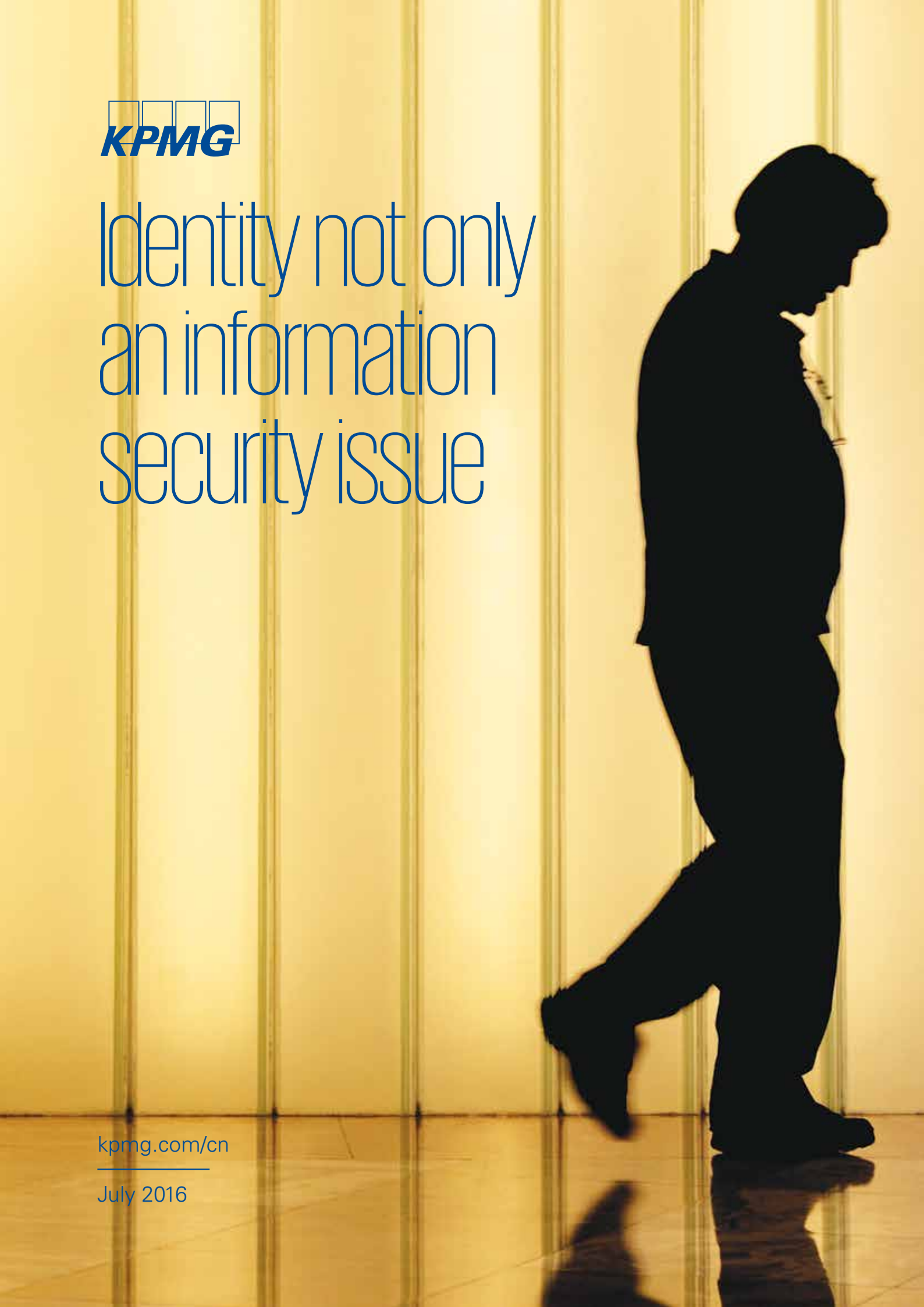


Identity not only an information security issue

kpmg.com/cn

July 2016

With enterprises rapidly transforming their businesses to take advantage of the new digital economy, digital identity has come to the fore. As topics such as cyber threat mitigation and customer engagement have moved up the enterprise food chain, digital identity has become a topic of importance at the executive level, increasingly gaining board level visibility.

A new European study, "Identity and Access Management in the Digital Age", sponsored by KPMG International, CyberArk and SailPoint, explores the issues faced in managing digital identities, and finds that 77 percent of information security executives had transformed at least some enterprise operations. Asked about the important goals of their organisation's digital transformation, 48 percent cited threat or breach mitigation, making it the most common objective.

Significantly, the study found that respondents were very aware of the transformation goals of other parts of the business. Increased revenue potential (important to 73 percent), enhanced customer experience and Customer Relationship Management (CRM) (70 percent), and creating a more agile business (68 percent) all ranked highly.

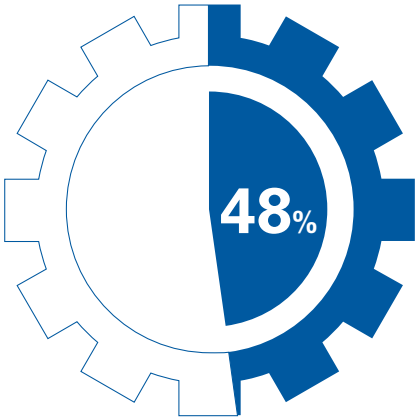
While the study only surveyed information security executives, the role of digital identity as a transformational capability goes well beyond traditional functions like user provisioning and authentication. It also underpins privacy protection, provides the basis for improving customer relationships and customer experience, facilitates an increasingly mobile and geographically dispersed workforce, and enables tighter collaboration between businesses.

However, the immediate challenge that information security executives face is that transformation introduces new cyber threat or breach vectors, with the potential to incur enormous damage and cost to business operations. This has major implications for the traditional enterprise digital identity function known as Identity and Access Management (IAM).

Almost two-thirds (65 percent) of respondents said Shadow IT, including cloud systems outside the control of the IT department, present a challenge to their IAM capabilities. Newly connected devices (cited by 50 percent) and the Internet of Things (IoT) (48 percent), were also cited as common challenges.

"These figures would not be very different in either North America or Asia Pacific."

— John Havers, KPMG Australia and Toby Emden, KPMG in the US



of the surveyed IT executives have emphasised that threat and breach mitigation is a pre-requisite for digital transformation.

This was reflected in respondents' IAM investment planning, with endpoint security included by 73 percent, the number one choice, and consumer identity applications by 65 percent. However, only a minority of respondents' IAM investments included social identities and logins (41 percent), Machine to Machine (M2M) or IoT applications (37 percent), or big data applications (28 percent).

It is here that the study reveals a divergence we often see between enterprise groups with different agendas. When it comes to investments in digital identity, it is likely in many cases that the information security executives surveyed were not speaking for their entire organisation. Although this is hardly a new trend, it does emphasise the continued importance of ensuring alignment between business leaders and information security executives.

This provides what is possibly the biggest take-away from this study. For China, these figures would not be very different because organisations in the country are also in the midst of a digital transformation. With the growing concern over cyber threats in the region, managing digital identity in transformation has become one of the key determining factors for the success of transformation.

While digital identity is attracting greater focus in the enterprise, different stakeholders need to come together if transformation is to succeed. Information security plays a key role, enabling a new set of opportunities to engage customers digitally, protect their privacy, reduce organisational risk and create trust.

Ultimately, the identity issue transcends technology, serving as a trust anchor for people, processes, data and governance. IAM is one of the most complex undertakings for any organisation, sharing many characteristics with an Enterprise Resource Planning (ERP) programme. It has a direct impact on how users interact with systems, perform their jobs and access sensitive data.

Accordingly, IAM can result in profound cultural change that requires sustained executive focus in order to be effective. "That makes it an organisational challenge that must be tackled holistically, not just by the IT department," says Havers. While this has always been the case, the emergence of disruptive trends such as cloud, Bring Your Own Device (BYOD) and an increasingly threatening landscape makes IAM more important than ever.

Sixty-five percent of senior information security decision makers surveyed see Shadow IT as a challenge to creating a secure IAM solution.

"For China, these figures would not be very different because organisations in the country are also in the midst of a digital transformation."

Contacts

Hong Kong

Henry Shek
Partner, IT Advisory
KPMG in China
T: +852 2143 8799
E: henry.shek@kpmg.com

Beijing

Calfen Cui
Director, IT Advisory
KPMG in China
T: +86 (10) 8508 5470
E: calfen.cui@kpmg.com

Shanghai

Richard Zhang
Director, IT Advisory
KPMG in China
T: +86 (21) 2212 3637
E: richard.zhang@kpmg.com

To read the full report
visit kpmg.com/digitalage

kpmg.com/socialmedia

kpmg.com/app

Available on the App Store

Publication name: Identity not only an information security issue
Publication number: 133547a-G
Publication date: July 2016