Thinkpiece

Number 108 July 2014

INDEPENDENTLY PROMOTING DEBATE AND FRESH THINKING IN THE FINANCIAL SERVICES INDUSTRY

Data Breach: Why Should We Care?

Paul Bantick
Team Leader, Technology, Media and Business Services,
Beazley Group

Summary

- Data breach is a phenomenon that every company that holds customer or sensitive personal information will experience – simply put, it is not a question of 'if' but 'when.'
- Data breaches take many forms and many cannot be planned for.
- The potential insurance market for this business is massive – as demonstrated by the rapid growth of data breach insurance in the US. New EU-wide data privacy legislation is due to be passed in the next year and will bring with it punitive measures for firms mishandling data. This will force companies to inform clients of any data breach – no matter how big or small. These regulations could to be a game changer in terms of insurance penetration.
- There are a number of insurers moving into this market, but not all policies are alike.
- There is confusion among clients as to what protection they have in existing policies – and they are looking to their brokers for advice.
- The unfamiliar risks, the service concept within many policies, even non-standard language of the cover all put a premium on education.
- Brokers need to understand the policies, clients need to know the facts, and insurers need to provide the services required to get a business back on its feet – and that is much more than just handing out a cheque when a valid claim occurs.

The Chartered Insurance Institute is the world's largest professional body for insurance and financial services and is the leader in awarding qualifications to industry practitioners. Our Thinkpieces are a key part of our ongoing commitment to promoting innovative thinking and debate within the insurance and financial sectors.

CII Introduction: cyber liability is one of those words that means many things to different people. For some it is about foreign governments spying on other governments or on corporations, for others it is criminals targeting individuals, or companies having their systems compromised. However, a key aspect to all of these risks is the loss of data. In this Thinkpiece, Paul Bantick, Team Leader of Technology and Media Services at Beazley Group focuses on data breaches and their implications.

What is a data breach?

A data breach usually involves financial information such as credit card or bank details, personal health or personally identifiable information, trade secrets or intellectual property being stolen or lost. Essentially it is any incident in which sensitive, protected or confidential data is potentially copied, transmitted, viewed, stolen or used by an individual who is not authorised to do so.

Many—and among the most expensive—instances derive from determined and often persistent attacks by external hackers. The sheer volume of personal information being stored means that perfect data security is not possible.

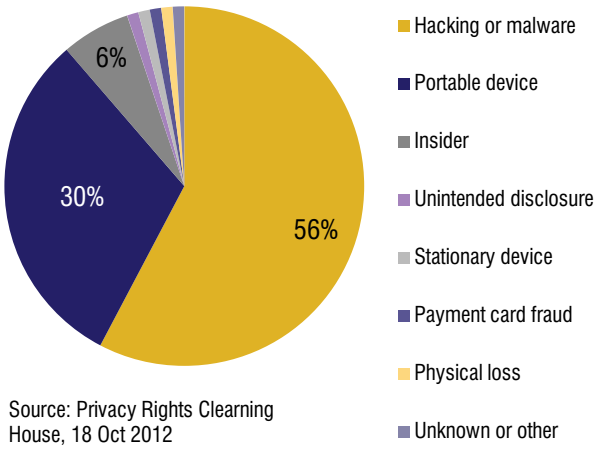
Data breaches may include the theft of digital media such as computer tapes, hard drives or electronic data files. Or it can be caused by something as simple as someone carelessly leaving a laptop on a train with un-encrypted sensitive data on it, or not storing hard copy records securely.

The problem for companies is that the causes of data breaches are extremely diverse. Many—and among the most expensive—instances derive from determined and often persistent attacks by external hackers. The sheer volume of personal information being stored means that perfect data security is not possible.

In many sectors such as: retail, healthcare, banking and hospitality, that hold significant quantities of customer personal data, data breaches are not just a once in a lifetime event, but a constant risk of doing business.

A quick look at recent statistics reveals the size of the problem. According to Experian, in the first half of 2012, 19.7m[1] pieces of data were traded illegally online, and the Ponemon Institute estimates that the cost of data breach to UK businesses is around £1bn[2] a year. The Privacy Rights Clearinghouse[3] revealed that 56% of data breaches last year came from hacking or malware, while nearly a third were from lost portable devices such as laptops and smart phones.

Figure 1: Where do data breaches come from?



Source: Privacy Rights Clearning House, 18 Oct 2012

What damage can a data breach do?

To date the financial impact in Europe has been less serious, because there is currently only data breach reporting requirements in a few European countries. In the UK, the Information Commissioner's Office has the powers to impose fines on companies not thought to be adequately protecting client data.The FCA has a track record of fining financial institutions millions of pounds if they are deemed to have put customers' data at risk. But there currently is no mandatory client notification requirement.

However, there are plans in the European Union to impose EU-wide data protection legislation. In January 2013, the European Justice Commissioner,

[1] Experian: www.experian.co.uk

[2] Symantec and Ponemon Institute – 2013 Cost of a Data Breach Study, United Kingdom: www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-uk-report-2013.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2013Jun_worldwide_CostofaDataBreach

[3] The Privacy Rights Clearinghouse: www.privacyrights.org

Viviane Reding unveiled far-reaching proposals for revising the EU's 17 year-old data protection laws. Under the new legislation, which is due to become law in 2015, safeguarding against a breach will place a considerable burden on businesses in a broad range of sectors.

Then on the 21 October last year, the Civil Liberties Committee took the proposed legislation one step further. They wanted to include an explicit consent requirement, a right for individuals to insist on the erasure of personal data (the so-called "right to be forgotten"), and bigger fines for breaking the rules: up to €100m or up to 5% of a company's annual worldwide turnover, whichever is greatest.

However, the financial impact could be the least of a company's worries. Even law suits and regulatory fines can seem trivial compared to the loss of customer trust. Our insureds say that their number one concern is reputational damage. As Warren Buffett famously said: "It takes 20 years to build a reputation and five minutes to ruin it."

Our insureds say that their number one concern is reputational damage. As Warren Buffett famously said: "It takes 20 years to build a reputation and five minutes to ruin it."

In a study undertaken by the Economist Intelligence Unit last year, a quarter of respondents said they had been the victim of a data breach in the past two years. Of those, 38% said they no longer did business with the organisation because of the data breach.

Prevention is not enough

Data breaches are happening all the time and on a very large scale. In the US, in the healthcare sector alone, 21,000 letters are mailed out on average every week to individuals whose personal information has been compromised through data breaches. Companies need to plan for an inevitable data breach. So the question C-suite executives should be asking themselves is not: "can it happen?" But:"how will we respond?" When it does.

It is not surprising that the demand for insurance against a data breach is growing rapidly. According to one of the big three brokers, the number of their clients buying data breach insurance rose 33% from 2011 to 2012. Demand is coming from businesses of all sizes and across a range of industries.

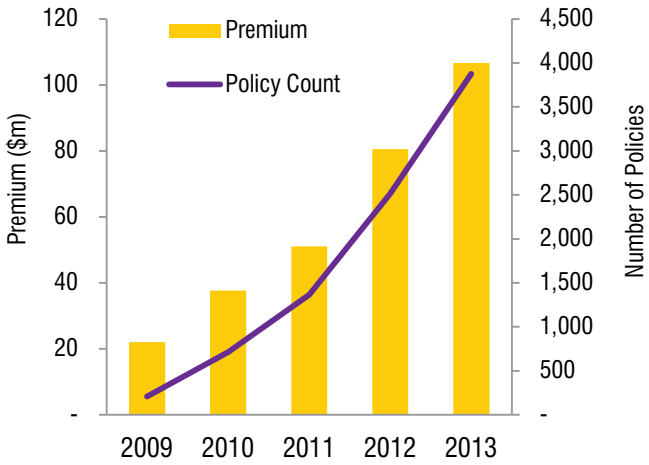
Larger companies, although often equipped with more substantial risk management and legal departments, can face significant costs because of the sheer volume of data that they hold.

Larger companies, although often equipped with more substantial risk management and legal departments, can face significant costs because of the sheer volume of data that they hold. Small and midsize businesses are also good candidates for data breach insurance, because they are likely to be less prepared for a data breach and less able to absorb the costs associated with it.

How is the insurance market responding?

Estimates of the value of the size of this market vary between $400m and $800m. At Beazley, we started writing this business in 2009. Over the past three years we have seen demand surge by 365%, with the largest market by far currently being in the US.

Figure 2: Standalone cyber & data liability insurance: premium and policy count



The development of the US market is an interesting example of what drives demand. The first step was the client notification statutes, which began in California in 2001 and now exist in 48 States. These regulations require companies to inform customers of

every data breach, no matter how large or small. This was a genuine market game changer.

With disclosure came potential legal exposure following breaches, and it became clear that dealing with data breaches was both complex and expensive. More recently, class action lawyers have become very aggressive following data breaches, and expensive litigation is now common. Regulators also have become more active, and are keen to show their teeth by imposing punitive fines on companies.

All of this has driven both demand and the development of insurance products because the exposures have become better defined and apparent.

There are now approximately 25 insurers offering data protection insurance, the market is very dynamic and the coverage available varies from insurer to insurer. However, all these carriers offer coverage for both first-party and third-party losses.

When the EU rules change and mandatory notification of all data breaches, and punitive fines for mishandling client data become law, this will force clients to take these risks seriously. It will increase demand for cover, and impact pricing and wordings.

First-party coverage protects companies against the often very heavy costs of responding to a data breach. This is really a new frontier in insurance. Many insurers simply offer a sum of money to cover these costs, but a few actually arrange for the provision of the services themselves from carefully vetted and approved specialist service providers. Third-party coverage insures for the liability of the policyholder to third parties—including clients and governmental entities—who might bring legal actions against the insured arising from a data breach or cyber attack.

London and the Lloyd's market are currently leading markets for data breach insurance, and there is ample capacity. However, when the EU rules change and mandatory notification of all data breaches, and punitive fines for mishandling client data become law, this will force clients to take these risks seriously. It is likely to increase demand for cover significantly, and this could have an impact on pricing and wordings.

Product development

We have learnt a lot from our clients in the US, where the data breach insurance market is much more mature. We have found that most clients want two things:

- Financial compensation to cover the costs of responding to a breach, and
- Access to help in responding to the breach.

The first element is the simplest part of the product, but the response element is the key.

Many clients feel they can manage a breach on their own. Others want some assistance and some want a carrier to shoulder most of the responsibility. A data breach is not a time to be learning on the job. Time is critical and broadly companies want expert partners, who've been there before – preferably numerous times.

Due to the complexity of a data breach, and the range of specialist assistance required instantly by an insured, we devised a service-led solution to provide clients with more than just financial assistance in the event of a breach. We have put together a total package in which we find, supply and pay for specialised lawyers, IT experts, a PR team, notification networks and, if needed, credit monitoring services.

This approach has proved invaluable to clients, especially those without sophisticated risk management teams. We help the client to determine what has been compromised, assess their responsibility, notify the right people and do what is necessary to get the business back on its feet again.

We also pay third party losses from law suits and in some instances regulatory judgments. But the key is that if you get the service right, the third party losses should be much more manageable. Evidence also suggests that companies that handle a breach efficiently and effectively can come out of the

experience with their reputation intact - and in some instances even enhanced.

The other good news is that data breach policies do not have to cost the earth. The price will depend on a number of factors including: the size of revenue, the spread of the insured's international business and whether or not insurers deem the insured to be a good risk or not.

What is a good risk?

Insurers are keen to see is evidence that risk management for data breach is embedded in the company's policies and procedures, and that it is a board responsibility. Some companies solely rely on the IT department for data protection risk management, but no matter how many firewalls a company has, or how good its IT-systems are, no set of controls can guarantee that they won't have a data breach. What we look for is a company that takes data security seriously at a board level, and which plans and prepares for a breach.

Some companies solely rely on the IT department for data protection risk management. But no matter how many firewalls a company has, or how good its IT-systems are, no set of controls can guarantee against a data breach

Also companies often tend to forget that good internal risk controls will not help when client data is stored with an outsourced data processing company or a cloud service provider. Even though these external companies hold the data, the security of the data remains the responsibility of the 'data owner' company, both in the eyes of the law and customers. So it is very important that the security procedures of these companies are well-scrutinised before allowing customer data to be held by them.

What can the insurance industry do to help companies?

Risk managers and company directors have a new and pressing need for information. And that, in turn, means they have new, compelling reasons to consult their brokers.

But breach response insurance is not an ordinary coverage – the unfamiliar risks, the service concept, even the non-standard language put a premium on education. Brokers need to know the details; and customers need to know the facts. Customers are confused about breach response; they don't know what they don't know.

Breach response insurance is still developing. The scope of coverage available and the cost can vary significantly from insurer to insurer. When you are evaluating risks in this area, understanding the specifics from data losses and the scope of coverage offered under data breach policies is vital. A team approach with the underwriter, broker and any technical experts will ensure that the right coverage with appropriate terms and conditions is bought.

When talking about what a company needs, it is worth thinking about the following issues:

1. What are the risks?

For some businesses, like banks and retailers, the primary concern is the theft of personal financial information. For an energy company, it might be the disruption through an attack on a network, and coverage should be tailored to the risks they face.

2. What insurance do they already have in place?

Some company's standard first- and third-party liability policies may provide some protection from cyber and data risks, and it is important to understand what coverage, if any, may be available under their existing policies.

3. What are the basics?

Consider whether all the cover being offered is required, and carefully review the exclusions or limitations in the policy.

4. What are the right limits and sub-limits?

It is important to assess the value of the policy compared to the anticipated costs associated with a data loss, which can be substantial. Clients need to match their limits of liability with a realistic exposure in the event of a data loss. Also, cyber/data policies

can impose sub-limits on some covers, such as for crisis management expenses, notification costs and regulatory investigation, so be prepared to review and negotiate.

5. What are the exclusions?

Policy language is not standardised, and policies may contain exclusions that have been cut and pasted from other insurance forms, which may not be appropriate.

6. Consider the actions of third parties

Many companies outsource data processing or storage to a third-party vendor, so their policy should provide cover for claims that arise from failure by an external data handler.

7. Review protection against regulatory actions

Loss of data could also result in regulatory actions against the company. Any data breach policy should provide coverage for a regulatory investigation or a regulatory action arising from a data breach.

8. Prevention is better than cure

Some insureds need specialist risk management services, and these are ideal clients to work with a carrier that offers a robust service-led programme.

9. What are the triggers?

Some policies are triggered on the date the loss occurs, while others are triggered on the date that a claim is made against the insured. In order to provide proper notice, it is important to understand how coverage applies under the policy.

10. Think about unencrypted devices

While company-owned laptops are encrypted, personally owned computers and storage devices are not, and if firms allow home-working, it is important they buy insurance that provides coverage for losses from personal computers

The bottom line is: clients need to understand that that it is not a case of "when" but "if" a data breach will happen. However, a data breach doesn't have to be a disaster, but mishandling will be.

If you have any questions or comments about this Thinkpiece, and/or would like to be added to a mailing list to receive new articles by email, please contact us: thinkpiece@cii.co.uk or by telephone: +44 (0)20 7417 4783.

Paul Bantick is the team leader for technology, media and business services at Beazley. He pioneered the development of Beazley's data breach insurance offering and has extensive experience in underwriting these exposures for healthcare accounts, retailers and other businesses. Paul sits on a UK Government cyber/data risks advisory panel.

Beazley plc (BEZ.L), is a market leader in many of its chosen lines, which include professional indemnity, property, marine, reinsurance, accident and life, and political risks and contingency business. It is the parent company of specialist insurance businesses with operations in Europe, the US, Asia and Australia. Beazley manages five Lloyd's syndicates and, in 2012, underwrote gross premiums worldwide of $1,895.9 million. All Lloyd's syndicates are rated A by A.M. Best.

As the leading professional body for the insurance and financial services sector with over 117,000 members in more than 150 countries, **the CII Group** is committed to protecting the public interest by guiding practitioners in the sector towards higher technical and ethical standards. We do this by offering them a broad portfolio of services and support, including membership, qualifications, continuing professional development, thought-leadership, lobbying and the maintenance of a benchmark Code of Ethics. Please see our website: www.cii.co.uk.

The CII/PFS Thinkpiece Series

The Thinkpiece series consists of short 1,500–2,500-word articles on subjects of interest to the insurance and financial services profession and stakeholders, and are written by a range of contributors. We publish them *not because we necessarily agree with the views* (or believe that they reflect in any way the policy of the CII or its members), but *to promote a free and open debate*.

All articles are freely and openly available on our website: www.cii.co.uk/thinkpiece. If you wish to be added to a mailing list to receive new articles by email, please contact us at thinkpiece@cii.co.uk

Recent articles in the series:

No.107: **Stop! Clean your hands! And think afresh... a social marketing perspective on treating customers fairly**, by Judith Cork, Business Ethics Consultant (July 2014)

No.106: **Ethics and economic growth: Preventing culture from going south as profits head north**, by Martin Wheatley, Chief Executive, Financial Conduct Authority (March)

No.105: **Are Baby Boomers Really the Generation That Has it All? Stark Realities for Resilience in Retirement**, by Tony Stenning, Head of UK Retail, BlackRock (March)

No.104: **New Approaches to Risk Management in the Twenty-First Century: Four Big Areas**, by Andrew Kendrick, President, ACE Group (March).

No.103: **Public Perception and the Professions: from Deference to Partnership?** by Sue Carette (November 2013).

No.102: **Scottish Independence: Dramatic Change or More of the Same?** by Alasdair Matheson and Charles Livingstone, Solicitors, Brodies LLP (October).

No.101: **Keeping the Lights On: Energy Security in the 21st century**, by Edward Russell-Walling (October).

No.100: **Product Intervention in Financial Regulation: Keeping the Customer's Interests at Heart**, by Chris Woolard, Director of Policy, Risk and Research, FCA (September).

No.99: **Success in the New World: Business Efficiency in the Post-RDR Financial Advice Sector**, by Tim Hines and Nick Siddle, Optimus Consulting (August).

No.98: **Can a Leopard Change its Spots? 'Repurposing' UK Conduct Regulation**, by Richard Hobbs, Director, Lansons Public Affairs (June).

No.97: **Managing the New Normal: Five Facts and Five "Do's" and "Don'ts" for Sustainable Underwriting**, by Andrew Kendrick, President, ACE European Group (June).

No.96: **The Great British PPI Truth and Reconciliation Scandal: Outcomes and Lessons**, by Teresa Perchard, former Director of Policy & Advocacy, Citizens Advice (June).

No.95: **Supporting Strategic Objectives or Another Compliance Exercise? Understanding Corporate Risk Culture in Insurance**, by Simon Ashby, Tomaso Palermo, and Michael Power, Centre for Analysis of Risk & Regulation, London School of Economics (May).

CPD Reflective Questions

Reading this Thinkpiece can count towards Structured CPD under the CII CPD Scheme, if you consider any of the Learning Objectives below to be relevant to your professional development needs. The Reflective Questions are designed to help you reflect on the issues raised in the article. Please note that the answers to the questions are not required for CPD records purposes.

Learning Objectives

- To understand the challenges posed by data breaches threat to major business, and the importance of insurance sector responses.
- To be able to summarise the different forms of data breach and damage this can entail.

Reflective Questions

- What are the major sources of data breaches, and other key pointers can you identify which would improve the success of the fictional campaign?
- Describe some of the recent legislative and regulatory changes in relation to protecting data. What do you think is the overall direction of travel for data breach regulation? Do you think the insurance industry is doing enough to prepare for this?
- What are the main lessons learnt from the development of the cyber and data liability market in the United States? What do you think are the central tenets to its growth in the UK?
- The author sets out an aide memoire of ten issues that an insurer should be thinking about when considering a company's needs. Can you add to this list?