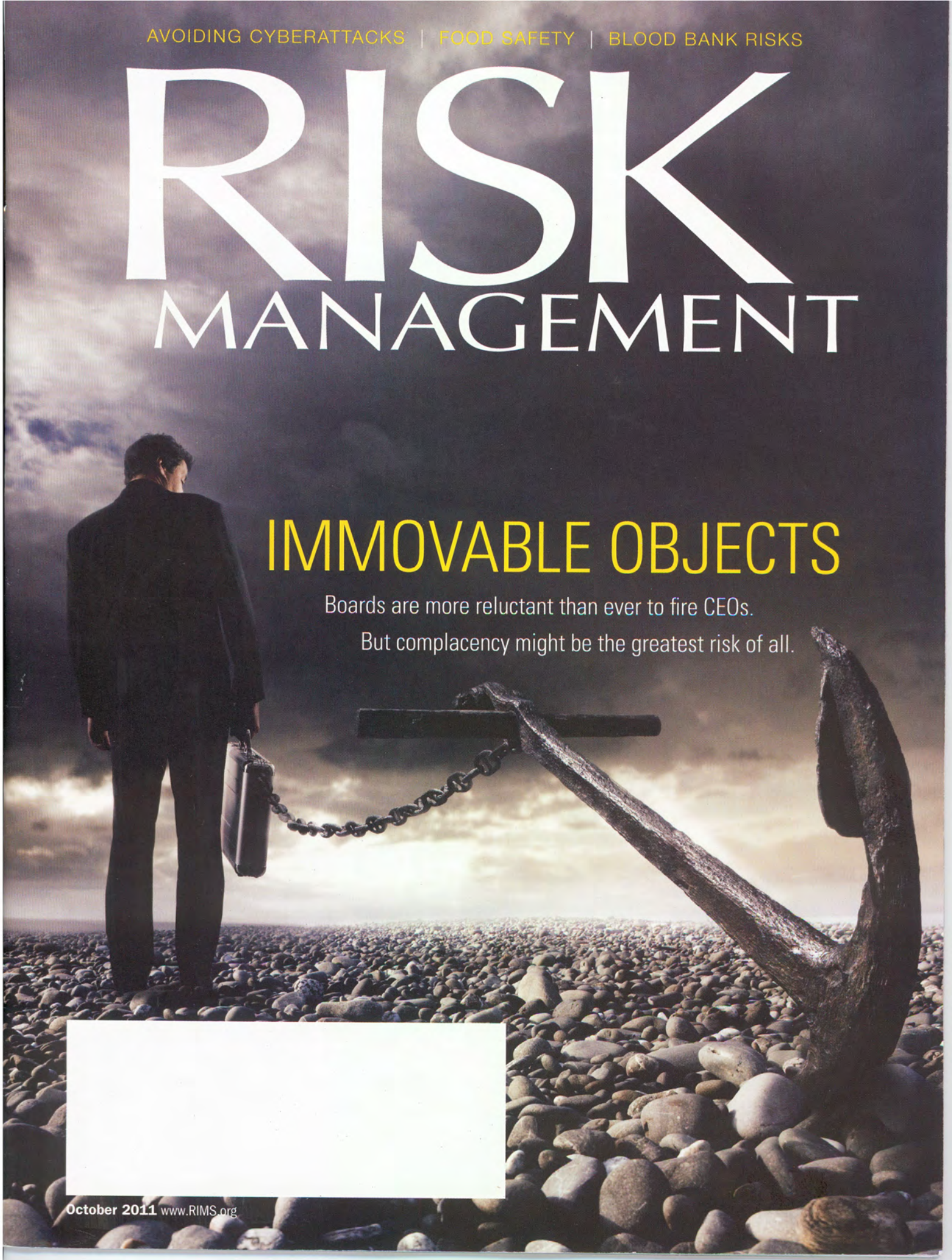
AVOIDING CYBERATTACKS | FOOD SAFETY | BLOOD BANK RISKS

# RISK MANAGEMENT



## IMMOVABLE OBJECTS

Boards are more reluctant than ever to fire CEOs.
But complacency might be the greatest risk of all.

# The Coverage Question

BY GREGG A. RAPOPORT AND DAVID LAM

## YOUR GUIDE TO SELECTING CYBER-INSURANCE

As they confront the sobering question of whether their networks and the data they carry are fully secure, today's "C-level" executives are becoming fluent in once-esoteric information security terms. Many have reached the conclusion that no matter the size of their IT and security budgets, there is no foolproof system for securing the confidentiality, integrity and availability of their data. Company networks remain vulnerable to attacks even if they adhere to industry best practices and run best-of-breed firewalls.

> Insurance has evolved over the past decade to become a standalone product rather than the assortment of special cyber-endorsements tacked onto traditional policies.

To address these security challenges, companies are relying on their risk managers to evaluate the applicability of existing insurance coverage to data breach incidents, and to assess the value of transferring some of the uncovered financial risk to one of the carriers now offering cyber-risk insurance policies. As the market for these products matures, premiums have come down significantly and policy limits have increased.

Additionally, companies are assessing their contractual relationships with vendors with respect to protecting sensitive data, confirming that the company is fully indemnified and also enjoys the status of an additional insured under a vendor's own insurance.

Cyber-risk insurance goes by various names, most of which include one or more terms such as "data," "cyber," "network" and "privacy." This insurance has evolved over the past decade to become a standalone product rather than the assortment of special cyber-endorsements that had been tacked onto traditional policies covering commercial general liability, employer practices, directors and officers, commercial crime, fidelity bond, professional liability, and errors and omissions.

These endorsements had provided tailored coverage that otherwise may have been excluded, such as losses from "digital asset replacement expense," "electronic data processing hardware and software," "computer and funds transfer fraud," "computer extortion," and "crisis management and public relations," as well as third party losses from "breach of privacy and security," "media liability," and "governmental fines and penalties." The current offerings include some or all of these coverages, but unlike the many traditional policies, are not necessarily built off of standardized ISO forms and are far from interchangeable in terms of both coverage provisions and exclusions.

Litigation involving insurance coverage for data breaches is becoming increasingly prevalent, with a number of courts

**An insured business that tenders a data breach claim against its existing CGL policy could get push-back from its carrier, as Sony recently discovered.**

addressing the reach of various traditional business policies. Clear guidance from the courts is somewhat elusive, however. So before drawing too many conclusions from one or two high-profile examples, it is essential to consider specific policy language and weigh the significance or prior judicial interpretations.

For example, an insured business that tenders a data breach claim against its existing CGL policy could get push-back from its carrier, as Sony recently discovered when it sought coverage against privacy litigation after its PlayStation Network was breached in April and the personal data of approximately 77 million customers was stolen. The typical CGL policy includes complex and debatable definitions of several key terms, as well as potentially ambiguous exclusions relating to electronic data. Commercial crime and E&O policies have also been the subject of coverage disputes arising from data breaches, with varying outcomes and ongoing cases now in the appellate courts.

It is still too early to predict the extent of coverage disputes relating to standalone cyber policies, but risk managers should expect the courts to begin hearing these cases in the near future. In short, great care should be taken before making any assumptions about whether coverage will or will not be found in a given case.

A risk manager thus faces the daunting task of assessing a highly technical set of security risks. He or she must weigh all the potential legal, financial, competitive and reputational consequences, compare those against existing insurance policies and determine if there is a need for specialized coverage. A mistake could devastate the company in the event of a data breach. Additionally, once an appropriate cyber-risk policy is selected, the company may undergo a technical audit by underwriters and may need to invest in additional security measures.

Due to the gravity and complexity of this process, it should involve a series of discussions among members of a team that includes well-informed risk, insurance, legal and information security professionals. Together, this partnership of experts will attempt to place the company's needs somewhere along a spectrum of possible exposures and outcomes.

At one end of the spectrum, no new coverage may be needed. For example, a software maker that already carries "tech E&O" insurance may already be sufficiently insured against the peril of a customer's damage claims for negligence arising from a data breach incident. At the other end, some coverage may be impossible to obtain, such as insurance for punitive damages, which is largely prohibited as a matter of public policy. Most companies face potential outcomes that fall in the middle of the spectrum, where the decision is most complex.

Certain questions can provide a framework for the team to exchange information and reach a consensus on appropriate coverage. Here are 10 that every company should ask:

1. What is the nature of the data that may be compromised in a network security breach incident?
2. What is the scope of the business risk that would arise from an attack on the network that involves the loss of data, the corruption of its integrity or the inability to access that data?
3. What technology controls have we used to mitigate this risk?
4. To what extent will our existing insurance policies cover this exposure?
5. What are the features and limits of cyber-risk policies available to address the residual risk, and how much do they cost?
6. Could we implement additional controls now to qualify for cyber-risk insurance at a lower cost?
7. Are there any additional controls the insurance underwriters would require as a condition for coverage?
8. Are there other steps we can take to reduce exposure to data breaches involving vendors and independent contractors who handle our data?
9. Until the courts address and resolve potential cyber policy coverage issues, what legal uncertainties will we continue to face, and can those be addressed by negotiating endorsements?
10. Whatever our decision today, under what circumstances should we revisit these issues?

By raising and responding to these questions, the management and advisory team will be able to navigate the company's course through this largely uncharted territory and provide critical protection against evolving cyber-risk exposures. ■

---

***Gregg A. Rapoport**, Esq., has represented policyholders in coverage litigation for more than 20 years as part of a broad business litigation practice based in Pasadena, California.*

***David Lam**, CISSP, CPP, is the vice president of the Los Angeles Information Systems Security Association and has more than 20 years of experience as an IT and information security professional and author.*