

## Security and Privacy for Boards

### How is your board managing the information security threat?

Information security has catapulted out of the IT domain and become an enterprise-wide risk issue. Why now?

**A sharp industry, regulatory and legislative focus.** Some 46 states require companies to notify consumers/customers if data in their care is compromised. The Federal Trade Commission's Red Flag Rules put the onus on any operation extending credit to "flag" potentially fraudulent activity, with review and sign-off on the Red Flag program required by the board of directors. The Payment Card Industry Data Security Standards (PCI DSS) set a high bar for merchants and service providers, imposing fines and penalties for noncompliance. The list of regulations goes on... and new federal regulations and legislation are pending.

**Not if, but when.** Data breaches happen every day. Some 143 million personal information records were breached in 2009.<sup>1</sup> No amount of IT security can protect a company; addressing the human element is essential, and especially challenging. Companies and board members can be held accountable if any type of personal information is wrongfully disclosed—whether it is financial account information or names and social security numbers, patient health information or confidential corporate information, such as third party trade secrets.

**Costly events, getting even costlier.** The average cost per breach incident was \$6.75 million in 2009.<sup>2</sup> Costs associated with a typical incident can include:

- Notification and identity monitoring expenses
- Computer forensics, legal assistance, public relations and crisis management consulting
- Potential legal liability from class action lawsuits
- Regulatory actions and fines/penalties

When an incident costs a company substantially, shareholder suits can potentially ensue.

**Board members at risk.** Ever-expanding regulations are giving plaintiff attorneys plenty of launching pads for lawsuits when an organization suffers a breach—whether the breach comes at the hands of a malicious hacker, a disgruntled employee, or an absent-minded administrator. Suits can allege:

- Negligence by the board in addressing the organizations information security program and complying with industry/regulatory standards
- Directors knew or should have known that information assets were vulnerable to attack and that serious losses would result if the data was breached
- Breach of care, loyalty and good faith causing the organization to sustain millions of dollars in damages

Surprisingly, 98 percent of senior executives say their boards are not "actively addressing" IT operations and vendor management, according to a 2010 Carnegie Mellon survey.<sup>3</sup>

<sup>1</sup> Verizon Business 2009 Data Breach Investigations Report

<sup>2</sup> Ponemon Institute Cost of a Data Breach Report 2010

<sup>3</sup> Carnegie Mellon Governance of Enterprise Security: CyLab 2010 Report

## How Specialty Risk Protector® can help

To further safeguard your organization beyond IT security, you can be prepared to effectively manage an incident and mitigate the financial damages to your company. Preparation should include:

- (1) Assigning a separate committee of directors to independently deal with security and privacy issues
- (2) Mandating that your internal risk team conduct a technology audit regularly, so vulnerabilities are frequently assessed and addressed
- (3) Securing insurance that will address the financial risk and help your organization to effectively manage a breach incident

While most cyber incidents are not covered by traditional commercial property, casualty, or crime policies, Specialty Risk Protector offers a simple, powerful way to protect your company and your board in a networked world. The coverage provides:

- Coverage for third party security and privacy liability
- Network business interruption insurance for loss of income and operating expenses your organization suffers when operations are interrupted or suspended due to a failure of network security
- Cyber extortion insurance to investigate and/or settle network security related extortion demands made against your company
- Event management insurance for myriad costs required to manage and mitigate a data security incident, such as:
  - Costs to retain public relations services to help protect your organization's reputation
  - Costs to notify consumers of a release of private information (mandated by law in most states)
  - Credit monitoring or other remediation services to help minimize damages to those victimized by a covered privacy or network security incident

To learn more about Security & Privacy Insurance, please visit [www.chartisinsurance.com](http://www.chartisinsurance.com), e-mail [executiveliability@chartisinsurance.com](mailto:executiveliability@chartisinsurance.com), or contact your insurance broker.

---

Chartis  
175 Water Street  
New York, NY 10038  
[www.chartisinsurance.com](http://www.chartisinsurance.com)



Chartis is a world leading property-casualty and general insurance organization serving more than 40 million clients in over 160 countries and jurisdictions. With a 90-year history, one of the industry's most extensive ranges of products and services, deep claims expertise and excellent financial strength, Chartis enables its commercial and personal insurance clients alike to manage virtually any risk with confidence.

Chartis is the marketing name for the worldwide property-casualty and general insurance operations of Chartis Inc. For additional information, please visit our website at [www.chartisinsurance.com](http://www.chartisinsurance.com). All products are written by insurance company subsidiaries or affiliates of Chartis Inc. Coverage may not be available in all jurisdictions and is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain coverage may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds and insureds are therefore not protected by such funds.