FEATURES

Learning to 'Manage the Risk Before It Manages You'

by **Ashley M. Marchand** I July 30, 2015

The Hon. Tom Ridge

While the Internet initially was a communication tool between the U.S. Department of Defense and multiple academic organizations, it has become the backbone of a global economy and government operations, the Hon. Tom Ridge told a rapt audience of more than 200 directors at the NACD Strategy & Risk Forum in San Diego. The first secretary of the U.S. Department of Homeland Security, Ridge currently serves as president and CEO of the strategic consulting firm Ridge Global and is a director for The Hershey Co. Ridge delivered the opening keynote to directors convened for the two-day forum co-hosted by the National Association of Corporate Directors (NACD) and its sponsors.

"We've come a long way from a simple communication tool," Ridge said. "What's really remarkable is the tool is designed to be an open platform. It wasn't designed to be secure. It wasn't designed to be global. The ubiquity of the Internet is its strength, and the ubiquity of the Internet is its weakness. For every promise of connectivity, there's a potential vulnerability."

These vulnerabilities bring implications for directors, Ridge continued. "Those of us who are working in corporations—whether publicly or privately held—have to accept this as a reality of this digital forevermore. The threat surface changes and expands every single day," he said.

A report released last year by McKinsey & Co. and the World Economic Forum found that more than half of all respondents

surveyed and 70 percent of executives from financial institutions view cybersecurity as a strategic risk to their companies. The report was based on interviews with more than 200 chief information officers, chief information security officers, law enforcement officials, and other practitioners in the United States and around the world.

About 60 percent of the survey respondents said they believe the frequency or sophistication of cyberattacks will grow faster than institutions' ability to defend themselves.

"In this world, you've got to manage the risk before it manages you," Ridge advised the audience.

Support for the forum was provided by BDO USA, the Center for Audit Quality, Dechert, Dentons, Diligent, Heidrick & Struggles, KPMG's Audit Committee Institute, Latham & Watkins, Pearl Meyer & Partners, Rapid7, and Vinson & Elkins.

The Chattering Class

Risks to reputation are nuanced and numerous. Panelist Andrea Bonime-Blanc, CEO and founder of GEK Risk Advisory, described reputation risk as an "amplifier" attached to all other risks. If a company is not properly handling other risks, like those related to cybersecurity or the environment, then reputation also is at risk.

The key to understanding a company's reputational risk is knowing the expectations of stakeholders, said Bonime-Blanc, author of *The Reputation Risk Handbook: Surviving and Thriving in the Age of Hyper-Transparency*. "The customers at a pharmaceutical company are going to expect products to be safe," she said. "If the products aren't safe, the expectations of the stakeholders will not be met and they leave that company—whether it's investors, customers, or partners."

Jonathan Blum, senior vice president and chief public affairs and global nutrition officer for Yum! Brands Inc., which operates 41,000 KFC, Pizza Hut, and Taco Bell restaurants worldwide, has seen firsthand the damage that can be done to a company's reputation. He recounted an incident that hit the brand's reputation and bottom line, and ultimately spurred substantial changes in the company's supply chain.

In December 2012, a state-owned television network in China reported that some local poultry suppliers were putting unlawful amounts of antibiotics in chicken. One of the many suppliers investigated happened to be one of KFC's suppliers, albeit one of the restaurant chain's smallest. "But, because we're the largest brand in China, not just the largest restaurant, we obviously bore the brunt of the publicity," Blum said.

The most damaging aspect of the negative attention, according to Blum, was not the investigative report that aired on television, but rather the chatter on social media in the wake of the report. The fallout was a tarnished reputation, a sharp downturn in sales, and

some decisive action.

"Consumer trust plummeted. Belief in our brand plummeted. Our sales plummeted. We saw a huge drop in our stock," Blum said. "Now, this was at the end of 2012, so the impact on our financial results that year was negligible. Up until 2013, we had had a 10-year run of at least 10 percent [earnings per share] growth year over year, which is pretty unusual. In 2013, given the ditch we were in in China, our earnings per share dropped 9 percent. We lost $270 million in profit as a result of this incident, and it took about a year to rebound." In the aftermath of the negative publicity, Yum! Brands learned that its stakeholders wanted answers to three questions:

1. What happened?
2. What was being done about it?
3. How would the company prevent it from happening again?

Yum! Brands apologized to the public, fired about 1,000 small poultry suppliers, and worked with the Chinese government to upgrade the quality of the poultry supply.

"Over time, that rebuilt consumer trust," Blum said.

The company also took a significant step toward managing its reputation on social media.

"As a result of this incident, around the globe, 24/7, we monitor what consumers are saying about us and we immediately respond," Blum said. "We have this device in place that's a 'word cloud,' and we see what consumers are saying in nine languages. We have analysts who do nothing but look at this and respond. We've trained 500 people on it around the globe."

Disclosure Questions

During a panel related to disclosure, liability, and reputational risk, attorney David H. Kistenbroker asked directors to consider what they should disclose in their normal filings. Then, when something negative and outside of the norm occurs, the board should again engage in a deep discussion about disclosure, Kistenbroker, global co-head of white collar and securities litigation at the Dechert law firm, noted that determining what and when to disclose can be difficult—especially in the emerging area of cyber risks, where policies and corporate practices are in development.

"For the regular public company filer, it can be nebulous," Kistenbroker said. "You have civil and criminal guidance. We tell people that criminal comes first, civil second." A company might not disclose a breach as soon as the Securities and Exchange Commission (SEC) prefers because the Department of Justice may still be probing the situation to the extent that your SEC disclosure could compromise the DoJ investigation, he added.

"It's a really critical point as to what type of breach it is, who was

affected, and the industry," said Leslie Thornton, senior vice president, general counsel, and secretary of WGL & Washington Gas Light Co. "If you are working with the federal government, they've not only told you not to talk about it, but have said it could compromise national security."

There are some cases, however, when timely disclosure is necessary. "If you have 10 million people who've been exposed to credit card breach, you have to disclose that quickly—that's a material breach," Thornton said.

Public companies are required to disclose to investors any material (i.e., financial) harm by filing with the SEC. That would include cyber or data breaches.

Some companies have been criticized for filings that do not comprehensively disclose the full effect of a breach or for not filing at all when a breach occurs.

Panelists agreed that directors should be comfortable turning to experts for assistance before and after a breach. Directors also should be familiar with disclosure or seek an overview on disclosure law from the general counsel, said Cheemin Bo-Linn, a director of Violin Memory, president and CEO of Peritus Partners, and former vice president of IBM.

The board may also opt to have a law firm facilitate the post-breach conversation, Kistenbroker said.

While local FBI agents can be helpful to a company after a breach, Thornton recommended contacting the FBI's National Cyber Investigative Joint Task Force, as well, to learn more about emerging cyber threats by industry.

"Once you think about the flexibility you have in disclosing, remember that you have civil codes that may come into play," Bo-Linn said. "Make sure the folks in customer service know how to respond and that the credit bureaus are alerted."

Chips Everywhere

One forum session was devoted to the strategic opportunities and cyber risk associated with the Internet of Things (IoT), which refers to the ability of everyday objects like cars and toothbrushes to connect to the Internet and transmit data, and what is commonly referred to as the next major computer age: that of social, mobile, analytics, and cloud technology, or SMAC. "In many ways, the IoT is going to ride on the coattails of SMAC," said John Hotta, former senior director of Microsoft and director of Swedish Healthcare and Martha Graham.

In a survey released last year, the Pew Research Center found widespread acceptance of chip-enabled devices. The survey of more than 1,600 Internet experts revealed that 83 percent of respondents believed that as billions of devices and accessories are networked, IoT will have widespread and beneficial effects on

daily life by the year 2025. Despite the perceived benefits, there may be embedded risks for IoT and SMAC.

"Former CIA Director George Tenet said, 'We are staking our future on a resource that we have not yet learned to protect,'" said Kevin R. Brock, former assistant director for intelligence at the FBI, and president and CEO of BrockCRS, which consults to companies and boards on issues related to cyber risk, and strategy.

One panelist highlighted what could prove to be companies' motivation to focus on cybersecurity as advances in technology proliferate. "It might not take a meltdown for companies to understand the need to adapt to cybersecurity risk," said Robert A. Clyde, a director at Zimbra and ISACA (formerly known as the Information Systems Audit and Control Association). "It just takes competition."

This story is from the July/August 2015 issue of NACD Directorship *magazine.*

National Association of Corporate Directors
2001 Pennsylvania Ave. NW, Suite 500
Washington DC 20006
Phone 202-775-0509 | Fax 202-775-4857