturity and understanding

To provide board members with a clear indication of how cyber threat could impact their business, Internal Audit teams can undertake an impact analysis to identify areas of particular focus, specific threat factors and likely information and systems that could be targeted. This can be used to pinpoint business units and activities that could be affected by specific threats and, identify what the real impact could be.

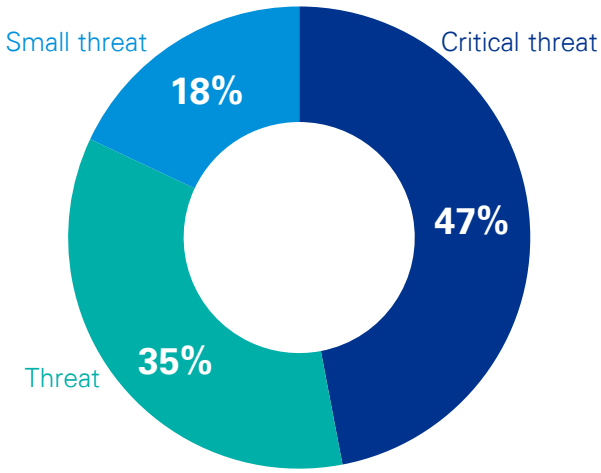
There is a clear concern amongst Internal Auditors that boards are not doing enough to ensure that sound risk management practices are adopted throughout the business. Cyber security is high on the agenda for Internal Auditors, yet without the support from leadership to tackle this challenge, it will be difficult to realize whole-business change in this area.

KPMG's view

From denial to opportunity

Internal Audit teams can help assess the state of readiness to manage a crisis i.e., reviewing the organization's ability to respond to cyber security incidents. Assessing readiness against cyber-attacks provides the opportunity to improve the business's incident response program. This may include subsequent monitoring of known issues for a limited period after the initial incident response.

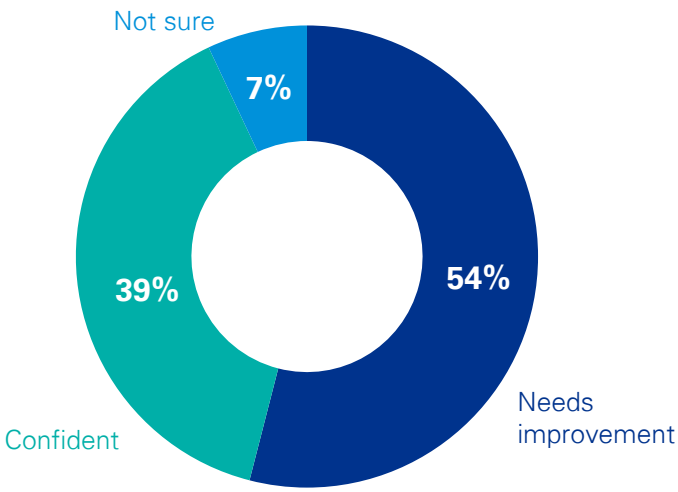
How much of a threat do you think cyber crime is to your business?



While no two companies are the same, with over 80 percent of respondents agreeing that cyber crime is a threat or a critical threat to their business, it is clear that action should be taken to address this.

There is no "one-size-fits-all" cyber security action plan and business-led protection strategies need to be embedded in governance models, operational processes, and culture. But when there is a breach, organizations also need to respond quickly, decisively and effectively.

How confident are you in your company's existing cyber controls?



KPMG's view

Protecting your assets

Building comprehensive security capability within the business can be costly and is not always fail-safe, given the continuous technological advancements, which expose businesses to ongoing and new cyber-attacks. Identifying critical assets at risk and managing these based on the business's risk appetite, will determine the level of controls needed by the business to mitigate cyber threats. Internal Audit teams can play a key role in assessing the efficiency and effectiveness of these controls.

Cyber security is a strategic enterprise risk that goes far beyond information technology. Uncontrolled, it can affect product integrity, the customer experience, investor confidence, operations, regulatory compliance, brand reputation and more. Despite this, over half of the respondents in Bahrain acknowledge that their cyber controls need improvement.

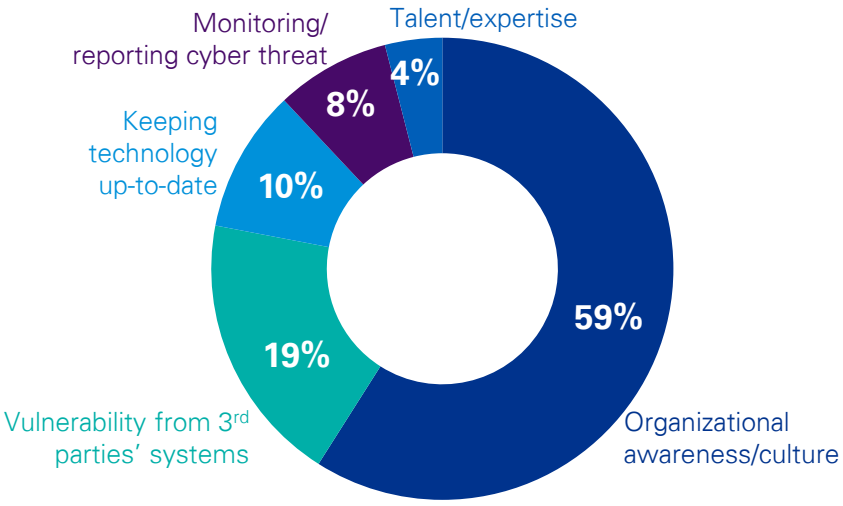
With the stakes so high, organizations must decide on their cyber security risk appetite and how they will respond to cyber security threats. There is a significant responsibility on executives to reassure customers, stakeholders and employees that appropriate safeguards are in place.

KPMG's view

Partnering

Through the risk assessment process, Internal Audit teams can continuously explore the risks faced by the business, brought about by changes in the way business is conducted e.g. new operating jurisdictions, new systems, new products, e-commerce, payment gateways etc. Working with the business's technology function, ongoing discussions and disseminating knowledge about emerging patterns in cyber incidents, helps keep both the business and the board updated on threats and opportunities.

What is the most significant gap in your company's ability to manage cyber risk?

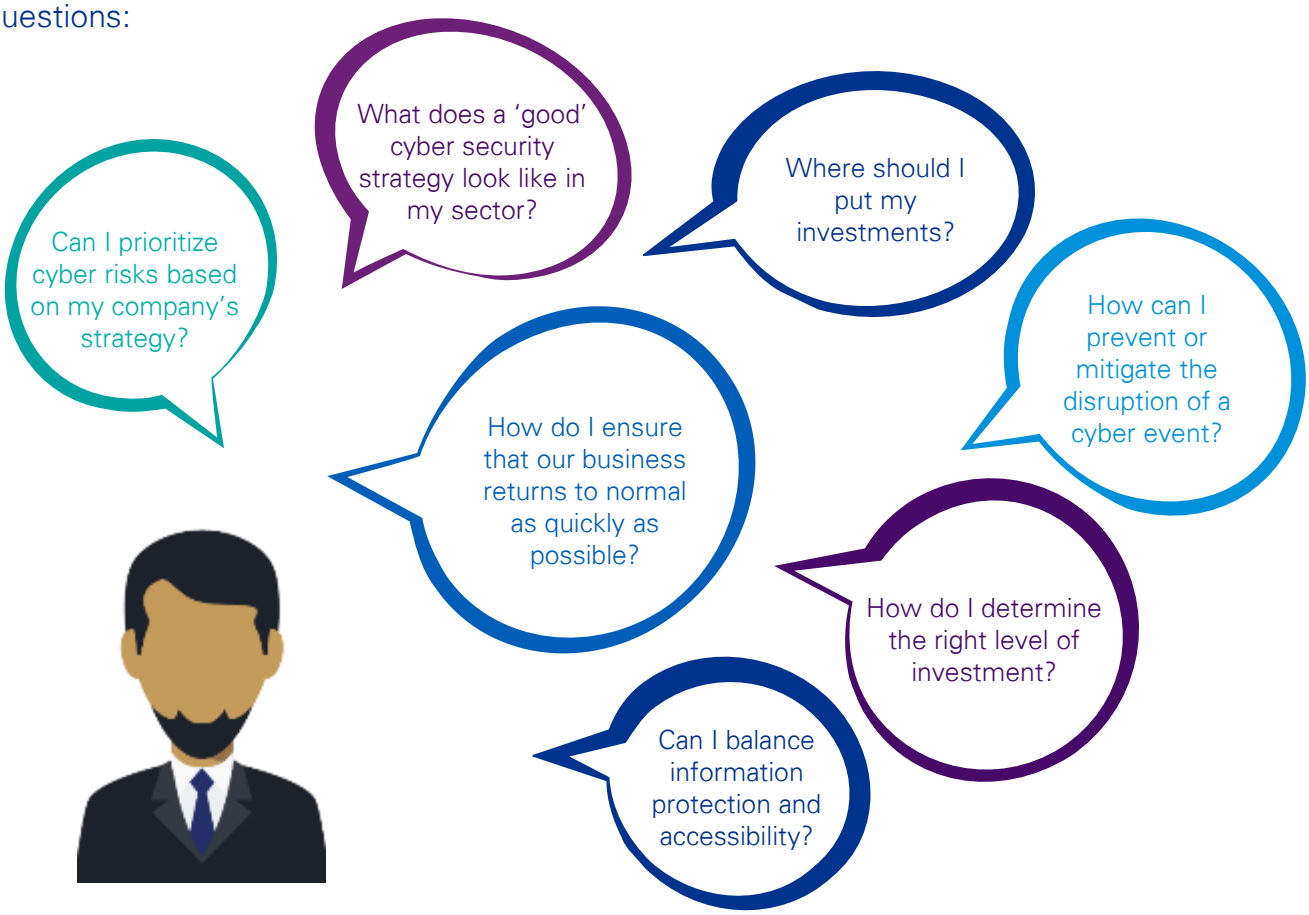


Understanding where the gaps are in an organization's cyber security protection is the first step to improvement. Carrying out a Cyber Maturity Assessment (CMA) will provide an in-depth review of an organization's ability to protect its information assets and its preparedness against cyber threats.

Taking a rounded view of people, process and technology helps organizations to understand areas of vulnerability, identify and prioritize areas for remediation and demonstrate both corporate and operational compliance, turning information risk to business advantage. However, this cannot be done in isolation and it is clear from the survey results that the whole organization must be drawn in to identifying, developing and ensuring that solutions are implemented consistently and continually.

How we can help

It is clear that cyber security is something that cannot be ignored. Across all sectors and in every geography, business executives and Internal Auditors are asking themselves the same questions:



At KPMG in Bahrain, our Internal Audit and Cyber Security professionals work closely with experts from around our global network to help clients tackle the challenges and grasp the opportunities that cyber threats present. We understand that businesses cannot be held back by cyber risk and recognize that cyber security is about risk management – not risk elimination.

Our cyber security services

Strategy and governance

— Information security strategy

— Target operating model development.

Cyber maturity assessment

— Compliance/framework gap assessment

— Information governance

— Business resilience

— Business continuity and disaster recovery planning.

Transformation

— Identity and access management

— Logging monitoring and analytics

— Asset protection

— Security program delivery.

Cyber defense

— Security testing and analytics

— Application security

— Security operations advisory.

Cyber response

— Readiness assessment and reporting.

Contact us

Jeyapriya Partiban
Head of Risk Consulting
KPMG in Bahrain
T: +973 17222322
E: jeyapriyapartiban@kpmg.com

Manav Prakash
Director
Information Technology Advisory
T: +973 17201443
E: mprakash@kpmg.com

Ramesh Gajula
Director
Risk Consulting
T: +973 17222377
E: rgajula@kpmg.com

Padmanabhan Nurani
Associate Director
Information Technology Advisory
T: +973 17224807 (extn: 439)
E: pnurani@kpmg.com