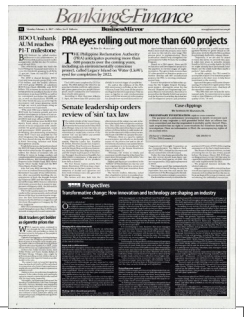
Headline	Transformative change: How innovation and technology are shaping an industry		
MediaTitle	Business Mirror		
Date	06 Feb 2017	Language	English
Section	Banking and Finance	Journalist	n/a
Page No	B4	Frequency	Daily



KPMG Perspectives

Transformative change: How innovation and technology are shaping an industry

Conclusion

What exactly is a blockchain?

OUR respondents showed little interest in blockchain as a digital-currency platform. It is much more likely that based on recent market developments, hedge fund managers may be utilizing blockchain-based technologies to provide faster and more secure transactions, streamlining and automating back-office operations and reducing costs.

As a distributed ledger database, blockchain is able to maintain a continuously growing list of transaction records that are considered immutable, and it is increasingly becoming the destination platform for financial services companies.

Managing risk in a data-driven world

AS hedge funds start to rely more heavily on technology across their front, middle and back office, many managers are becoming increasingly concerned about data risk. Cyber security is a top-level agenda item and will attract significant investment. But, at the same time, many managers also seem concerned about how their data is protected when it is outside of the control of the firm.

From risk to differentiator

HEDGE-FUND managers around the world are clearly worried about the safety of their most valuable data. Indeed, cyber security is ranked as an important technology capability by 83 percent of our respondents. Not surprisingly, larger companies are more focused on cyber security than most; 92 percent of large funds say they see cyber-security tools as an important technology over the next five years.

Cyber-security technologies are also expected to enjoy a flood of new investment from hedge-fund managers over the coming years, with 65 percent of our respondents saying they would put significant or very significant investment into cyber capabilities. Thirty-one percent of the largest funds in our survey went so far as to say that cyber security would be a key differentiator for their firm.

"Cyber is a massively important issue for our firm and we put a lot of effort into improving our control over our data," said the COO of one large firm. "We do security intrusion testing twice a year, we do technology training every quarter and we spend a lot of time educating our employees about threats, like phishing e-mails and targeted attacks."

Making cyber a boardroom priority

WHILE concern may run high, our data also suggests that cyber security may not be receiving the attention it deserves at the management or the Board level. Less than half of our respondents (46 percent) say cyber security is raised at every Board meeting, while 38 percent say it is raised only annually. Around one-in-six managers say that cyber security is only brought to the attention of their fund's board when there is a problem. Interestingly, large funds are twice as likely as small funds to say cyber is raised at every board meeting.

"I think a lot of fund managers rely heavily on the belief that their outsourced providers are taking care of their cyber security, but the reality is that you can't rely on a third party to protect your data," Robert Mirsky added. "You need to have a really strong oversight function because, at the end of the day, it is the fund manager that is left dealing with the fallout, not the service provider."

It is encouraging to note, however, that most managers expect to increase their investment into cyber security over the next five years. Almost two-thirds (64 percent) report that their cyber investment will increase in that time, while 36 percent say it will likely remain the same. No managers involved in our survey suggest that they will decrease cyber funding over the next five years.

Interestingly, it is the smaller funds that express the greatest intention to increase cyber-security investments. In fact, where 73 percent of small funds (those with assets under management (AUM) of less than $500 million) say cyber investments will increase, just 54 percent of large funds (those with AUMs of more than $5 billion) say the same. However, this may be indicative of the current low level of spend on cyber security by smaller funds rather than a reflection of any higher risk.

"Cyber security is a key concern for our members and for the industry at large," notes Jack Inglis, CEO of AIMA. "One of our key areas of focus has been on helping prepare our members for cyber-security challenges and regulation".

Extending your control

WHERE fund managers and executives demonstrate less confidence, however, is in the security of their data when it leaves the control of the firm. In our interviews, many hedge-fund managers voiced concerns about the cyber capabilities of their service providers, particularly smaller funds who may be using a "public cloud" service platform.

"A challenge with security preparedness on the public cloud often comes down to support. If an incident occurs on a public cloud, clients are often left sitting in a public queue waiting for the next available service technician rather than picking up the hotline to your dedicated helpdesk," Daniel Page noted. "Private clouds are purposely built for alternative investment firms and the associated applications, which allow these providers to provide customized services and rapid support to clients. Those fund managers relying on public cloud and off-the-shelf applications will have a hard time defending their approach to investors if their data gets hacked."

According to our survey, this lack of confidence extends from service providers to government bodies. In fact, just one in 10 of our respondents voice a high level of confidence in the ability of governmental bodies to keep their fund data secure. Six in 10 indicate a strong lack of confidence.

"Today, the globally regulated alternative investment industry is more transparent than it has ever been," MFA President and CEO Richard H. Baker said. "Regulators have substantial information about many funds, including data on activities, holdings, size, leverage and liquidity. The security of this often sensitive and proprietary information is a top concern for MFA members."

As the MFA noted in a recent letter to the Security and Exchange Commission, the list of federal government cyber breaches is long and growing, including the White House (2014), Department of State (2014), Federal Deposit Insurance Corporation (2015, 2016), Federal Aviation Administration (2015), Department of Defense (2015), Internal Revenue Service (2015, 2016), Office of Personnel Management (2015), the Pentagon (2015) and the Federal Reserve (2011 to 2015) It is perhaps not surprising, therefore, that managers' trust in government security is low.

At the same time, however, respondents also suggest that current cyber regulations may be nearing maturity with almost half—48 percent—of our respondents saying current regulatory requirements are sufficient for the industry. Just 30 percent say current cyber regulation was insufficient.

"You can't count on simply meeting current cyber-security regulatory standards as a strong defense against the evolving cyber threat," Robert Mirsky noted. "You need to be at least as good as the industry and—if you hope to avoid litigation and regulatory fines—you probably want to be above average in your cyber capabilities."

The article was taken from KPMG's publication, entitled Transformative change. How innovation and technology are shaping an industry by Robert Mirsky of KPMG International, Jeffery Kollin and Adam Hirsh of KPMG in the US and Daniel Page of KPMG Ireland.