CORPORATE BOARD MEMBER®
A DIVISION OF CHIEF EXECUTIVE GROUP, LLC

FALL 2017

A NEW GLOBAL SECURITY IMPERATIVE

By Tom Kennedy and Matt Moynahan

IMAGINE MASKED intruders charging into a hospital, holding its critical operations and patient records hostage until a ransom is paid. Now imagine that happening across continents indiscriminately, disrupting industries in more than 150 countries by halting everything from assembly lines and global shipments to important government services.

This kind of global attack is the computer network equivalent of what happened earlier this year when the ransomware computer virus WannaCry was launched by hackers demanding payment to release computer files held hostage. Another incident a few weeks later involved a super-charged variation of the previously discovered Petya ransomware. It spread across the globe, shutting down critical networks, including the radiation monitoring systems of the Chernobyl nuclear power plant in Ukraine.

These global attacks make clear that sophisticated hackers—many of them employed or supported by foreign nations—are escalating the number of cyberattacks on ill-prepared commercial companies and private institutions. By targeting commercial networks, attackers threaten the critical services we rely on and our underlying stability, creating the potential for a global security crisis.

"ORGANIZATIONS THAT DO NOT PRIORITIZE CYBERSECURITY FACE LAWSUITS, COSTLY SETTLEMENTS, OR WORSE: A DIMINISHED BRAND, ALONG WITH LOSS OF BUSINESS CONTINUITY, INTELLECTUAL PROPERTY, AND CUSTOMER CONFIDENCE."

Consider that more than 85% of the networks, devices, and infrastructure of the internet is in commercial hands. That makes the future of the internet dependent on commercial companies elevating their security and resiliency. Nation-state defense and commercial network defense are now inextricably linked in the cybersecurity arena.

As the CEOs of a major defense technology company and a commercial cybersecurity company, we are in agreement, these attacks exemplify a new dimension of global security—one that puts the commercial and private sectors on the front lines.

Simply put, these attacks are a wake-up call. We have entered a new era when business leaders must evaluate their companies' exposure to risk through a broader security lens, something that will not come naturally to CEOs or boards.

Yet, from our vantage point, the commercial sector is not prepared for the looming threat. Few boards fully appreciate their exposure to cyber risk, whether from negligent or malicious insiders, a compromised supply chain, the growing attack surface area represented by the internet of things, or the increasing number of sophisticated attackers who see businesses as easy targets.

For boards and senior leaders, this means realizing their company's operations reside in a contested domain. No longer can they assume the only targets within their company are trade secrets and credit card numbers. Cybersecurity must be treated as much more than an IT issue; for too long it's been an afterthought, taking a backseat to a focus on cost, convenience, or speed to market when new products, online services, devices, and software are introduced. Given today's threat environment, every company must assume that their network has been compromised, that threats will penetrate the perimeter and get inside.

Actively questioning management about cybersecurity within the organization is a critical part of board oversight and risk mitigation. Boards should insist that the company's cybersecurity plan includes network intruder detection, data leakage prevention (DLP), and insider threat protection (internally focused security and monitoring to detect inappropriate user activity). Boards must also work with management to ensure the cybersecurity operation is adequately staffed and funded.

The threat and consequences from cyberattacks will continue to increase as the commercial sector continues to grow its dependence on the internet of things and drive automation, artificial intelligence, robotics, and other innovations into critical services that underpin our society. We have to get this right. Organizations that do not prioritize cybersecurity face lawsuits, costly settlements, or worse: a diminished brand, along with loss of business continuity, intellectual property, and customer confidence.

In our networked, big data–driven economy, a new paradigm has emerged: When everything is connected, everything is vulnerable. This is a message we've been sharing as widely as possible; it's that important. The good news is that companies that successfully navigate these security concerns will gain a strategic advantage and help enhance our global security.

Tom Kennedy is Chairman and CEO of Raytheon Co. and Matt Moynahan is CEO of Forcepoint.