

Privacy Insurance

Frequently Asked Questions on Privacy and Data Security Insurance



William Gallagher Associates
Phone: 888.261.8884
www.WGAins.com

*Financial liability for breaches of privacy and data security is rising exponentially. The 2009 Ponemon Institute study revealed the average cost of **\$204 per breached record**, with companies bearing **average aggregate costs of \$6.75M per incident** - both amounts representing significant increases over costs incurred in previous breaches.*

These unique risks cannot be managed by diligent network security measures alone.

Everyone who uses, stores or controls personal information about others – whether in business, finance, law, medicine, education, or other fields - is at risk.

William Gallagher Associates is a leading provider of insurance brokerage, risk management and employee benefits services to firms with complex risks, within industries that include technology, life sciences, financial risks, health care, aviation, energy, and environmental services. WGA has offices in Boston, MA; New York, NY; Hartford, CT; Princeton, NJ; Columbia, MD; Atlanta, GA; and Paris, France.

What is "privacy insurance"?

Privacy insurance is intended to cover the insured for liability arising from the failure to protect or maintain the privacy of many types of confidential or non-public information. Privacy insurance can also protect the insured for its failure to comply with the growing number of laws requiring companies and institutions to protect personal information.

Is it the same thing as "cyberliability" insurance?

The term "cyberliability insurance" is often used to describe a related group of insurance products that are intended to provide coverage for some of the risks associated with doing business in the Internet age. These can include privacy insurance, network security insurance, cyber extortion insurance, media insurance, intellectual property insurance, or insurance that will provide coverage for allegedly defamatory statements or false advertising transmitted over the Internet (whether in connection with business activities or in social media). The common thread is that the insurance is designed to cover exposures that can arise when computers and networks are involved in the conduct of business or otherwise in the use, storage of, access to or transmission of information.

Privacy insurance is a type of cyberliability insurance. It is focused on the financial exposures that arise from the collection, handling, use, transmission, publication, management, storage or disposal of information. Such information is often electronic in nature but need not be so: a national pharmacy chain has faced significant exposure from the improper disposal, into dumpsters outside its stores, of paper-based information about its customers' prescriptions.

Why does there seem to be a lot of recent attention to this kind of insurance?

Several factors have contributed to the increased visibility of privacy-related exposures and of the insurance for the significant financial losses that can result from breaches of privacy. As

computers, networks and social media penetrate more deeply into our lives, increasing amounts of personal or otherwise private information is stored on or accessible via computer networks and the Internet. We make use computers and the Internet to make purchases using credit cards, manage our bank accounts, store and transmit health and medical information, apply for and receive government benefits, reveal our personal preferences and closest secrets via email and other social media, store information "in the cloud" and otherwise make confidential information available to others. Companies, health organizations and governmental bodies collect many types of confidential information, which they use, store, grant access to, and transmit over networks.

The vast amounts of information residing on computers has led to several high-profile breaches of privacy that have garnered media attention. Many of these breaches have been deliberate (driven by such phenomena as the growing black market for medical and financial information of individuals), others have been inadvertent (such as lost laptops or inadequate disposal of documents), but all have served to help focus the public's attention to the risks associated with the collection and storage of private information.

Largely in response to the public's increased awareness of and sensitivity to privacy matters, there has also been a significant increase in the number of laws and regulations governing the collection, use, storage, protection and disposal of data. There are numerous laws at the federal level, in more than 45 states, and in many foreign countries -- most notably (and probably stringently) in the European Union -- that require specific actions to protect data security and impose meaningful financial penalties for the failure to protect private information.

Two recent legal and regulatory efforts illustrate the growing scope of responsibilities and risks relating to the protection of private information. Massachusetts' Data Security Regulations, effective in March 2010, represent the most extensive state imposition of detailed requirements for the protection of non-public information of individuals. Whether or not businesses are located in Massachusetts, if they have personal information (as defined in the Regulations) of Massachusetts residents, then they are subject to the Regulations' stringent data security obligations and potential financial exposures.

While healthcare organizations have grown accustomed to the privacy requirements of the federal Health Insurance Portability and Accountability Act (HIPAA), the American Recovery and Reinvestment Act of 2009 (ARRA) contains a provision, called the Health Information Technology for Economic and Clinical Health Act (HITECH) Act, that greatly expands the scope of HIPAA's data privacy and security obligations to "business associates" providing services to those healthcare organizations. Now a broad swath of vendors and service providers to healthcare organizations -- but not themselves directly in the healthcare field -- are subject to HIPAA's substantial data privacy and security obligations.

The Massachusetts Data Security Regulations and the HITECH Act are examples of the tectonic shifts in companies' data privacy responsibilities. As a result of legislative and regulatory efforts such as these, most businesses and organizations are now subject to broad and deep obligations relating to the protection of private information -- and to the financial risks associated with the breach of those obligations.

What are some of the major sources of privacy breaches?

Privacy and network security experts often describe the principal data breach perils as being lost or stolen laptops or storage devices (USB keys or portable hard drives), lost or stolen backup tapes, hacking, employee inadvertence, rogue employees, misdelivery or the improper disposal of documents, or the activities of business partners such as vendors or other service providers (whose own data breach risk management practices may be less than optimal).

How expensive are data breaches for the companies that experience them?

The 2009 Ponemon Institute study noted above indicated that the average overall cost of a data breach has risen to about \$204 per breached record, with companies bearing average aggregate costs of about \$6.75M in addressing and remedying data breaches. These amounts are expected to continue increasing.

We have very strong network security protections and a great IT staff, do we have much risk?

It has become abundantly clear that the risk of a privacy breach cannot be "managed away." The well-regarded 2009 Ponemon Institute survey surprised many people in its reporting on the common causes of data breaches. The survey revealed that among the surveyed companies:

- More than 40% of breaches involved errors made by third parties such as vendors or service providers, or compromises to data while it was in the control of third parties.
- Approximately 35% of breaches involved lost or stolen laptops or other mobile computing devices. The cost of a data breach from a lost or stolen laptop or mobile device was a little more than \$224 per record, while the cost of other breach was about \$192 per record.
- Approximately 25% of breaches resulted from a criminal or other deliberate act rather than from negligence.
- More than 80% of breaches involved organizations that had suffered multiple data breach involving the compromise of more than 1,000 records containing personal information.

Companies can and should undertake vigorous and ongoing steps to reduce the risk of a data breach, with the same diligence with which they undertake vigorous and ongoing steps to reduce the risk of fire or other catastrophic damage to their physical assets. But just as the presence of sprinklers and other precautions and trained behaviors do not eliminate the risk of fire (thus the ubiquity of fire insurance), so too the presence of firewalls and other IT best-practices do not eliminate the risk of data breach.

While there is wide agreement that companies in certain industries -- primarily healthcare and related businesses and organizations, financial institutions, and those in the fields of retailing, hospitality and education -- have the most glaring need for privacy insurance, the reality is that any company or organization that handles, stores, uses or transmits personally identifiable information has financial exposure for failing to protect this information. An organization

needn't have "customers" in order to face liability for breaches of privacy; there is exposure with respect to the confidential information of employees or of business partners as well.

Companies increasingly understand that data breaches are almost inevitable, and that they face significant financial exposures and reputational risks from such breaches. This awareness has increased interest in insuring against the risks that can't be eliminated by risk management. As Samuel Johnson said, "when a man knows he is to be hanged in a fortnight, it concentrates his mind wonderfully."

We already have several insurance policies. Aren't we covered under those policies for data security and other network-related exposures?

Some of the financial risks arising from privacy breaches may be covered by CGL, crime, E&O and other policies. There is considerable debate about the extent of such coverage, and a considerable amount of coverage litigation as well. Sometimes there is an outright exclusion denying coverage for privacy or network security liability. Other times coverage appears to be granted in one place and excluded in another. Often the policy language is ambiguous at best. While it is quite possible that some privacy-related exposures are covered by one or more of the insurance policies that most companies already have in place for other reasons, it is clear that many or most of the greatest financial costs resulting from a data breach will not be covered under these other policies.

Are privacy insurance policies issued by different insurers largely the same, similar to many other types of insurance coverages?

No. This is a rapidly developing area of insurance, and there are important coverage differences among the privacy insurance policies and endorsements provided by different carriers. There is a broad -- and growing -- range of financial exposures associated with breaches of privacy or data security. These can include, for example, liability to individuals affected by a breach of their personal information, liability to companies for breach of their confidential corporate information, out-of-pocket costs for notifying potential victims of a privacy breach and for providing call center and credit monitoring services, the costs of determining the cause of the breach and of restoring lost or stolen data, regulatory and other fines and penalties imposed on the insured as a result of a privacy breach, and the costs incurred in trying to minimize the damage to the insured's reputation caused by the breach. Insurers have widely different appetites for covering the range and extent of financial risks arising from data breaches, and the scope of coverage is often different from one insurer to the next. All insurers are willing to negotiate coverage terms if pressed with specifics, so it is important for a prospective insured to be knowledgeable, diligent and dogged throughout the insurance purchasing process.

For more information or a free quote on insurance go to <http://www.privacy-insurance.com>

