THE
NATIONAL LAW REVIEW

Preparing to Deal with Digital's Looming Dark Side

Article By
Risk Management Magazine
Risk and Insurance Management Society, Inc. (RIMS)

- Criminal Law / Business Crimes
- Consumer Protection
- Insurance Reinsurance & Surety
- Intellectual Property
- Communications, Media & Internet
- Administrative & Regulatory

- All Federal

Wednesday, October 31, 2012

Extraordinary online business benefits have revolutionized business and, as digital interconnectedness continues growing daily around the globe, so too do the implications of its power. Managing assets and financial risk in business today relies heavily on the speed and ubiquity of computer connections and networks globally. As Microsoft founder Bill Gates noted, "Information technology and business are becoming inextricably interwoven. I don't think anybody can talk meaningfully about one without the talking about the other."

But, for the nation's risk managers, it is clear that cyber-risk has become the revolution's menacing dark side. Increasingly, headlines spotlight massive credit card privacy breaches, allegations of sovereign espionage, and "hacktivists" penetrating the firewalls at the Department of Justice and other federal agencies, sending shudders through risk officers charged with protecting corporate assets, regardless of whether those assets are intellectual property, financial transactions, customer data, supply chains or infrastructure. Adding new urgency to the

cybersecurity topic are increasingly commonplace—and alarming—headlines on news stories, such as the Wall Street Journal's recent story, "U.S. Outgunned in Hacker War."

In the "2011 Emerging Risk Survey Report" of 2,500 members of the Joint Risk Management Section of the Society of Actuaries, the Canadian Institute of Actuaries and the Casualty Actuarial Society, cybersecurity/interconnectedness emerged as the risk likely to have the greatest impact over the next few years, rising from 23% in 2010 to 38% in 2011.

Only "financial volatility" at 69% and "failed/failing states" at 42% ranked ahead of cybersecurity in the current survey, which was conducted by Max Rudolph, a fellow and chartered enterprise risk analyst of the Society of Actuaries. "Chinese hard landing" and "oil price shock" round out the top five risks, though oil price shock is viewed as more important in combination with various other risks.

Even after acknowledging cognitive bias that encroaches on almost all surveys and prompts respondents to "anchor in" or be influenced by recent events, cybersecurity concerns and cyber-risk fears have emerged as high-priority concerns across a broad spectrum of influential leaders and decision makers. For example, at the 2012 World Economic Forum (WEF) in Davos, Switzerland, the topic was top of mind with global CEOs, who ranked cyberattacks among the top five events in terms of "likelihood," noting that increasing connectivity (internet users per 100 people globally) was expected to grow from 17% in 2005 to 40% by 2015.

Further, the WEF report suggested a key axiom for the Cyber Age: "Any device connected to a network of any sort, in any way, can be compromised by an external party. Many such compromises have not yet been detected."

Clearly, the axiom focuses on the heart of the risk: the pervasiveness of the potential ignition points for an intentional or accidental significant cyberevent. Of greatest concern is a major disruption of critical information infrastructure caused by cybercrime, terrorist attack or technical failure that results in a failure of a critical-service infrastructure, such as power distribution, water supply, transportation, telecommunication, emergency services or finance.

For the entire enterprise risk management field, accurately assessing the potential impact of cyberevents for organizations is a task well-suited to actuarial expertise. As they always have, actuaries assess risk, bringing specialty skills related to modeling, statistics and probabilities to the task. But, potentially even more important today is the actuary's ability to integrate disparate information from diverse sources—external sources as well internal functions such as IT, finance, business continuity, etc. By building meaningful, coherent risk scenarios that integrate a broad range of relevant factors, actuaries generate predictive models that can weigh complex risks and opportunities and communicate these issues to inform strategic decision making within an organization.

Source URL: https://www.natlawreview.com/article/preparing-to-deal-digital-s-

looming-dark-side