Cyberinsurance in IT Security Management

Cyberinsurance to cover losses and liabilities from network or information security breaches can provide incentives for security investments that reduce risk. Although cyberinsurance has evolved, industry has been slow to adopt it as a risk management tool.

WALTER S. BAER
Annenberg Center for Communication

ANDREW PARKINSON
RAND Europe

Individuals, businesses, and other organizations routinely use insurance to help manage risks. They buy insurance policies to cover potential losses from property damage, theft, and liability that they can't or don't want to bear alone. Insurance carriers' offerings have evolved to address increased demand (such as directors' and officers' liability), new perils (such as loss of intellectual property), and previously uncovered risks (such as college students' property losses).

This article discusses the emergence of cyberinsurance to address growing risks and vulnerabilities from our increased dependence on computer systems, the Internet, and other networked information technology. The steadily rising number of virus attacks, hacker assaults, and other IT security incidents are well documented and bring new urgency to efforts to strengthen IT security at every level.

IT security has traditionally referred to technical protective measures such as firewalls, authentication systems, and antivirus software to counter such attacks, and mitigation measures such as backup hardware and software systems to reduce losses should a security breach occur. In a networked IT environment, however, the economic incentives to invest in protective security measures can be perverse. My investments in IT security might do me little good if other systems connected to me remain insecure because an adversary can use any unprotected system to launch an attack on others. In economic terms, the private benefits of investment are less than the social benefits, making networked IT security a public good—and susceptible to the free-rider problem. As a consequence, private individuals and organizations won't invest sufficiently in IT security to provide an optimal (or even adequate) level of societal protection.

Benefits of cyberinsurance

In other areas, such as fire protection, insurance has helped align private incentives with the overall public good. A building owner must have fire insurance to obtain a mortgage or a commercial business license. Obtaining insurance requires that the building meet local fire codes and underwriting standards, which can involve visits from local government and insurance company inspectors. Insurance investigators also follow up on serious incidents and claims, both to learn what went wrong and to guard against possible insurance abuses such as arson or fraud. Insurance companies often sponsor research, offer training, and develop best-practice standards for fire prevention and mitigation. Most important, insurers offer lower premiums to building owners who keep their facilities clean, install sprinklers, test their control systems regularly, and take other protective measures. Fire insurance markets thus involve not only underwriters, agents, and clients, but also code writers, inspectors, and vendors of products and services for fire prevention and protection. Although government remains involved, well-functioning markets for fire insurance keep the responsibility for and cost of preventive and protective measures largely within the private sector.

As with fire insurance, the prospective benefits of well-functioning markets for cyberinsurance can accrue to stakeholders both individually and collectively. They include

- a focus on market-based risk management for informa-

tion security, with a mechanism for spreading risk among participating stakeholders;
- greater incentives for private investments in information security that reduce risk not only for the investing organization but also for the network as a whole;
- better alignment of private and public benefits from security investments;
- better quantitative tools and metrics for assessing security;
- data aggregation and promulgation of best practices; and
- development of a robust institutional infrastructure that supports information security management.

Thus cyberinsurance can, in principle, be an important risk-management tool for strengthening IT security and reliability, both for individual stakeholders and for society at large.

But are these prospective benefits realistic and achievable? Is it likely, as security expert Bruce Schneier expects, that

> "[T]he insurance industry [is] going to move into cyberinsurance in a big way. And when they do, they're going to drive the computer-security industry…just like they drive the security industry in the brick-and-mortar world"?[1]

Evolution, trends, and current status

Before the late 1990s, little commercial demand existed for property or liability insurance specifically covering losses from network security breaches or other IT-related problems. However, the rapid growth of e-commerce, followed by distributed denial-of-service (DDoS) attacks that took down several leading commercial Web sites in February 2000, kindled significant interest in such coverage. The Y2K computer problem, although ultimately resulting in little direct damage or loss, brought further attention to cyberrisk issues and pointed out the limitations of existing insurance coverage for IT failures.

Potential liability from IT security breaches has increased as a result of such federal legislation as the Health Insurance Portability and Accountability Act and the Graham-Leach-Bliley Act, which mandate protection of sensitive personal medical and financial records. California also passed a Security Breach Information Act (www.securitymanagement.com/library/SB1386_ca0203.pdf) requiring prompt public disclosure of any breach that might have compromised computer-based personal information about a California resident. This California law, which went into effect in July 2003, essentially sets a national requirement for any business or other organization that maintains a database with identifiable individual records.

Starting around 1998, a few insurance companies developed specialized policies covering losses from computer viruses or other malicious code, destruction or theft of data, business interruption, denial of service, and/or liability resulting from e-commerce or other networked IT failures. Coverage was spotty and limited, but premiums were high. Moreover, numerous legal disputes arose over whether such losses could come under general commercial property or liability policies that were written to cover direct physical damage to tangible assets.[2–4]

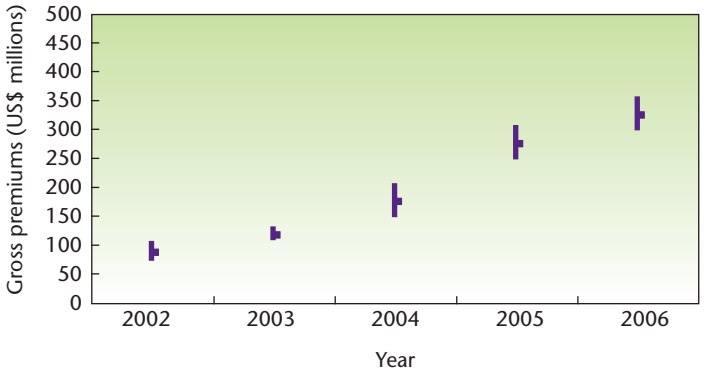

Figure 1. Cyberinsurance market growth. (SOURCE: BETTERLEY MARKET SURVEYS, 2002–2006; USED WITH PERMISSION.)

By 2002, in response to the legal uncertainties, insurers had written specific exclusionary language into their commercial property and liability policies to exclude coverage of "electronic data," "computer code," and similar terms as tangible property. As David O'Neill, vice president for e-business solutions at Zurich North America, stated: "Computer code is deemed to be intangible […] Property and casualty policies were never written to assess these exposures and were never priced to include them."[5] Two Appeals Court rulings in 2003 affirmed that data aren't considered tangible property under general property or liability coverage (*Ward General Insurance Services v. Employers First Insurance*, 2003; http://fsnews.findlaw.com/cases/ca/caapp4th/slip/2003/g031624.html; and *AOL v. St. Paul Mercury Insurance*, 2003; http://pacer.ca4.uscourts.gov/opinion.pdf/022018.P.pdf).

As a consequence, businesses now generally buy stand-alone, specialized policies to cover cyberrisks. According to Betterley Risk Consultants surveys, the annual gross premium revenue for cyberinsurance policies has grown from less than US$100 million in 2002 to US$300 to 350 million by mid 2006 (see Figure 1).[6] These estimates, which are based on confidential survey responses from companies offering cyberinsurance, are nearly an order of magnitude below earlier projections made by market researchers and industry groups such as the Insurance Information Institute. But Betterley, like many other industry experts, believes that cyberinsurance will be one of the fastest growing segments of the

Table 1. Coverage offered by major cyberinsurance carriers.

	INSURANCE CARRIER					
COVERAGE	**ACE**	**AIG**	**CHUBB**	**CNA**	**ST. PAUL TRAVELERS**	**ZURICH**
PROPERTY AND THEFT						
Maximum limit (US$ millions)	15	25[a]	25	10[b]	N/A[c]	7.5
Destruction of data or software	✓	✓	✓	✓	✓[c]	✓
Recovery from viruses or other malicious code		✓	✓	✓	✓[c]	✓
Business interruption	✓	✓	✓	✓	✓[c]	✓
Denial of service	✓	✓	✓	✓		✓
Data theft		✓	✓	✓		✓
Cyberextortion	✓	✓	✓	✓		✓
Losses due to terrorist acts	✓	✓	✓	✓	✓[c]	✓
LIABILITY						
Maximum limit (US$ millions)	25	25[a]	50	10[b]	25	7.5
Network security liability	✓	✓	✓	✓	✓	✓
Content/electronic media injury	✓	✓	✓	✓	✓	✓
Privacy/breach of confidentiality liability	✓	✓	✓	✓	✓	✓

The company (a) will assist in placing higher limits up to US$75 million, (b) offers limits up to US$20 million on a highly selected basis, (c) offers some first-party cybercoverage as part of traditional property policies, not as specialized policies. (SOURCE: *THE BETTERLEY REPORT*, JUNE 2006.[6])

property and casualty market over the next several years. With only 25 percent of respondents to the most recent Computer Security Institute/US Federal Bureau of Investigation Computer Crime and Security survey reporting that, "their organizations use external insurance to help manage cybersecurity risks,"[7] the market has plenty of room for growth.

Current policies and markets

Over the past five years, the cyberinsurance market has both broadened and differentiated. Underwriters include both large insurance companies and several smaller, more specialized firms. A few carriers, such as Media/Professional, sell only liability policies, but most now offer a combination of property, theft, and liability coverage (see Table 1). Increasingly, cyberinsurance products are designed for specific markets—for example, AIG and Chubb have policies tailored for financial service organizations.

All carriers now offer coverage of losses due to foreign-based, government-certified acts of terrorism as per the Terrorism Risk Insurance Act of 2002 (the TRIA has been extended through December 2007; see www.ustreas.gov/offices/domestic-finance/financial-institution/terrorism-insurance/pdf/hr3210.pdf), and some provide additional endorsements for domestic-based and other noncertified terrorist acts. Policy limits have increased somewhat since 2002 as underwriters have gained experience with insuring cyberrisks. Still, the upper limits of US$25 million shown in Table 1 for *first-party coverage* (that is, policies covering the insured's property losses, as opposed to those covering liability, or *third-party coverage*) might appear quite low to large organizations, particularly for possible catastrophic losses from a highly coordinated cyberattacks.

Both carriers and customers have become more sophisticated in dealing with security assessments before obtaining cyberinsurance coverage. Carriers require audits by independent IT security consultants on a case-by-case basis, depending on the risks to be covered and the policy limits sought. AIG, the largest cyberinsurance underwriter, first asks prospective clients to complete an "Information Security Self Assessment" that applicants can download from its Web site (www.aignationalunion.com/nationalunion/public/natproductdetail/0,2128,448-13-2995,00.html) and return via email. The AIG self-assessment covers such items as

- standard configurations with security documentation for firewalls, routers, and operating systems;
- information security policies, including password management, virus protection, encryption, and security training for employees;
- vulnerability monitoring and patch management;
- physical security and access controls, including remote access;
- privacy and confidentiality policies;

- backup and restoration provisions;
- business continuity planning;
- periodic testing of security controls; and
- outsourcing and other third-party security provisions.

Based on the results of such self-assessments, underwriters will determine whether they require an onsite audit to bind coverage. Nearly all insurers also provide cyberrisk-management services to help clients identify exposures and take loss prevention and mitigation measures.

Although policy language about what is insured and what perils and risks are covered has become more standardized, cyberinsurance policies are still largely written and priced to match individual client practices and exposures. Consequently, there are no published standard rates as state insurance regulators would require for standard products. According to industry insiders, rates have generally decreased over the past two years, but they continue to be set on a customer-by-customer basis and can vary considerably based on the results of IT security assessments and audits.

Barriers to cyberinsurance expansion

The reported 25 percent cyberinsurance adoption rate[7] appears low to many observers, given well-publicized increases in IT security breaches and greater regulatory pressures to deal with them.[8] Although we could partially attribute the slow uptake to how long it takes organizations to acknowledge new security risks and budget for them, several other factors seem to be of particular concern for cyberinsurance. They include problems of asymmetric information, interdependent and correlated risks, and inadequate reinsurance capacity.

Asymmetric information

The insurance industry has studied the asymmetric information problem (in which different parties have differing access to information) extensively, and the conclusions that hold for more established insurance markets also apply to cyberinsurance.

Insurance companies feel the effect of asymmetric information both before and after a customer signs an insurance contract. They face the adverse selection problem—that is, a customer who has a higher risk of incurring a loss (through risky behaviors or other—perhaps innate—factors) will find insurance at a given premium more attractive than a lower-risk customer. If the insurer can't differentiate between them—and offer differentiated premiums—it won't be able to sustain a profitable business.

Of course, to some extent, insurance companies can differentiate between risk types; sophisticated models can predict risk for traditional property/casualty insurance, and health insurance providers try to identify risk factors through questionnaires and medical examinations. Insurers can also apply these mechanisms to cyberinsurance: they can undertake rigorous security assessments, examining in-depth IT deployment and security processes.[9] Although such methods can reduce the asymmetric information between insurer and policyholder, they can never completely eliminate it. Particularly in the information security field, because risk depends on many factors, including technical and human factors and their interaction, surveys can't perfectly quantify risk, and premium differentiation will be imperfect.

The second impact of asymmetric information occurs after an insurance contract has been signed. Insured parties can take (hidden) actions that increase or decrease the risk of claiming (for example, in the case of car insurance, driving carelessly, not wearing a seatbelt, or failing to properly maintain the car), but the insurer can't observe the insured's actions perfectly. Under full insurance, an individual has little incentive to undertake precautionary measures because any loss is fully compensated—a problem economists term *moral hazard*.

Insurers may be able to mitigate certain actions through partial insurance (so making a claim carries a monetary or convenience cost) and clauses in the insurance contract—for example, policyholders must usually meet a set standard of care, and fraudulent or other criminal actions (such as arson) are prohibited. However, many actions remain unobservable, and it's difficult to prove that a client didn't meet a due standard of care. Cyberinsurers could administer surveys at regular intervals and link coverage to a certain minimum standard of security. Although this might be feasible from a technical standpoint, human factors are often the weakest link in the chain and possibly unobservable, so the moral hazard problem might not be completely alleviated, implying that the purchase of cyberinsurance could in fact reduce efforts on information security. Nevertheless, purchasers also have incentives to increase effort—that is, to invest in security to obtain insurance or reduce premiums—that would outweigh moral hazard effects in a viable and well-functioning market.

The problem of asymmetric information is common to all insurance markets; however, most markets function adequately given the range of tactics used by insurance companies to overcome these information asymmetries. Many of these remedies have developed over time in response to experience and result in the well-functioning insurance markets we see today.

Interdependent and correlated risks

To face a steady claim stream and avoid large spikes in payouts, insurers must maintain a sufficiently large policyholder base and insure risks that are relatively independent and uncorrelated. However, in the case of cyberinsurance, risks might be correlated and interdependent. A monoculture in installed systems can make

most systems vulnerable to the same event.[10] (For various reasons, the structures in certain software markets tend to result in one dominant product,[11] and thus a monoculture in installed systems—for example, the Microsoft Windows operating system.) Furthermore, risk can be interdependent: one compromised system can impact the risk to other systems.[12] Both characteristics are apparent in the case of worm attacks, which exploit vulnerabilities in widely installed software (generally Microsoft Windows or Microsoft Outlook) and propagate from compromised systems. Worms can infect a significant number of systems within a short period of time. For example, the Mydoom worm infected more than one million computers within six days of being identified, and at its peak was responsible for 20 to 30 percent of worldwide email traffic.

Despite several obstacles, cyberinsurance is moving into the mainstream as a tool for managing IT security risks.

Events that are likely to result in concurrent claims from a substantial proportion of policyholders—such as virus or worm attacks, or coordinated cyberattacks such as DDoS attacks—impose a high "probability of ruin" on a cyberinsurer. Initial academic studies have shown that interdependency and correlation of risk could pose major hurdles to a cyberinsurance market's effective functioning;[13–15] obtaining reliable estimates of loss correlation is key to our future understanding of this problem's scale.

Inadequate reinsurance capacity

In other insurance markets, insurers also face events that prompt many claims at once, such as large natural disasters. In these situations, primary underwriters can limit their total exposure while still writing large individual policies and insuring many parties that might be affected by the same event by passing some of their risk to well-capitalized reinsurers. Reinsurance is essentially insurance purchased by insurance companies. Global reinsurance capacity is estimated at US$400 billion, and reinsurance covered nearly half of the US$83 billion in insured property losses in 2005 (losses of US$38 billion from Hurricane Katrina alone).[16] Reinsurers use loss data spanning several years to set premiums and diversify risks geographically as well as by peril so that they can survive even major catastrophes like Katrina.

Geographically diversifying or even quantifying cyberrisks seems more problematic, however, because cyberattacks might be globally correlated and interdependent. The paucity of prior claims data coupled with the plausibility of simultaneous attacks worldwide make reinsurers reluctant to provide catastrophe protection for business interruption or related cyberlosses that some think could reach US$100 billion (see http://mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//mi2g.com/cgi/mi2g/press/160204.php). Harrison Oellrich, managing director at Guy Carpenter & Co., calls it the "Cyber Hurricane" problem:[17]

> "Insurers and reinsurers have spent a tremendous amount of time and resources over the last decade in an effort to quantify, through the use of sophisticated probabilistic and deterministic modeling, the actual expected losses to any existing or theoretical portfolio of risks and in just about any real or hypothetical loss scenario, be it an earthquake, windstorm, or other physical peril. Having convinced themselves that they can thus construct a portfolio of business from which they can expect an acceptable exposure to catastrophic loss from any one of these natural perils, along come these new Internet exposures. The Internet is very unique in that on the surface at least, it does not look to be able to be modeled in this way. Whereas natural perils losses occur in a specific geographical location, the Internet is both everywhere and nowhere at the same time, while the perils to be protected are still being fully identified and defined."

Reinsurers are also securitizing risks from low-frequency, high-impact events such as hurricanes and earthquakes by selling special-purpose catastrophe bonds to investors that can be traded on securities markets. Catastrophe bonds pay high rates of interest, but the investor stands to lose interest payments and sometimes principal if insurance losses from the disaster exceed a specified amount. Catastrophe bonds represent a growing part of the reinsurance market and are being issued to cover perils beyond natural disasters, but they haven't yet been used to reinsure cyberrisks.

The practical consequences of correlated and interdependent risks are seen in limited reinsurance capacity, which makes it difficult for large firms to obtain cyberinsurance policy limits greater than those set out in Table 1. For Fortune 500 companies, an underwriter's US$25-million limit for coverage of direct, first-party losses simply isn't enough to make cyberinsurance an important factor in managing IT security.

Future directions

Despite these obstacles, cyberinsurance is moving into the mainstream as a tool for managing IT security risks. Demand for both liability and first-party coverage is rising,

and the insurance industry is responding by cautiously increasing its capacity to underwrite cyberpolicies. In time, insurers will be able to aggregate information from policyholders and claim records to create a better information base—thereby enabling them to further broaden coverage, expand policy limits, and better differentiate premiums by known risk factors. Oellrich compares cyberinsurance development to the way the market for insuring environmental risks has played out:[5]

> "The initial forms and exposures were very similar in that there [were] no data to underpin the rates […] People began by putting a very restrictive policy form with high pricing on the market; and over time, as they began to develop experience, they were able to broaden policy forms and modify the pricing significantly."

Differentiating premiums by security measures deployed also gives a metric of the measures' *value*—that is, the reduction in expected loss as a consequence of installing the measure as opposed to the measure's monetary cost[13]—which lets you apply standard tools (such as cost-benefit analysis) more accurately to evaluate IT security investments. Consequently, we'd expect to see insurance underwriters working with security hardware and software vendors to evaluate and recommend adoption of products and services that can make networked IT systems more secure.

Cyberinsurance is an intensely complicated topic, however, and we're still far from having a mature, well-functioning market for cyberinsurance that would help align incentives for private investments in IT security. Because of the many public-good aspects and other possible market failures surrounding network security, it seems appropriate to consider possible ways in which public policies or actions could facilitate private market development (even though government involvement inevitably affects market dynamics and results in costs as well as benefits).

For example, the 2003 *National Strategy to Secure Cyberspace* (NSSC)[18] called for greater government–industry collaboration in sharing information about IT security threats and vulnerabilities, and encouraged firms to participate in industry-specific information sharing and analysis centers (ISACs) that had been authorized under Presidential Decision Directive 63 in 1998. Insurance companies are active members of the financial services ISAC (www.FSISAC.com). However, it isn't clear that the FS/ISAC has improved underwriters' abilities to aggregate cyberrisk or loss data, or that other recommendations from the NSSC have had much effect on cyberinsurance industry practices—at least as yet. (The US Department of Justice's Bureau of Justice Statistics and the Department of Homeland Security's National Cyber Security Division are sponsoring a national computer security survey to provide better quantitative data about cyberrisks and losses. The NSSC is intended to be an annual or biannual data-collection effort providing valuable information to insurers and risk managers. For additional information, see www.ncss.rand.org.)

Other government actions to spur development of the cyberinsurance market could include assigning liability for IT security breaches, mandating incident reporting, mandating cyberinsurance or financial responsibility, or facilitating reinsurance by indemnifying catastrophic losses. Clarifying liability law to assign liability "to the party that can do the best job of managing risk"[19] would make good economic sense, but it seems a political nonstarter in the US—and the problem's global nature would require a global response. Similarly, government regulations that mandate reporting of cyberincidents (similar to that required for civil aviation incidents and contagious disease exposures) appear to have little political support. Probably more plausible in the short run would be contractual requirements that government contractors carry cyberliability insurance on projects highly dependent on IT security.

Jane Winn of the University of Washington School of Law has proposed a self-regulatory strategy, based on voluntary disclosures of compliance with security standards and enforcement through existing trade practices law, as a politically more viable alternative than new government regulation.[20] Such a strategy would require increased public awareness of cybersecurity (with possible roles for government) as well as public demand that organizations disclose whether they comply with technical standards or industry best practices. Disclosures would be monitored for compliance by their customers and competitors; and in the case of deceptive advertising, the US Federal Trade Commission could take enforcement action under existing regulation. This strategy could spur cyberinsurance adoption, which would indicate that the organization has passed a security audit or otherwise met underwriters' security standards.

Perhaps the most important role for government would be to facilitate a full and deep cyberreinsurance market, as the UK and US have done for reinsurance of losses due to acts of terrorism. When IRA terrorist attacks in London in the early 1990s threatened to make property insurance unavailable to commercial building owners, the UK government worked with insurers to maintain property damage and business interruption coverage. Pool Re was established under the Reinsurance (Acts of Terrorism) Act of 1993 as a mutual reinsurance company owned by the insurers and backed by the UK Treasury as a reinsurer of last resort. Similarly, after September 11, 2001, the US Congress passed the TRIA, providing a federal backstop to effectively limit insurers' losses from major terrorist acts. Both Pool Re and TRIA

have successfully stimulated development of private markets for terrorism reinsurance, and thus might serve as models for overcoming the reinsurance barrier to cyberinsurance expansion. However, such interventions are more typically reactive than proactive, so government efforts to facilitate cyberreinsurance might not occur unless prompted by a major cybercatastrophe.

Cyberinsurance market development has thus far been tentative, and, given the fact that government interventions that would catalyze the market are unlikely in the foreseeable future, further development will probably remain slow. However, experience should gradually enable insurers to overcome (or at least better cope with) the barriers to a full and efficient market. With greater experience, coverage of cyberrisks will likely become more fully integrated with other property and liability coverage. Over time, cyberinsurance might become as important and as ubiquitous in the IT security toolbox as are firewalls and antivirus software. □

References

1. B. Schneier, "Computer Security: It's the Economics, Stupid," *Workshop on the Economics of Information Security* (WEIS), 2002; www2.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/18.doc.
2. W.S. Baer, "Rewarding IT Security in the Marketplace," *Proc. 31st Research Conf. Comm., Information, and Internet Policy,* 2003; http://intel.si.umich.edu/tprc/papers/2003/190/BaerITSecurity.pdf.
3. J. Kesan et al., "The Economic Case for Cyberinsurance," Univ. of Ill. Law and Economics working paper no. 2, July 2004; http://law.bepress.com/uiuclwps/papers/art2/.
4. J. Kesan et al., "Cyber-Insurance as a Market-Based Solution to the Problem of Cybersecurity," *Workshop on the Economics of Information Security* (WEIS), 2005; http://infosecon.net/workshop/pdf/42.pdf.
5. D. Duffy, "Safety at a Premium," *CSO*, Dec. 2002; www.csoonline.com/read/120902/safety.html.
6. R.S. Betterley, "CyberRisk Market Survey 2006," *The Betterley Report*, June 2006; www.betterley.com/products.html.
7. L. Gordon et al., *2005 CSI/FBI Computer Crime and Security Survey*, Computer Security Inst., 2005; www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf.
8. *Global Information Security Survey 2005*, Ernst & Young, Nov. 2005; www.ey.com/global/download.nsf/International/Global_Information_Security_Survey_2005/$file/EY_Global_Information_Security_survey_2005.pdf.
9. R.P. Majuca, W. Yurcik, and J.P. Kesan, "The Evolution of Cyberinsurance," *ACM Computing Research Repository* (CoRR), tech. report cs.CR/0601020, Jan. 2006; www.projects.ncassr.org/econsec/cyberinsuranceTR06.pdf.
10. D. Geer, *Cyber Insecurity: The Cost of Monopoly*, Computer and Comm. Industry Assoc., 2003; www.ccianet.org/papers/cyberinsecurity.pdf.
11. R. Anderson, "Why Information Security Is Hard—An Economic Perspective," Univ. of Cambridge Computer Laboratory working paper, 2001; www.ftp.cl.cam.ac.uk/ftp/users/rja14/econ.pdf.
12. H. Kunreuther and G. Heal, "Interdependent Security: The Case of Identical Agents," working paper no. 8871, Nat'l Bureau of Economic Research, 2002.
13. R. Böhme, "Cyber-Insurance Revisited," *Workshop on the Economics of Information Security* (WEIS), 2005; http://infosecon.net/workshop/pdf/15.pdf.
14. R. Böhme and G. Kataria, "Models and Measures for Correlation in Cyber-Insurance," *Workshop on the Economics of Information Security* (WEIS), 2006; http://weis2006.econinfosec.org/docs/16.pdf.
15. H. Ogut, N. Menon, and S. Raghunathan, "Cyber Insurance and IT Security Investment: Impact of Interdependent Risk," *Workshop on the Economics of Information Security* (WEIS), 2005; http://infosecon.net/workshop/pdf/56.pdf.
16. G. Carpenter, "The World Catastrophe Reinsurance Market," Guy Carpenter & Co., Aug. 2006; www.guycarp.com/portal/extranet/insights/reports.html?vid=22.
17. H. Oellrich, "Cyber Insurance Update," *The CIP Report*, Dec. 2003; http://cipp.gmu.edu/archive/cip_report_2.6.
18. US Dept. of Homeland Security, *The Nat'l Strategy to Secure Cyberspace*, Feb. 2003; www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.
19. H.R. Varian, "Liability for Net Vandalism Should Rest with Those That Can Best Manage the Risk," *The New York Times*, 1 June 2000, section C, p. 2; www.ischool.berkeley.edu/~hal/people/hal/NYTimes/2000-06-01.html.
20. J. Winn, "Should Vulnerability Be Actionable? Improving Critical Infrastructure Computer Security with Trade Practices Law," *George Mason Univ. Critical Infrastructure Protection Project Papers Vol. II*, 2004; www.law.washington.edu/Faculty/Winn/Publications/Should_Vulnerability.pdf.

Walter S. Baer *is a senior fellow at the Annenberg Center for Communication at the University of Southern California. His research interests include the evolution of networked media and ways to better align public- and private-sector incentives in telecommunications, information technology, and energy. Baer is a Fellow of the American Association for the Advancement of Science and has served on the Electric Power Research Institute (EPRI) advisory council, the Governor's Council on Information Technology for the state of California, and the external advisory board of the UCLA Center for Embedded Network Sensing. He has a PhD in physics from the University of Wisconsin. Contact him at wsbaer@yahoo.com.*

Andrew Parkinson *is a research assistant at RAND Europe. His research interests include the economics of information security and the economics of privacy. He has a BA Hons in economics from the University of Cambridge. Contact him at andy.parkinson@cantab.net.*