Reaping the security advantage: Talking to bank CEOs

Six ways bank CEOs can turn cyber into opportunity

Bank CEOs have made great headway on the cyber agenda over recent years. Most banks have made significant investment into cyber security and their CEOs recognize it as part of their personal responsibility. For the most part, major events have been avoided, regulatory requirements have been met, and awareness is rising.

So it is not surprising that bank CEOs say they are increasingly confident about their cyber capabilities. Indeed, in a recent global survey of 120 bank CEOs conducted by KPMG International last year, 42 percent reported that they were now 'fully prepared' for a cyber event (a massive jump from the 19 percent who said the same the previous year). And at least six-in-ten said they are now fully prepared for a customer data breach or software attack.

Bank CEOs are so confident, in fact, that many seem to believe that their cyber security prowess could help them improve their brand reputation and rebuild trust with customers. In our survey, two-thirds of the respondents said they see investment into cyber as an opportunity to find new revenue streams and drive innovation. And 78 percent said they plan to increase investment into cyber security over the next 3 years.

Hitting a moving target

While bank CEOs have lots of reason to be confident in their progress, my experience working with leading banks over the last 20 years suggests that some may be underestimating the challenge.

The reality is that it is very difficult to be 'fully' prepared for a cyber event. In part, this is because the nature of the threat and the risk vectors are continuously evolving and cyber attackers are constantly adapting. At the same time, the introduction, development and adoption of new technologies and business models also lead to new and unexpected cyber risks. It's hard to be 'fully' prepared for something that is rapidly changing.

The response may also suggest that — while awareness of the cyber risk has certainly increased at the board level — this may not be translating through the business management structures in a way that allows them to fully understand or appreciate the real nature of the risk they are trying to manage. More often than not, cyber is viewed through the lens of a technical discipline and set of controls rather than through a genuine understanding of the cyber risks and their business impacts. It is easier to be confident in whether a control is operating or not; less so to understand the end-to-end business operational risk.

The survey data also indicates that there may be a bit of a gap between executive awareness and execution. Bank CEOs may be aware of the challenge, they may be pouring in investment and driving development of the right frameworks and controls, but this may only provide a false sense of security if the rank-and-file don't understand the risk and take ownership of it.

Sleep better at night

CEOs have a lot to be proud of on cyber security. And they should keep up their momentum. Keep improving awareness of the risks and threat environment. Keep championing the drive for better cyber security. Keep encouraging your organization to be better, more aware and more responsible. And keep investing in the cyber technical capability (this is increasingly critical to securing the ever-evolving business technology infrastructure).

However, my experience also suggests that there are a few areas where bank CEOs may want to focus if they hope to turn cyber into a real competitive advantage.

1. **Improve the quality of the board discussion.** In part, this is about simplifying the reporting to allow decision-makers to focus on the risks that matter most. But it is also about changing the language of the discussion from a technical base to a more business-oriented strategic one. Boards should also try to integrate cyber into the enterprise and operational risk registry — recognizing cyber as a fluent and integrated business risk rather than an add on — to improve integration and help identify unexpected but related risks to the business.
2. **Enhance the relevance at the business level.** To take ownership over the risk, the business first needs to genuinely understand it. That means explaining it in business terms, supported by understandable data and real-life implications. Some banks are starting on this journey by translating their threat intelligence into more understandable business processes and metrics such as the value of fraud prevented, third-party risk or critical business data protected.
3. **Embed security into the culture of the enterprise.** Controls are fairly easy to fix. Changing behaviors is much more difficult. Bank CEOs will want to renew their efforts to create a culture of cyber security where awareness and individual ownership is balanced against the growing demand for business innovation and flexibility. While setting the right tone from the top is crucial, this is about making sure employees live and breathe cyber in their daily activities.
4. **Monitor your investments and your risks.** Banks are certainly pouring significant investment into cyber. But few are able to accurately explain how these investments are changing their risk profiles or how their activities are helping mitigate risks. In order to improve the value of investments, bank CEOs will want to start by improving the way their investments and risks are monitored.
5. **Assess your cyber response model.** Look across your entire security ecosystem and try to identify opportunities to improve performance and increase alignment of cyber capabilities across the enterprise. Seek out areas where automation and artificial intelligence might improve efficiency and lead to better quality outputs. Where necessary, leverage outside service providers and advisors with unique skills and capabilities in the right way to allow your internal team to focus.
6. **Get the right talent.** Finding and retaining the right cyber talent will become increasingly difficult as organizations across business sectors start to improve their cyber response. More than just good cyber talent, however, banks will need to find (or develop) individuals that are able to not only stay ahead of the threat, but also bridge the gap between cyber and the business.

No time to slow the pace

While it may be easy to become discouraged or fatigued by the never-ending cyber battle, bank CEOs should take heart; they are making good progress and seem to be maintaining an upper hand. They should keep doing what they have been doing. But if bank CEOs want to turn cyber into a competitive advantage, they'll need to invest more effort in key areas.

Contact

KPMG AG
Badenerstrasse 172
PO Box
CH-8036 Zurich

kpmg.ch

Matthias Bossardt
Partner
Head of Cyber Security

+41 58 249 36 98
mbossardt@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence.

© 2018 KPMG AG is a subsidiary of KPMG Holding AG, which is a member of the KPMG network of independent firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss legal entity.
All rights reserved.

Reaping the security advantage: Talking to bank CEOs May 2018