Managing Organizational Security

Cybersecurity's technical challenges are manifold, from finding the best cryptographic algorithms to building robust intrusion detection systems. But sometimes, as we play with our security techniques and toys, we forget that the technology is embedded in the larger context of creating and managing secure organizations—organizations that function as a combination of interacting parts. As with software, in which the bulk of problems arise in the interfaces, it's in the combination and interaction that the most significant challenges occur. Moreover, cybersecurity is a complex problem, particularly for businesses operating from multiple locations, or whose financial well-being depends as much on the steady, controlled flow of electricity into their computer systems as it does on the secure, controlled flows of sensitive data among those computers. Security breakdowns extend beyond data leaks, losses, or thefts; instead, they threaten the business itself, adversely affecting reputation, brand, commercial dealings, and, most significant, the company's long-term corporate transactions. Effective cybersecurity will remain elusive if viewed in isolation from these larger concerns.

In short, "it's not just about the technology, stupid." It's also about creating an organizational atmosphere that views security with an appreciation and attentiveness that encourages responsible behavior throughout the enterprise. Such attitudes emerge only when cybersecurity is considered in the context of the legal and business constraints on the technology and how it's used. Without the larger organizational context, even the best technologies can be unused, underused, or misused.

In this special issue, we focus on the challenges of managing organizational security, examining some of the nontechnical aspects of security that assure that the technology is chosen, implemented, and used appropriately and well.

What are the most effective structures?

We begin with an article by M. Eric Johnson and Eric Goetz that summarizes the findings of a workshop for chief information security officers, sponsored by the US Department of Homeland Security's Science and Technology Directorate and Dartmouth College's Institute for Information Infrastructure Protection (I3P). The workshop encouraged CISOs of major corporations to speak candidly about their cybersecurity needs. The general sense of the participants was that they understood cybersecurity, but are looking to the research and development community for more tools, techniques, and measurements to assist them in decision making—especially when the decisions involve trade-offs among constrained resources, some of which aren't related to cybersecurity. For example, what information can help a chief executive officer choose between improving her company's cybersecurity, buying a start-up with an appealing product, or issuing a dividend to shareholders? How can a CEO know how much more security he or she is buying for a given amount of money? How much security is enough? Johnson and Goetz argue that middle management is the weakest link in the decision-making process.

How does security fit into a company's business model?

In the past, practitioners and busi-

Shari Lawrence Pfleeger
RAND Corp.

Roland L. Trope
Trope and Schramm LLP

Charles C. Palmer
IBM Research

More about managing organizational security

Although this emerging topic is most often discussed in manuscripts, the following offer other sources of information:

Books

Christopher Alberts and Audrey Dorofee, *Managing Information Security Risks: The Octave Approach*, Addison-Wesley, 2003.

Roland L. Trope et al., *Checkpoints in Cyberspace: Best Practices to Avert Liability in Cross-Border Transactions*, American Bar Assoc., 2006.

Harold F. Tipton and Micki Krause, *Information Security Management Handbook*, 6th ed., Auerbach, 2007.

Charles Pfleeger and Shari L. Pfleeger, *Security in Computing*, 4th ed., Prentice Hall, 2007.

Mark Ackerman and Don David, "Privacy and Security in the New Economy," *New Economy Handbook*, D.C. Jones, ed., Elsevier, 2003.

Conferences

The International Telecommunication Union (www.itu.int/ITU-D/e-strategies/e-security/) runs workshops for 128 countries to share information and best practices in security and trust technologies and policies for e-business. It has also organized workshops and seminars addressing technology strategies for e-security in several countries.

The US National Institute For Technology and Standards (NIST), Small Business Administration (SBA), Federal Bureau of Investigation (FBI), InfraGuard, Multi-State ISAC, and the National Cyber Security Alliance have collaborated to build a "Cyber Security Is Good Business" online workshop series. This nontechnical "how to" guide to securing critical information from thieves and hackers outlines a model for developing and implementing a security policy that fits each business. Find it at www.staysafeonline.org/basics/cybersecurityisgoodbusinessvideo.html.

October is national cybersecurity awareness month. The US Department of Homeland Security, as well as state and local governments, hosts special programs and workshops for citizens and businesses (www.dhs.gov/xprevprot/programs/gc_1158611596104.shtm).

Web resources

OCTAVE: CERT's organizational security evaluation methodology, www.cert.org/octave/

NIST's federal agency security practices Web site, http://csrc.nist.gov/fasp/index.html

ness officials have been loathe to reveal their experiences, attitudes, and practices to researchers for fear of losing customer trust or competitive advantage. Surveys and studies have presented information that's too general to be useful or selected in such a way that it's impossible to tell to whom the findings apply. In our second article, Shari Lawrence Pfleeger, Martin Libicki, and Michael Webber add rigor to the current research by taking a more disciplined approach to soliciting information. By interviewing (and protecting the identities of) six CISOs from the "Internet supply chain," they elicited in-depth information about attitudes toward cybersecurity in the larger context of how companies do business. Their analysis suggests that a company is likely to take one of three well-defined but very different strategic attitudes toward security. A company's preference for one of those strategic attitudes reflects its belief in its competitive advantages, but also brings with it certain weaknesses that its security management must anticipate and address. The authors suggest several hypotheses that future research can test across other business sectors.

What role should boards of directors play?

In our third article, Roland L. Trope, E. Michael Power, Vincent I. Polley, and Bradford C. Morley observe that the chief cybersecurity challenge derives from multiple security regimes existing within a company, each designed to comply with regulations that apply to a particular business sector or class of commercial activities. The result is that none address the interrelationship of the parts or encourage companies to harmonize compliance programs into single comprehensive data governance programs. As such, when two companies negotiate a merger, an often-overlooked risk is that the resulting venture will not only take years to integrate, but during that time it might have a substantially lower level of cybersecurity than existed at each company prior to the transaction. The authors advance the view that, in the digital era, any legal requirement for secure data management should be treated as part of an enterprise's overall data governance, and that legal compliance, organizational security, and good corporate governance are interdependent.

How do we address new attitudes toward security?

Online social networks are among the many emerging constructs that introduce new and potentially severe security risks to business, consumer, government, and academic environments. For this reason, we invited David Rosenblum, a Harvard undergraduate, to write about a young person's perspective on cybersecurity risks and how they derive, in part, from the diminished privacy of communications on such sites. His descriptions provide

insights into the customs that young adults will be bringing to the organizations that will soon employ them. Rosenblum's invited article also provides a perceptive account of what motivates the behavior observed in online social networks and of the long-term security risks young adults face because of the duration of expression and ease of searching for it on the Internet. These prospective employees' over-the-top behavior and diminished respect for privacy online might eventually taper down, but they could also shift to taking user-generated content into the workplace and using events and information from the workplace for online social networking. His article suggests that companies must consider how they'll manage the opportunities and risks of online social networks and other new constructs. Whether the new practices will clash or can be harmonized with older practices remains to be seen.

Can we really transfer security risk?

As technologists, we often assume that our role is to reduce risk by preventing attacks or at least mitigating their effects. But in a business setting, there is often a third choice: transferring the risk to someone or something else. In other domains, insurance companies rely on a substantial body of credible actuarial data on which to base projections and premiums. However, in cybersecurity, reliable data are hard to come by. Transferring the risk depends on organizations' willingness to chance releasing information about the magnitude, frequency, and nature of cyberattacks. In our final article, Walter S. Baer and Andrew Parkinson explore the possibilities of using insurance policies to transfer cybersecurity risks.

Our first three articles assess the current situation, raising issues and setting hypotheses to be explored in later studies. The final two look forward, at what's likely to happen in the future. All five examine cybersecurity through a multidisciplinary lens, using techniques from management and social science to help us understand how to improve cybersecurity choices and outcomes. The sidebar contains pointers to organizations, publications, and conferences where you can learn more. ▢

Shari Lawrence Pfleeger *is a senior information scientist at RAND Corp. Her technical interests include empirical software engineering, cybersecurity, and technology transfer. Pfleeger has a PhD in information technology and engineering from George Mason University. She is a member of the ACM and a senior member of the IEEE and the IEEE Computer Society. Contact her at shari_pfleeger@rand.org.*

Roland L. Trope *is a partner in Trope and Schramm LLP and an adjunct professor in the Department of Law at the US Military Academy. He has a BA in political science from the University of Southern California, a BA and MA in English language and literature from Oxford University, and a JD from Yale Law School. Trope coauthored the treatise* Checkpoints in Cyberspace: Best Practices for Averting Liability in Cross-Border Transactions *(American Bar Association, 2006). Contact him at roland.trope@verizon.net.*

Charles C. Palmer *is CTO of security and privacy at IBM Research and the director of research for the Institute for Information Infrastructure Protection (I3P). His technical interests vary widely, including cybersecurity, security engineering and usable security, and privacy. He has a PhD in computer science from Polytechnic University, New York. He is an ACM Distinguished Engineer and a member of the IEEE. Contact him at ccpalmer@thei3p.org.*