NATIONAL ASSOCIATION OF CORPORATE DIRECTORS
CHICAGO CHAPTER

OCTOBER 13, 2017
CHICAGO CHAPTER EVENT SUMMARY

## A Conversation with Tom Ridge: The Board's Responsibility for Cybersecurity

On October 13, our members and guests gathered to hear Tom Ridge, the first Secretary of the U.S. Department of Homeland Security and twice-elected governor of Pennsylvania, engage in a lively discussion on The Board's Responsibility for Cybersecurity. The session was expertly moderated by Alan Raul, founder and leader of Sidley Austin's privacy and cybersecurity practice. Sidley also hosted this NACD event.

Cyber-risk oversight is one of the top concerns that Boards of Directors are facing today. As is witnessed daily, most recently with Equifax, it is an enterprise-wide risk management issue, not just an IT issue. As Tom Ridge described cybersecurity, "It is the 5th dimension in the geo-political and economic warfare that is happening 24/7." This warfare is being conducted by such known "bad actors" as China, Russia and Iran among many others. They are after unique information that has high reward and they have very little risk of being caught or held accountable. The landscape for risk is only going to accelerate. The internet, or digital echo system as Ridge referred to it, is open, ubiquitous, and has no borders, and the Internet of things (IoT) is creating an even larger virtual portal of vulnerability

As a first step in evaluating potential vulnerability to a cyber-attack, Ridge recommended that companies need to ask:

1. What data in my shop has value to someone else? His many examples include employee data, M&A transaction data, marketing data, for starters.
2. Does my company have a culture in place to manage risk? While it is impossible to eliminate the problem, are we doing everything we can to manage the risk?
3. How prepared are we with a response and recovery plan and how quickly can we respond to all our key stakeholders—customers, shareholders, employees, regulators and others?

While cybersecurity is the #1 security threat this country faces, Ridge cautions that the private sector, to its detriment, relies too much on the government for a solution. He warns in the case of a cyber-attack, the government can be punitive and agencies like the FCC and FTC are likely to blame the company that has been victimized for being insufficiently prepared and protected.

He suggests that the best defense is a strong offense, and the paramount importance of having state-of-the art tools, a strong IT team and a readiness plan. To him, resiliency is critical. And, while historically cybersecurity has been considered a corporate expense, he believes it should be considered an investment in risk management. Although there has been a modest paradigm shift to this thinking, he does not believe it is enough.

Since managing risk to the enterprise is a fiduciary responsibility of a Board of Directors, here are some parting suggestions to help Board members think about vulnerability to a cyberattack:

- Make sure there is a plan in place for the Board to be timely informed of any cyber breach. Ridge cited the Yahoo situation as a learning opportunity.
- While most Boards do not have a separate cybersecurity committee, decide what committee should handle first line responsibility. He doesn't think it is important where this responsibility lies, only that it exists and that it has the attention of the C-Suite.
- Do not be complacent. Instead do some skeptical probing in a constructive way—are our networks segmented? Who has access to what? Who does the analysis of the monitoring logs?

- Find out what the IT team is most worried about as opposed to focusing only on what they do well.
- Accept the reality that you have to manage the risk before it manages you.