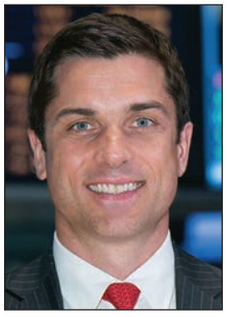
Views on Cyber

LEADERS asked a number of C-suite executives the following two questions regarding cyber risk today:

What are the key issues that CEOs and boards need to address to protect their organizations from the increasingly high risks associated with cybersecurity?

How critical is the role of the chief information security officer (CISO) in your organization?

Their answers follow:



Tom Farley

Tom Farley, Group President, NYSE

Cybersecurity risk is a pervasive threat that exists across all industries and regions and requires responsibility for cyber governance to be a top priority in every company. Corporate executives and directors must address cybersecurity as a foundational governance issue in order to understand and prepare for the risks.

The NYSE supports exemplary governance and risk oversight practices because they underpin the sound operation of our capital markets. Cybersecurity risk is endemic and, as nearly every expert will say, cannot be avoided. The key for public companies is to prepare, respond, and develop resilience so that confidence in our public markets remains steadfast and certain. ●

Bill Pence

Bill Pence, Chief Technology Officer, AOL Inc.

The level and sophistication of the attacks is continually increasing. In addition to moving beyond traditional IT security solutions (perimeter protection), new tools need to be employed that look for malicious activity inside the network. In addition, employee vigilance is critical to avoid social engineering attacks (such as spear phishing), which are simple modes of attack that can do great damage. Finally, response plans must be in place in the event that a breach occurs. How a company responds in the event of a breach is just as important as how it works to avoid one.

The CISO role is critically important and getting harder all the time as the "attack surface" increases. The CISO has to define a protection strategy, which is increasingly based on not just tools but organizational behavior and awareness, in a world where qualified IT Security skills are scarce. We continue to invest in the security function in terms of leadership, resources, and support across all parts of the organization. ●

Michael I. Roth

Michael I. Roth, Chairman and Chief Executive Officer, Interpublic Group

Cybersecurity risks continue to escalate and no company is immune from the threat. Today, CEOs and Boards need to view cybersecurity as a critical business issue, one that requires governance at the highest levels. As new digital lines of business and new digital channels are created, cybersecurity is critical to a company's business, no matter the sector.

CEOs and boards need to set the tone within the company on the importance of managing the risk. No company can completely defend against all attacks, so it's important to identify the critical data within an organization, and go beyond traditional defenses in those areas. For us, we've put in place a "risk management" approach, with advanced monitoring that can detect any breach and execute on a formal incident response plan to quickly deal with an attack.

The CISO role is extremely important to our company as she's fully dedicated to the oversight of our cybersecurity program. Through independent management, the CISO provides guidance to our IT departments and business leaders, she sets IPG's overall cybersecurity strategy, and she determines our security architecture.

Within our company, the CISO acts as a single point of contact for our board and is responsible for communicating the overall cybersecurity risk profile of our company. While cybersecurity is the responsibility of all our business units and our employees, the CISO provides continuity to our program and vital expertise to our agencies. ●

David Thompson

David Thompson, Executive Vice President, Global Operations and Technology and CTO, Western Union

Some key issues today include insider threats, so it is crucial that organizations understand normal employee and contractor baseline behaviors, while ensuring a culture of security where those internal to the organization understand how they may be used as a conduit for others to obtain information. It is also important for the CISO and his/her team to constantly monitor the ever-changing outside world of IT to stay up to speed.

Investment in analytics has played a key role for Western Union in merging data to reduce risk and conduct compliance and fraud modeling across all channels. As a transaction is processed, the company has built a real-time risk decision engine to help prevent fraudulent transactions. They marry WU's offline data with its real-time data in a cluster for real-time risk analysis. In addition, Western Union's digital end capabilities allow its compliance analysts to review the transaction and feed this with 22 different data sources, providing data for the risk decisioning.

The company possesses an industry-leading pay-in, pay-out capability that leverages technology, foreign exchange conversion, and data management, as well as a regulatory, compliance, and anti-money laundering (AML) infrastructure, to expedite efficient and timely money movement almost anywhere in the world. In order to successfully operate in this manner, the role of the CISO at Western Union is critical.

The company's CISO has the responsibility of managing all aspects of the company's information security strategy and risk management programs worldwide, including development and execution of the enterprise-wide information security strategy and driving the implementation of security-related programs within the business. The CISO is also responsible for ensuring proper development and implementation of corporate information security control policies and standards, as well as ensuring the appropriate tools and metrics are in place. ●