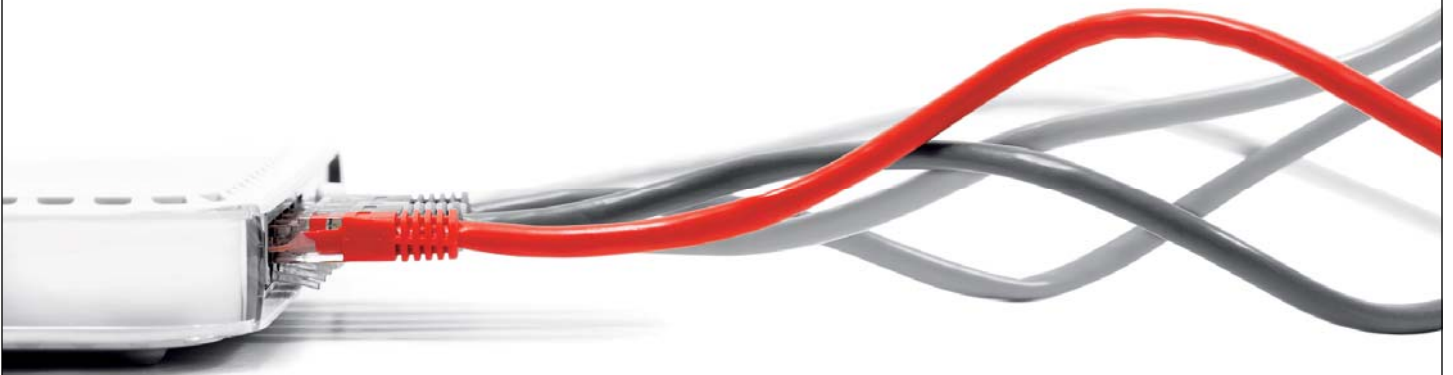




Mitigating Privacy Risk



Mitigating Privacy Risk

Small Businesses Face Large Exposures

As recent headlines suggest, the threat of data breaches is becoming a greater everyday issue for businesses. Since 2005, there have been more than 166 million breaches¹ of customer records with more than 80 percent striking small merchants² and a new breach is reported every day. An influx of criminal activity and data security legislation should be taken as a cue to protect business assets before they are compromised. All businesses that transmit or store any form of personally identifiable information face a severe and common threat.

Currently, 38 states and the District of Columbia have laws regulating consumer notification and assignment of liability. Additionally, there is momentum in Congress to create national standards for reporting and other issues. These legislative efforts combined with the large number of data breaches are alerting businesses to proactively implement risk prevention programs, but many times, those responsible for risk management do not have full understanding of privacy risks.

Since the road to proper data breach prevention requires time, financial and manpower commitments, small and medium sized businesses with less resources than large organizations face more potent challenges in implementing effective privacy protection processes. Effective data protection should also be considered on a case by case basis, which means there is not one blanket way to implement it.

Businesses to protect against compromised data

Privacy risks differ for every business, but all businesses face them one way or another. Many businesses have yet to recognize that any organization that maintains any form of private records risks suffering a data breach.

One part of the solution is specific insurance coverage that provides one part of a sound privacy protection program. Many companies are unaware of privacy risks, due to lack of clarity on general liability and errors-and-omissions policies. General liability policies typically do not cover data breach liability, while errors-and-omissions policies offer limited protection.

Threat of legal action if ignored

From a broader perspective, businesses are at risk for lawsuits, regulatory investigations and fines. Although consequences are onerous for large organizations, they have the potential to impose costly burdens on firms with limited resources. More specific risks include the costs of notifying any client, vendor or anyone else affected by a breach. The cost for each record can exceed \$182, according to one study³. There are also looming costs for repairing and restoring IT systems, reputation damage and hindered customer relations. If the data breach is potent enough to endanger a majority of company assets, financial liability could include costs for closing a business.

Risk management effective but underused

More specific areas where small and medium sized businesses can face liability include:

- Liability arising out of breach of confidentiality
- Statutory liability for breach of laws relating to personally identifiable information
- Liability under contract for breach of confidentiality clause
- Defense costs and fines and penalties arising out of regulatory action
- Security breach notification costs

Why now?

To understand the need to protect their businesses, entrepreneurs need to know why and how data breaches are a threat to them and their businesses. For one, there has been an increase in the amount of data stored. Online storage space in particular houses financial data for many industries, including retail and financial services. The cost of computer storage is reducing rapidly, so it's easier for companies to hold sensitive data longer. What's more, companies are increasingly looking to outsource operations, such as payroll and benefits administration, to cut costs. By outsourcing a previously internal process, companies can further increase their vulnerability and provoke additional risk. Contractual relations and data security programs are crucial to maintaining strong data security.

There has also been a proliferation of data storage options and mobile devices, such as laptops, PDAs and portable hard drives. Laptops continue to be particularly vulnerable, mostly as the result of human error.

To fully understand the scope of risk, small and medium-sized businesses must also look externally. For larger companies and across business sectors, individuals and industries are demanding better protections and clearer lines of responsibility. Businesses that are adversely affected by another company's breach – such as banks that must reissue millions of credit cards and absorb the costs – are also pushing for laws to help shift liability and costs.

Legislation on the increase

Many of those efforts have been successful and many more are pending. Overall, there is a trend toward better protections, expanded notification and more stringent liability through legislation.

A new Minnesota law, for example, prohibits any business that accepts credit, debit or stored value (e.g., gift, prepaid phone cards) from retaining certain data after a transaction has been authorized. The law also permits the financial institutions that issue the cards to recover the costs of a security breach if the business has improperly retained data (effective August 2008). In other states, including Massachusetts, equivalent laws are under discussion.

In California, Governor Arnold Schwarzenegger recently refused to sign a similar data security law relating to retaining sensitive post-transaction data, but supporters have said they will introduce a modified version.

Nationally, industry specific legislation such as the Health Insurance Portability and Accountability Act (HIPAA), and Graham-Leach-Bliley (financial institutions) echo the severity of data breaches and provide initial guidelines to protect personal health information (PHI), credit card information, Social Security numbers, addresses and confidential data stored by third parties.

Clearly, the risks are coming from all directions and businesses must protect themselves actively. While insurance coverage is critical, they also need risk-management strategies that encompass both technology and the human factor.

Focus on technology, procedures and people

Businesses must also understand their obligations to safeguard the data they collect, process and store. But many small businesses don't have full-time risk or IT managers. Some depend on outside vendors while others implement their own protections. Also, while risk management policies and procedures must be integrated thoroughly throughout an organization, many are piecemeal and incomplete. There may be minimal or no coordination among the people involved, from the IT specialist to the employees to the president. Further, many small businesses have minimal security budgets.

There are some guidelines businesses can follow. For technology, key actions include encryption, software quality assurance and testing, frequent updating of hardware and software, password protection of vital information, and erasing thoroughly the data on any computer or storage device that is being discarded. These activities will help eliminate hacker practices such as phishing, in which thieves send fraudulent e-mails for the purpose of extracting personal information. Companies must also take practical, simple steps. For example, thoroughly shredding paper records with sensitive information will curtail breaches generated from activities like dumpster diving.

An emphasis on personnel and company policies is equally important. All companies should have a written data-security plan that includes a clear hierarchy that limits access to data. There should also be procedures that instruct a group on how to handle related situations like reporting a lost or stolen laptop. Additionally, employee training and awareness programs should be implemented to ensure guidelines are practiced.

Against this backdrop, however, there is some good news. Data breach insurance is increasingly available and affordable. Purchasing data-breach coverage is a simple

process with a straightforward application. Moreover, it typically covers a range of costs, including:

- Notification and reporting expenses
- IT forensic services
- Crisis management
- Credit monitoring
- Business interruption losses
- Defense costs, fines and penalties

With risks increasing by the day, no small business should assume it will remain unscathed. Ensuring that appropriate cover is in place can help protect businesses from the increasing global threat of data breach.

¹Privacy Clearinghouse

²Visa USA

³2006 Ponemon Data Breach Study

Please contact the following for more information:

Oliver Brew

Vice President of Technology, Media and Telecoms Underwriting
Hiscox USA
Phone: 914.273.7448
Email: Oliver.Brew@Hiscox.com

Brian Thornton

Vice President of Technology, Media and Telecoms Underwriting
Hiscox USA
Phone: 312.380.5556
Email: Brian.Thornton@Hiscox.com

Brian Ross

Underwriter
Hiscox USA
Direct: 914.273.7421
Email: Brian.Ross@Hiscox.com