Resilient and Risk-Aware: Ah-ha Moments in Cyber Risk

By Melanie Lockwood Herman

Executive Director

Resource Type: Risk eNews

Topic: Data Privacy, Tech Risk, Cybersecurity

This week I've been engrossed in *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*, by Richard A. Clarke and Robert K. Knake. The book is one of several I've been reading this Summer to inspire my team's obsessive focus on resilience and business continuity planning. Clark and Knake describe 'resilience' in a way that fits perfectly with our aspirations for effective risk management: ". . . resilience is about the ability to rapidly respond, return to a good state, manage bad outcomes, and learn from the incident so that future incidents are less likely."

Much of the book is music to a risk professional's ears, including: "Above all, our guiding principle is to avoid solutions that would cause more disruption than the problems they are meant to solve." In the NRMC team's view, all new risk policies and practices should be evaluated in terms of their potential to cause 'organizational drag.' In a prior RISK eNews titled "Risk Management's Unintended Consequences," we discuss how "sometimes risk management can hamper decision-making and cause an organization to be less nimble in responding to risk events or in leveraging opportunities." Sound familiar?

The authors' optimism about our potential to manage cyber threats rings loud and clear: "We think it is possible to reduce the risks posed by offensive cyber technologies and actors, and to increase peacetime stability for corporations and crisis stability for nations." They also affirm the belief that "the specter of cyber warfare does not overshadow all the good things that are made possible by the internet," and "… for most purposes, the security bang for the buck you get by moving to the cloud is well worth accepting the residual risk."

Much of the book is devoted to a wakeup call about the potential—and the reality—of the harm and chaos that organizations and nation-states face today. Although I customarily write in the margins of the books I'm reading, I found myself using 'ah-ha' to mark some of the most thought-provoking passages. My ah-ha moments from *The Fifth Domain* included:

The Cloud

- "The danger with cloud computing is that it is concentrating risk in the hands of a few players that now have a near monopoly."
- "Because the cloud is 'multitenant,' meaning that multiple companies or users are running on the same

hardware, there is the potential that an adversary who could compromise a vulnerability like this could access multiple sets of data at once."

Backups

- "Cybersecurity experts have been warning companies that hackers are placing ransomware in database backups, so that when network operators attempt to activate their business continuity systems, they will find that the backup is inoperable too."
- "If you back up your data every day, you may well have backed up the malicious software that later infected your network. Hackers are waiting a week or so after they get on your network before activating their encryption software. By so doing, they get in your backup."

Cyber Crime

- "It's no secret the United States typically ranks up with China as the country where most malicious cyber activity occurs. That is, in large part, because there are more computers that are more powerful and connected at higher rates of bandwidth in the United States than anywhere else in the world."
- "…cyber criminals are now doing what fledgling start-ups are doing and buying computing power from Amazon's cloud (the only difference is that they use stolen credit cards to make the purchase)."

Tech Economics

- "Information systems technology does not always reduce the cost of doing business, as some people believed in the 1990s."

This week the NRMC team is proud to publish **The Business Continuity Planning Issue** of our magazine, *Risk Management Essentials*. The issue features two articles exploring BCP basics and options, and one piece on cloud computing's BCP benefits. You can read or download the entire issue here or view the individual articles at the following links:

- "Business Continuity Planning: Taking it from the Backburner to Front and Center"
- "Cloud Computing – BCP Boon or Boobytrap?"
- "Three Chords & The Truth: Methods for Approaching Business Continuity Planning"

We hope that your team has been inspired by your own resilience in the face of COVID-19 to dust off and reimagine your business continuity plan. And we hope that the new issue of RME offers food for thought and practical ideas as you work to shape your plans and planning processes to ensure readiness for 'what's next.'

Melanie Lockwood Herman is Executive Director of the Nonprofit Risk Management Center. She welcomes your questions about cyber threats and risk management at 703.777.3504 or melanie@nonprofitrisk.org.