Five Key Strategies for Bank Boards to Improve Cybersecurity Defense and Awareness

Jeffry Powell
Executive Vice President, The Americas

Charlie Horrell
Managing Director, Europe, Middle East and Africa

Al Percival
Managing Director, Australia and New Zealand

Diligent

The world continues to experience an increase in the number and severity of high-profile cyberattacks, a trend that shows no signs of easing. From large financial institutions and brokerages to blue-chip retailers, ***hackers are gaining traction and notoriety as they breach systems with greater impact and severity****—many of them stealing private customer data. The reality is that every organisation—big and small—is susceptible to these attacks.*

Five Key Strategies for Bank Boards to Improve Cybersecurity Defense and Awareness

Banks, in particular, are challenged to protect proprietary information, client data and in many cases, shareholder value. Bank directors and board members equipped with the proper tools and information about cybersecurity are more prepared to keep their organisation safe in the event of a cybersecurity breach. In order to ensure an organisation is fully equipped to mitigate risks associated with hacks and other cyberattacks, there must be a clear understanding among all levels of the financial institution's management team about who is responsible for managing this issue. When the senior management and the board ensure that cyber policies are up to date, understood by all and frequently tested, companies decrease their chance of exposure. For directors at financial institutions, here are five key strategies to improve cybersecurity defenses and awareness:

SECURE COMMUNICATION:
Companies must provide board members with a secure way to share and communicate critically sensitive information. This information should never be sent over email.

COLLABORATION IS KEY:
When directors have a clear understanding of cyber security and the associated risks, they are more equipped to work together to manage issues related to cybersecurity.

HAVE A STRATEGY:
Determine, in advance of a data breach or other cyber attack, who is responsible for managing cybersecurity, whether it be an audit committee, another committee, the organisation's IT department or the chief information officer.

UNDERSTAND THE CLOUD:
Understand what cloud services your bank and your bank's vendors are using, public or private, for file sharing or downloading sensitive information. While cloud solutions can offer easy uploading and downloading of files as well as security features like encryption and authentication, many have been successfully hacked, compromising private files and email addresses.

EDUCATION AND PREPARATION:
Ensure board members educate themselves on cybersecurity to understand the risks and be prepared for whatever comes their way; this is where many vulnerabilities surface, not because a board lacks the appetite, but because directors are not provided with the proper tools and information.

Cybersecurity should be a topic on all bank directors' radar, and they should continue to embrace new strategies as they grapple with ways to confront, manage and control issues around cybersecurity.

Additionally, adopting technologies in order to ensure secure, fast and accessible communication is vital. This is especially true for a company's board of directors, which is privy to sensitive, confidential and market-moving information. Throughout history, financial institutions have constantly evolved to reflect changes both in society and in the market. Cybersecurity presents a complicated challenge, but it is one that can be confronted successfully with the correct management strategy and tools.