Cybersecurity and the Resilient Mindset

By Cindy Fornelli

If you spend some time around the issue of cybersecurity, it won't be long before you encounter the notion of resilience.

"Cyber resilience is a public good," observed a 2017 white paper from the World Economic Forum. A 2013 Presidential Policy Directive declared that "it is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats."

For company leaders and boards of directors grappling with cybersecurity challenges, it's worth pausing for a moment to reflect on the meaning of "resilience." Merriam-Webster defines the word as "an ability to recover from or adjust easily to misfortune or change." Synonyms for resilient include flexible, elastic, and supple. Among its antonyms are inelastic, inflexible, and rigid.

Each of those synonyms and antonyms could be used to describe a system or infrastructure. They could also describe a mindset. Resilience, in other words, doesn't just apply to the nuts, bolts, bits, and bytes of cybersecurity—it also should inform how we think about cybersecurity.

And in fact, this resilient mindset is evident in a growing number of tools and resources that can help companies, investors, boards of directors, and others face cyber-challenges.

The Changing Cyber Landscape

Grasping the importance of cyber resilience starts with having an overall sense of the cyber-threat landscape. A key aspect of that landscape is that it is not static. It changes and evolves with a velocity driven by the grim economics of cyber-crime.

Adding complexity, organizations face varying threats and actors. Criminals seek to steal data from organizations to use it for quick, unlawful financial gain. Nation-states may launch cyber-attacks to conduct economic espionage or to fulfill geopolitical objectives (or both). Employees, whether intentionally or unintentionally, are all too often a source of compromised security access.

Complicating all these threats is the fact that technology continues to evolve rapidly. As organizations harden their security defenses, adversaries shift to new tactics and targets, requiring organizations to continuously evolve their cybersecurity risk management programs.

Tools to Aid a Resilient Mindset

If the shifting cyber landscape demands continuous evolution, then executives and directors cannot afford to be inelastic, inflexible, and rigid. They must be the opposite: resilient.

What does that resiliency mean in practice? Several cybersecurity resources show the resilient mindset at work. One of those resources certainly should be of interest to boards of directors: the *Director's Handbook on Cyber-Risk Oversight*. The *Handbook* is a collaboration of the Internet Security Alliance and the National Association of Corporate Directors (NACD), and it notes that "there is no single approach that will fit every board." The publication includes key questions to ask regarding situational awareness, strategy and operations, insider threats, third-party risks, and incident response.

Boards, management, and others should also consider a valuable new resource from the American Institute of CPAs (AICPA). Its recently unveiled cybersecurity risk management framework has three key components:

- Management's description of the entity's cybersecurity risk management program, based on suitable criteria

- Management's assertion as to the presentation of their description and to the effectiveness of controls implemented to achieve the entity's cybersecurity objectives

- A CPA's opinion on that description and the effectiveness of the controls to meet the entity's cybersecurity objectives

Emphasizing flexibility, the AICPA framework is principles-based and voluntary; companies do not need to implement all its components at once. Rather than prescribing specific requirements, the framework sets forth the types of policies and procedures that companies can adopt for cybersecurity risk management.

With the aid of the criteria, companies can assess their cybersecurity efforts and decide on the best path forward. The AICPA framework leverages existing cybersecurity and risk management structures. It maps to commonly used cybersecurity risk management frameworks, such as those put forward by the International Organization for Standardization and the National Institute of Standards and Technology.

Learn more about the framework at the AICPA website and in this 2017 white paper from the Center for Audit Quality.

Tools such as the ones from the AICPA and the NACD don't rigidly prescribe how companies and directors should act. They provide questions to ask, principles to follow, and options for action. They enable a resilient mindset, which is vital to tackling the many challenges of cybersecurity.

A securities lawyer, Cindy Fornelli has served as the Executive Director of the Center for Audit Quality since its establishment in 2007.