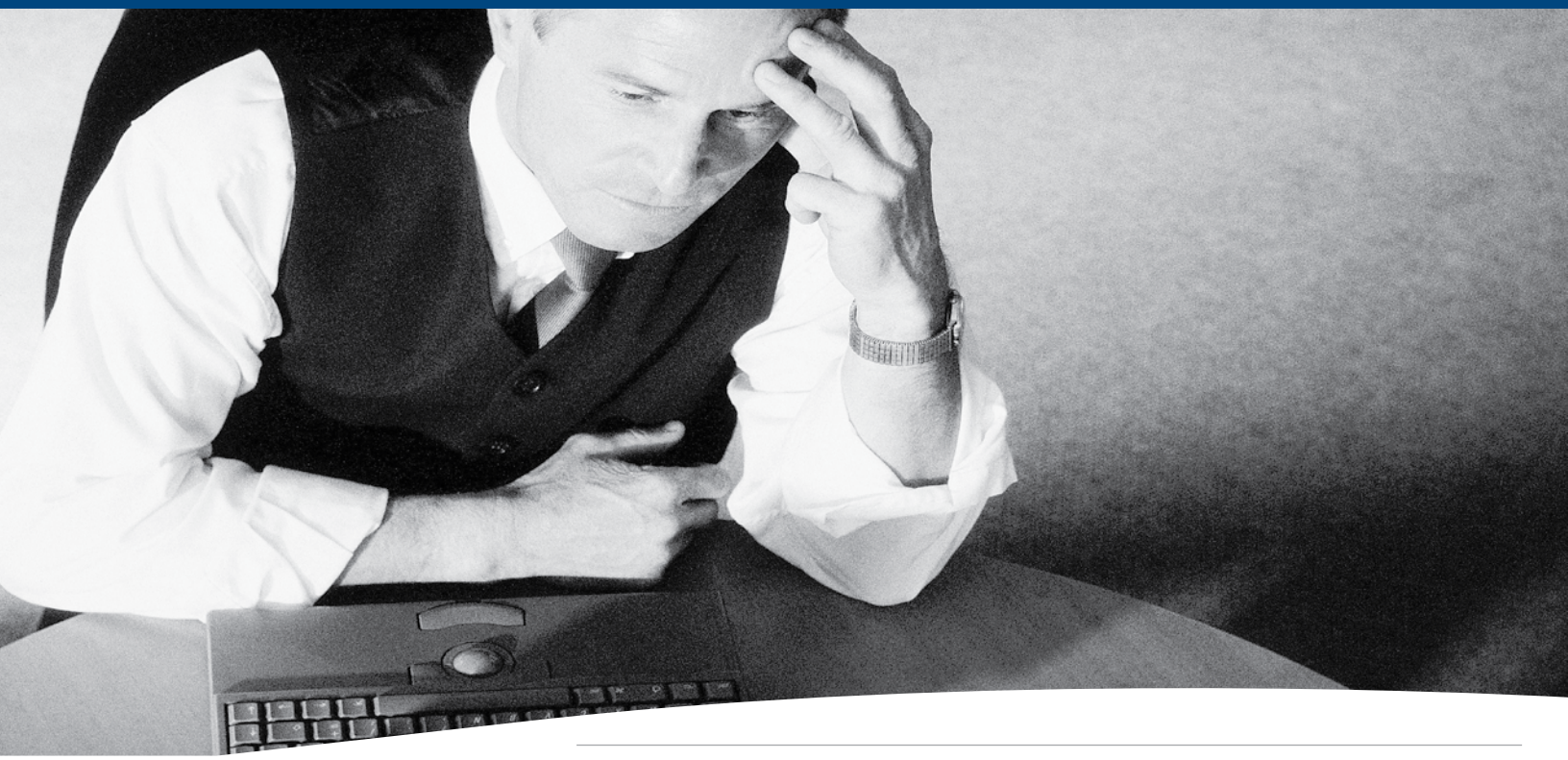
Exposed in Europe

Data Breaches and Their Impact in a Changing Legal and Regulatory Environment

By: Emily Q. Freeman and Ben Beeson
Lockton Global Technology & Privacy Risks Practice | January 2011



Emily Q. Freeman, ARM, AU
Executive Director
Global Technology & Privacy Risks Practice

011 44 20 7933 2224
emily.freeman@uk.lockton.com

Ben Beeson
Partner
Global Technology & Privacy Risks Practice

011 44 20 7933 2857
ben.beeson@uk.lockton.com

"With more intense scrutiny from media and regulators, private enterprise and government entities alike are increasingly aware that the old approach of hushing up data leaks has well and truly run its course."

In recent years, the headline events in data breaches have been dominated by events originating in the U.S. However, there have certainly been significant data breaches with a multi-country impact. For example, the TJX Companies, whose wireless network compromise was revealed in January 2007, involved millions of credit card transactions, which included brands and store locations in the U.K. and Ireland.

Of the 15 largest known data breaches in the world, one was caused by a government entity in the U.K., HM Revenues and Customs. In 2007, two CDs containing the names, birth dates and National Insurance numbers of 25 million children, parents, guardians and caregivers were lost. The unencrypted CD was lost in transit between two government locations.

There has also been the all too familiar pattern of data breaches and cyber theft involving EU financial institutions, telecommunications, professional services, hospitality industry, and merchants.

However, the legal and financial consequences in Europe are quite different than in the U.S.

Cyber security continues to make the list of "global risk issues to watch," from the growing prevalence of cyber theft to the little understood possibility of cyber warfare.

Cyber security encompasses sensitive data/information (especially nonpublic personal financial or medical data, and sensitive corporate data) and critical information infrastructure breakdown, and ranges from motivations of mischief, revenge, fraud, extortion, espionage and terrorism. With more intense scrutiny from media and regulators, private enterprise and government entities alike are increasingly aware that the old approach of hushing up data leaks has well and truly run its course. The loss of third-party data, in particular customers, patients, and employees can entail significant financial and reputational costs.

There are strong indications that Europe is at a tipping point in its legal and regulatory environment surrounding data breaches. Here we examine the risks your organization may face in the changing data security landscape in Europe – *whether you have employees in Europe, locations, client contracts, subsidiaries or possible acquisitions* – and what you can do to mitigate and protect your business and operations.

Europe—Basis in Privacy Rights

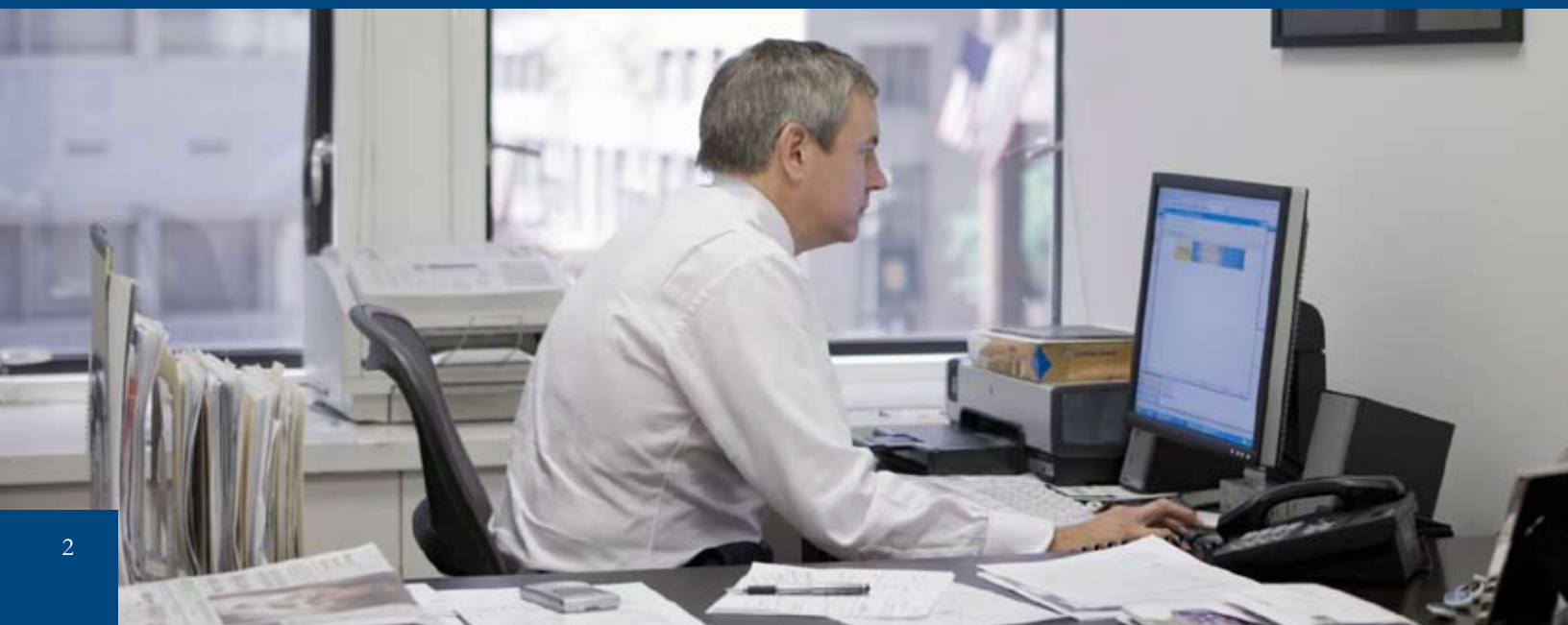
The right to privacy is a highly developed area of law in Europe. All the member states of the European Union (EU) are signatories of the European Convention on Human Rights (ECHR). Article 8 of the ECHR provides a right of respect for one's "private and family life, home and correspondence," subject to certain restrictions. The European Court of Human Rights has given this article a very broad interpretation.

Effective in 1998, these privacy rights are represented in the EU Data Protection Directive (officially Directive 95/46/EC), which regulates the processing of personal data within the European Union on the basis of seven principles:

- Notice
- Purpose
- Consent
- Security
- Disclosure
- Access
- Accountability

EU directives are addressed to the member states and are not legally binding for EU citizens in principle. However, the member states must transpose the directive into internal law, and all member states have enacted their own data protection legislation. There is no such single over-riding privacy law in effect in the U.S. Rather it is an evolving collection of state and federal laws and regulations.

"The right to privacy is a highly developed area of law in Europe."



Like the U.S., the responsibility for compliance rests on the shoulders of the "controller," meaning the person, public authority, agency or any other body that processes the personal data. This responsibility is expressed in the U.S. as the "data owner" or "covered entity."

One critical difference to U.S. privacy laws is certainly the obligation of consent and the right to be informed when nonpublic personal information linked to an individual is being processed or shared. These rights transcend EU states and have created significant obligations regarding the transfer of such information to non-EU states, significantly to the U.S. (Refer to articles regarding the "Safe Harbor Agreement" signed between the U.S. and Europe in 2000.)

The Recognition of Data Security

Though EU governments and regulators clearly have data security issues in their sights, European law still has some catching up to do in this relatively new and fast-evolving sphere of malicious and criminal activity. Unlike the vast majority of U.S. states, for instance, most European countries still have no legal requirement for "data controllers" to notify individuals about data security breaches.

The key point of reference here is the European Community Data Protection Directive 95/46/EC, which is currently under review to address "new challenges of the information age," including globalization, e-commerce, cloud computing and – importantly – for the first time, "data security breach." Up to now, the emphasis has been on protecting data, rather than on what happens when data is lost or stolen.

In response to increasingly alarming press reports of personal data going astray, a number of countries, including Austria, Germany and Norway, have pushed ahead of the mainstream EC legislative agenda to introduce national laws that include a notification requirement for data breaches.

There are signs that other countries are heading in the same direction, with Ireland and the U.K. both recently introducing codes of practice on personal data security breach, and strong demand for legislation in Finland and the Netherlands. Several other countries, rather than introducing new data-breach legislation, have chosen the path of interpreting existing law as implying a duty to notify. These include Cyprus, the Czech Republic, Estonia, Sweden and Hungary.

Where not required by EU country law, a data breach involving EU-affected persons in many cases involved "voluntary notification" to preserve brand and reputation, which is a real risk for industries where the data subjects have a choice of where to do business—especially if the data controller is a financial services company, retailer, hospitality, travel, or professional services company. "Notification" included the actual costs of notification for legal, mailing, tracking, crisis management communications, and public relations. It also included voluntary mitigation services to the affected individuals, such as free credit reports, credit monitoring, professional call center and other support activities. These facets of notification costs are similar to the U.S. environment of a "legal obligation to notify."

The EU Legal Net Tightens on Data Security Lapses

The other significant Directive to consider is the E-Privacy Directive 2002/58/EC. One of the effects of amendments agreed to this Directive last year (due to come into effect in early 2011) will be to introduce a new obligation on Internet Service Providers (ISPs) and telecom companies to notify the authorities and potentially affected individuals of a data breach. We expect more clarity on the rules regarding data breach notification requirements from the EU cyber security advisory board, ENISA. This appears to be another potentially significant step toward compulsory notification for all data collectors.

At the same time, sector-specific legislation in various European countries—particularly within the financial services sector—has also introduced new requirements for data breach notification. So the overall tendency is clear: Organizations that prefer not to notify data breaches are living on borrowed time.

Regulatory Investigations and Penalties

Declaring data breaches inevitably entails dealing with their fallout. Aside from the direct cost of communicating with data subjects whose personal details may not have been kept secure, there is financial cost and reputational harm associated with regulatory investigations.

The issues surrounding privacy concerns of Google maps has been widely publicized around the world and has been the subject of investigation by Information Commissioner Offices in France, Germany and Switzerland. There have been a number of ICO investigations regarding data privacy issues, including Spain, U.K., France and Germany.

In the U.K., for example, the Information Commissioner's Office requires that "organizations which process personal data must take appropriate measures against unauthorized or unlawful processing and against accidental loss, destruction of or damage to personal data." Until recently, however, the sanctions for failing to take such appropriate measures amounted to little more than an official reprimand. Since April 2010, however, the U.K. ICO has been empowered to issue fines of up to £500,000. It has not held back from handing out six-figure fines, wherever a data breach has occurred with the potential to cause damage or distress, regardless of whether this potential has been realized. In practice, the ICO seems particularly keen to punish breaches involving unencrypted data held on portable devices.

The U.K. Financial Services Authority (FSA) has already shown itself ready to impose fines running into millions of pounds for financial services companies guilty of allowing customer data to be at significant risk. The U.K. arm of a major global insurance company, for example, was fined £2,750,000 in August 2010 for having allowed thousands of customers' bank account and credit card details to go missing. This event involved policyholder data being transferred to a non-EU based data center. A strong recommendation from the FSA to a data collector to notify would be treated with great seriousness and would make notification to the affected data subjects highly likely. It is a safe bet to assume, however, that the cost of voluntarily notifying and reassuring the affected customers and mitigating damage to the company's brand from a high-profile data breach would already have cost the company far more. When a regulatory investigation commences, it becomes a public event that engenders a sense of urgency behind "voluntary" notification.

Civil Liability

One major difference between data breaches affecting U.S. data subjects vs. European counterparts is the issue of civil liability and the threat of class actions. In the EU, it is much more difficult and expensive for plaintiffs to bring civil cases, and the class action potential, up to now, is virtually nonexistent. The U.S. has been the showcase for data breach class actions, which is a key driver of legal costs.

A major component of defendant legal costs in the U.S. is associated with process of fighting to decertify the class. In January 2011, it bears reading the U.S. Ninth Circuit Court of Appeals decision in two class actions filed by Starbucks employees in Washington (Case No. 09-35823/24) following a stolen laptop containing unencrypted employment-related details like names, addresses and Social Security numbers of 100,000 employees. Although the decision granted the plaintiff's standing to sue in federal court, the court also held—consistent with many other U.S. courts deciding security breach notification cases—that the plaintiffs had not pleaded, and could not prove, that Starbucks' actions caused them harm under state tort or contract law.

This sort of case would most likely never have gotten off the ground in Europe, where plaintiff legal costs are not on a "contingency" basis, certain countries prohibit such classes, and there are other high barriers to filing.

Data Breach Cost Metrics

Lockton recently conducted a webinar on EU developments with the well-known researcher and consultant, Dr. Larry Ponemon. The Ponemon Institute *(www.ponemon.org)* has published various excellent surveys on data breach costs in France, Germany and the U.K. There are striking similarities and major differences in the results of these surveys of private enterprise and government entities in EU states vs. the U.S.

First the similarities:

- Data protection is an important part of an organization's enterprise risks and risk management efforts in industries where customer/patient personal information is necessary to conduct business.
- Data breaches have occurred to the majority of the surveyed organization. For example, the 2009 German study indicated that 53 percent of all companies and organizations surveyed suffered at least one data breach in the last 12 months. In the U.K. survey, 70 percent of the U.K. organizations had at least one data breach in the past year, with public service institutions and financial services firms the worst affected.
- There is a trend in the increasing cost of data breaches and incidents of such by third-party vendors and business associates.
- The requirement to notify under law or regulation is a key driver of financial loss and reputational harm.
- Adoption of encryption technologies has been driven by data protection laws, industry requirements (such as PCI DSS regarding credit cards), as an IT best practice, and increasing recognition at senior management and board level about resultant brand damage from data breaches.

Now the key difference: Cost metrics reflecting the differences between mandatory vs. voluntary notification and civil liability landscape.

DIRECT LOSS OF DATA BREACHES
U.S. MANDATORY NOTIFICATION

- Data breach front-end, direct costs are a major component of loss.
- Direct costs average $6.65M.

DATA BREACHES CONTINUE TO BE A VERY COSTLY EVENT FOR ORGANIZATIONS
(Ponemon 2009 Annual Study of a Data Breach)

COST	2007	2008	2009
Detection & Escalation	$9	$8	$8
Notification	$15	$15	$15
Response	$46	$39	$46
Lost Business	$128	$139	$135
TOTAL	**$199**	**$202**	**$204**

Source: Ponemen Institute

DIRECT LOSS OF DATA BREACHES
U.K. VOLUNTARY NOTIFICATION

- Costs reflect voluntary notification, regulatory exposure.
- Average organizational costs— £1.68M.

DATA BREACHES CONTINUE TO BE A VERY COSTLY EVENT FOR ORGANIZATIONS
(Ponemon 2009 Annual Study of a Data Breach)

COST	2007	2008	2009
Detection & Escalation	£15	£11	£12
Notification	£1	£3	£7
Response	£15	£14	£17
Lost Business	£17	£32	£29
TOTAL	**£48**	**£60**	**£65**

According to the latest Ponemon Institute's findings, the U.K. data breaches involving the loss of between 5,000 and 60,000 records cost an average of £65 per record in 2009, up from £60 in 2008. The largest component of this cost for the U.K. firms and public bodies is an average £29 due to lost business, of which abnormal customer churn/loss of trust is a key contributor.

In the U.S., by comparison, the average per-record cost of similarly sized data breaches is twice as high ($204 compared with an equivalent $98 in converted £/USD in the U.K.). The main reason for this difference is that compulsory notification of data loss breaches in 46 out of 50 states entails far higher costs for detection, escalation and notification.

Moving to mandatory notification, as has Germany, results in cost levels more in line with the U.S. In Germany, for example, the average per-record data breach cost already stands at $177 in converted Euro/USD—far closer to the U.S. figure of $204.

The charts for the U.K. and the U.S. follow a breakdown of costs as follows per record: detection and escalation, notification, post-event response and lost business.

The average per-record cost masks huge disparities in the actual costs incurred. The loss of many thousands of records could in practice cost far less than losing the data belonging to a smaller number of very-high-value individual or key corporate customers. Abnormal churn rates for customers affected by data breach appear to average at around 3 percent, but can be as high as 10 percent for financial services, communications and healthcare organizations. Losing the lifetime value of one in ten customers affected by a breach involving thousands of records could prove very painful indeed.

Other response costs could include those associated with restrictions or injunctions imposed by the authorities following a data breach, or with follow-up audits and investigations into the business practices that have given rise to the data security breach. As European law tightens up on data security, regulators may also in future require that formal compensation schemes be established for customers affected.

All of which clearly illustrates that data breaches represent a key enterprise risk. So what can you do to mitigate the risks to your organization?

Limiting Your Exposure to Data Breach Risk

As a fundamental requirement, it is important to view data protection as an enterprise risk involving a cross-functional risk committee or team. This effort to improve security involves investment and senior management support.

Looking at how data breaches come about can provide some clues to risk prevention. The Ponemon Institute's research shows that human error and systems glitches – often not that easy to distinguish – collectively account for around three quarters of the U.K. data breaches. But it is the 24 percent caused by malicious or criminal action that tend to be most costly. Breaches that involve vendors, independent contractors and business associates tend to be somewhat more expensive that those that do not, while those involving intellectual property and corporate trade secrets tend to be considerably more costly.

Basic IT security measures such as ensuring sensitive records are encrypted—still far from universally adopted—at rest, in transit and on mobile devices—can of course significantly help to mitigate the risk of sensitive data falling into the hands of unauthorized persons. Other improvements (lower per-record costs) include a designated person(s) responsible for IT security, outside testing and auditing of IT security effectiveness, including penetration testing and policy/procedures audits, and achieving security certifications (ISO for example) or industry security requirements (PCI DSS for credit cards).

Other common post-event activities reported by organizations that have suffered a data breach recognized the core people and processes risks:

- Security awareness and training.
- Improved identity and access management.
- Data leakage programs.
- Application security built into application development process from the beginning of concept/design.

Third-Party Vendors and Data Breach

Lockton has written extensively on the subject of vendor risk management from due diligence through contract requirements and insurance. There is a white paper that we would recommend from the Lockton library, and the Lockton Global Technology and Privacy Risks Practice would be available to discuss outsourcing and offshoring vendor requirements in more detail with your special client needs in mind.

Lockton can also advise on the latest developments in insurance requirements for different types of vendor relationships and how to avoid critical pitfalls in such requirements. There have been a number of well-publicized breaches by vendors, where nothing stood behind the indemnity they signed in the client contract and resulted in an inability to pay for notification costs and other downstream loss.

The Need for a Cross-Border Data Breach Contingency Plan

The global nature of data breaches and the changes in the legal and regulatory environment mirror the developments in global business, mobile work force, outsourcing and off-shoring, and major advancements in technology (mobile devices, cloud computing, etc.).

Organizations have developed contingency plans for physical events—pandemics, natural catastrophes, product recall and the like. IT has developed hopefully effective internal communication and escalation to recognize when an incident needs to come to the attention of senior staff and department heads (CSO and CIO level).

The missing element is planning for the mitigation and outside experts required to deal with a real data breach involving a single country, or increasingly, the possibility of multiple countries where local law or regulation needs to be considered.

“Organizations that prefer not to notify data breaches are living on borrowed time”

The identification of outside experts pre-breach is an important component of an effective data breach contingency plan, as well as the internal crisis team that would be involved. Such experts would include forensics experts and privacy law experts. On the privacy law side, the team needs to include specialists who have knowledge and language skills to address cross-border data breach issues.

Again, Lockton is very engaged with clients and insurance markets regarding data breach response and the need for expert panels that can respond very quickly post discovery. We would be glad to discuss this in more detail with our clients, and we view data breach response to be a key differentiator in evaluating potential cyber insurers.

Insurance Solutions to Data Breach Risk

In the final analysis, the incidence of data breach is as much a people and processes issue as a technology issue. No organization can ultimately make itself invulnerable to the actions of a malicious insider with trusted access, either as an employee or an employee of a key vendor.

Beyond internal risk management, there is now an increasing array of cyber insurance solutions available in the U.S., London and European insurance markets that can help offset some of the specific costs of a data breach. This is an evolving area of policy development – and no two policy documents speak exactly the same language, but it is certainly possible to find appropriate quality coverage for the full range of risks you may face in this area now, whether you are domiciled in the U.S. or Europe. Underwriters have experience in paying claims and the wordings have evolved to address voluntary notification, and not just the legal obligation to notify.

London-based underwriters in particular have been proactive in developing covers against reputation harm and first-party network business interruption caused by viruses, denial of service attacks, administrative and operational mistakes.

For clients who are service providers, vendors, business associates and the like, Lockton has worked extensively with the insurance marketplace to provide coverage for contractual indemnification for notification costs of customers, as well as other damages emanating from the contract. We have effectively tailored the data collector/data owner policies to cover the vicarious liability from functions or services performed by independent contractors and business associates.

With growing unease over the emerging issue of cyber extortion, cover is also available against such things as threats to your data or your network with ransom demands attached.

Another key element is the limits for notification costs/crisis management and regulatory defense/payment of a civil fine or penalty arising from a data breach have increased substantially in the last few years with increasing primary limits and ability of the excess insurers to provide additional capacity for sublimits exhausted in the primary policy.

Conclusion

Lockton is one of the leading authorities and innovators in the field of data breach and cyber liability. We design insurance programs for both first-party risks (direct business interruption and extra expense associated with a breach or outage) and third-party liability on an integrated basis with other risks where possible (for example, combined with technology and miscellaneous professional liability) or on a stand-alone basis.

We have developed unique line slips as well as specific wordings with underwriters amending their standard forms. We have insurance coverage to address reputational harm from a third-party data breach and also work closely with our clients to help them understand the underlying risks, relevant claims and regulatory environment.

We can provide valuable benchmarking information to assist in discussions about limits and retentions. As there are no standard industry wordings, we highlight the differences in various policy forms and have authored a number of manuscript changes to broaden the industry versions to better suit our clients' needs. We assist our clients in preparing the necessary underwriting information to upgrade insurance or purchase insurance in areas where the client policies are not adequate.

Finally, we can assist in developing data breach contingency plans or coordinate with data breach expert panels developed by individual insurers or in concert with Lockton.

If you would like to discuss any of the issues raised in this white paper or any other data protection risk management concerns, please advise your client team or the authors.

About Lockton

More than 3,800 professionals at Lockton provide more than 15,000 clients around the world with insurance, benefits, and risk management services, offering an uncommon level of client service. From its founding in 1966 in Kansas City, Missouri, USA, Lockton has grown to become the largest privately held insurance broker in the world and 9th largest overall. Business Insurance recognized Lockton as a "Best Place to Work in Insurance."

LOCKTON®

www.lockton.com