ORRICK

POLICYHOLDER OBSERVER

MARCH 7, 2012

Into the Data-Security Breach: Risks, Liability, and Insurance Recovery for Companies and their Directors

By Marc S. Mayerson and Darren S. Teshima

At the same time as we begin to emerge from recent financial dislocations and economic turbulence—and as we face continued uncertainty in the Eurozone, election politics, and regional conflicts—businesses face increasing risks from technological failures, cyber-crime, and data-privacy violations.

According to a recent study by Lloyd's of London, cyber-risk—both malicious attacks and non-malicious ones—is approaching the top 10 of risks threatening businesses worldwide; in the U.S. malicious attacks were ranked in the top 5. Last year, hackers succeeded in attacking government networks in the U.S., India and Brazil. Data breach in various forms has struck major financial institutions, pharmaceutical companies, manufacturers, stock exchanges, defense manufacturers, electronics manufacturers, and Internet-based businesses. Stats from a year ago estimated that cyber-crime was costing companies $114 billion, with $96 billion in the U.S. alone.

Against this backdrop, the Securities and Exchange Commission recently provided written guidance for registrants about the need to provide disclosure of the risk of cyber security breaches and companies' plans to mitigate that risk. In CF Disclosure Guidance: Topic No. 2 (October 13, 2011), the SEC directed that the risk of cyber incidents should be disclosed to investors if an incident would make the investment speculative or risky, that is if cyber incidents are reasonably likely to have a material financial impact. If an attack, breach, or failure would lead to reduced revenues, increased cyber security costs, data-breach litigation, or the like, registrants may be required to discuss possible outcomes, including the amount and duration of material costs. As the SEC states, cyber incidents "may result in losses from asserted and unasserted claims, including those related to warranties, breach of warranties, breach of contract, product recall and replacement, and indemnification of counter losses from their remediation efforts." Further, such incidents may result "in diminished future cash flows" and "impairment of certain assets including goodwill, custom-related intangible assets, trademarks, patents, capitalized software or other long-lived assets associated with hardware or software, and inventory."

The SEC also identified a potential source of solace for companies faced with this list of horribles, one that it deemed appropriate for disclosure to investors: "Description of relevant insurance coverage." Usually, potential insurance recovery is not considered to be a contingent asset that can offset potential liabilities on a balance sheet; however, the SEC recognized that insurance might play a key role in protecting shareholder value and aid in recovering from the consequences of a data breach or cyber-crime.

Contact the Authors:

Marc S. Mayerson
Of Counsel, Washington, D.C.
(202) 339-8456
mmayerson@orrick.com

Darren S. Teshima
Senior Associate, San Francisco
(415) 773-4286
dteshima@orrick.com

This article is adapted from an article originally appearing in the February 3, 2012 edition of The Recorder*, and reprinted with permission.*

The market for cyber-risk specific insurance policies has grown substantially in the past few years. It has yielded approximately $800 million in premiums, increasing in volume by roughly 30 percent in each of the last two years. Last year, a worldwide survey of more than 12,000 companies showed that nearly half of C-level executives confirmed that that their companies purchased cyber-risk insurance, and that 17 percent had already submitted claims under those policies. It is estimated that the price of such policies ranges from $7,000 to $40,000 per million dollars of coverage, and most companies purchasing such policies buy somewhere between $10 and $50 million of coverage, with one in twelve purchasing more than $50 million in policy limits.

These specialized insurance policies respond in part to uncertainty in the marketplace about whether existing insurance policies—commercial general liability and first-party property in particular—apply to cyber losses. Cyber-related losses include operational losses, risks from inadequate or failed internal processes and systems producing loss of service provided to customers, loss of data, and interruption in production and supply chains; financial risks, including the ability to conduct operations and maintain customer relationships, fraud, and theft; intellectual-property risks, including loss of development and planning documents and stealing of proprietary products and systems; legal and regulatory risks, such as compliance fines, notification costs, and litigation; and reputation risks, such as injury to the brand and loss of confidence in management.

These risks now are board and executive suite level concerns. While the awareness of executives of the importance of these issues is increasing, courts have for nearly twenty years imposed on directors the obligation to be aware of and to manage corporate information and reporting systems—on pain of personal liability for failure. *E.g., In re Caremark Int'l Inc. Derivative Litigation*, 698 A.2d 958, 970 (Del. Ch. 1996). This leads to the prospect of shareholder suits against directors and officers. Just over two years ago, following data breach Heartland Payment Systems—a payment-processing company—incurred more than $125 million in expenses and suffered a share-price loss of roughly 70 percent; while the securities action in that instance was dismissed, the new SEC guidance only highlights that directors and officers will continue to face exposure to litigation and the cost of responding to government investigations.

Recently, the First Circuit in *Anderson v. Hannaford Brothers Co.* (Oct. 20, 2011), held that consumers may have a right to recover damages in class-action litigation arising from data-privacy violations. In another instance, organized thieves hacked into a retailer's wireless network over a several-year period and compromised between 46 million and 94 million customers' payment card information; once the retailer realized the hack and disclosed it to regulators, some 20 class action suits were brought on behalf of consumers, payment-card issuing banks, and shareholders. The Federal Trade Commission and various state attorneys general launched investigations as did authorities in Canada and the UK. The retailer eventually agreed to provide three years' worth of credit-monitoring services to customers, reimbursed documented identity theft costs, and provided special customer-appreciation discounts. Estimated costs of the entire incident were more than $150 million.

In addition to such large scale losses, companies routinely are facing exposures from one-time data breaches, insider or disgruntled former employees' data thefts, hacks to secure systems safeguarding intellectual property assets, and losses of employee laptops or handhelds that contain or allow access to confidential business or customer information.

In the event of a data breach or malicious software attack that affects the value of a company's stock price, directors can expect to be greeted by shareholder suits. Directors in turn will seek protection from their company's corporate indemnities and available directors' and officers' insurance. These policies will pay for lawyers to defend the directors from shareholder actions and government investigations.

But the company itself may face potentially large losses and look to corporate insurance policies as sources of potential indemnification. First-party property policies, including business-interruption and extra expense, may be available to offset losses in part, but coverage will depend on the particular policy language and the surrounding legal issues are far from settled. *See American Guarantee & Liability Ins. Co. v. Ingram Micro, Inc.*, 2000 WL 726789 (D. Ariz. April 18, 2000); *but see Ward General Ins. Services v. Employers Fire Ins. Co.*, 114 Cal App. 4th 548 (2003) (The loss of "the database, with its consequent economic loss, but with no loss of or damage to tangible property, was not a "direct physical loss of or damage to' covered property under the language of the subject insurance policy, and therefore, the loss [was] not covered"). Liability policies also may afford coverage for invasions of privacy of customer data, website hijacking, and related injury to non-physical interests. *Creative Hospitality Ventures, Inc. v. US Liability Insurance Co.*, 655 F. Supp. 2d 1319 (S.D. Fla. 2009). Yet, some insurers have denied claims for property damage, invasion of privacy, and associated mental distress by arguing that their policies require actual, tangible physical injury—even though such limitations are not stated in the policy. The uncertainties of the application of existing policies combined with the potential size of cyber-risk losses has led to the rapid expansion in market offerings from insurers to target this particular risk; those policies are early drafts of what eventually will be developed and standardized. But companies that have purchased dedicated cyber-risk policies will turn—and already have turned—to them to cover the costs of data restoration, customer protections, crisis management, notices to consumers, credit monitoring, and implementing remedial security measures.

Most important, companies—directors, officers, IT departments, and risk managers—need to assess their exposures, securities measures, and remediation plans. The decision to maintain internal services for IT infrastructure or migrate to cloud-computing platforms, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS), all pose risks that need to be evaluated—and, for publicly traded companies, potentially disclosed in registration statements and in Management Discussion and Analysis (MD&A) in annual financial reports. Companies furthermore need to review their existing insurance policies as a source of potential indemnification and should evaluate the suitability of purchasing cyber-risk insurance policies. Companies should review carefully and seek to tailor proposed cyber-risk insurance policies being offered to them, given that the development of these products is in its infancy and some of the available forms contain exclusions and conditions that substantially limit coverage. Ultimately, only a multi-pronged approach—involving coordination across business segments and departments—and financial planning, including purchasing appropriate insurance, will prove to be a successful recipe to mitigate the risks and financial consequences of cyber-crime, consumer privacy data invasions, and other risks that computers, communication technology, and the internet pose to business.