info security
STRATEGY /// INSIGHT /// TECHNIQUE

September/October 2012

Data Breach Insurance: Underwriting your Liabilities

by Wendy M. Grossman

As high-profile data loss incidents become commonplace, Wendy M. Grossman examines the nascent field of data breach insurance aiming to hedge against the risks

Whenever Bridget Treacy, a data privacy expert and managing partner of the London office of law firm Hunton and Williams, speaks in front of groups, she likes to challenge them with: “Hands up if you’ve had a data breach incident in the last 12 months.” On average, she says, about 25% raise their hands. Here’s what she tells the rest of them: “You may not be looking in the right place.”

This lack of awareness can be expensive. The direct costs of a data breach may include forensic examination, system remediation, employee training, legal action (particularly in the US), and regulatory fines. Indirect costs include reputational damage and customer churn through loss of trust. On top of these are notification costs, legally required in most US states since California began the trend in 2003, and likely to form part of the EU’s data protection reform package when it’s passed in the next couple of years.

The upshot of all these costs – particularly in the wake of laws requiring notification – is the development of a market for data breach insurance. As Daljitt Barn, strategic account director for risk management specialist NCC Group, explains: “It’s already quite a known insurance line in the US. The UK is leading the EU, even though we’re not quite there yet with EU law.”

Symantec’s 2011 report on data breaches, conducted by the Ponemon Institute, provides more detail on the cost of data breaches worldwide. The most expensive location – partly because of litigation and partly because of notification requirements – is the US, at $194 per compromised record, slightly down from 2010; the UK comes in somewhat lower, at $124.

The report also estimates that the cost of lost business following a data breach was $3 million in the US, and the average total organizational cost of a data breach was $5.5 million in the US, while clocking in at $2.7 million in the UK. The average size of a data breach was between 20,000 to 30,000 records, depending on the country. Small wonder that increasingly in the US – and just beginning in the UK – companies are looking at insurance to lay off these risks.

A Local Flavor

A key difference between the US and EU approaches, says Treacy, is that US data breach notification statutes grew out of consumer protection law. In Europe, it has developed from data protection law. Organizations need to be aware of both approaches, however, if they have overseas subsidiaries or do business with international partners.

In some cases, forensics and remediation for larger companies with serious infrastructure issues can run as high as $6 million, says Matthew Hogg, vice president of Liberty International Underwriters. "Plus notification costs, PCI fines, reimbursement of credit card charges, lawyers' draft letters, call centers, and opening yourself to litigation", he adds. "One of the larger breaches in the US in 2011 has 10 class-action suits filed against it."

He notes, however, that a lot depends on the kind of organization that suffers the breach: a retailer may hold a lot of financial information provided by its customers, but if the attraction is quality clothes at a decent price, then the breach may not do much damage. The loss of trust in a credit card processing company that has a breach, conversely, could be highly damaging. In addition, smaller businesses may be the most vulnerable, because they typically lack the IT departments, security personnel, and budgets available to larger organizations.

The Tipping Point

Hogg's company is one of the early members of the months-old Cyber Risk Insurance Forum, set up by NCC Group to create a framework of security practices and procedures for companies wishing to take out cyber insurance – including the latest addition, data breach insurance. Part of the immediate stimulus was 2011's "summer of hacking", NCC's Barn says: "LulzSec, Anonymous, targeting corporations, banks, and enterprises."

At that point, it seemed necessary to enable the exchange of information so insurance companies could help each other assess what the risks were. The insurance industry, says Barn, who worked in security for 15 years, "sees the claims, what's happening, where, and what's gone wrong. We'd like to pass on the benefits of that knowledge to our insurers."

One of the stumbling blocks to wider acceptance is IT departments, which have typically balked at the idea of purchasing data breach insurance, says Ben Beeson, a partner in Lockton's technology and global privacy practice.

"In the US for a long time we struggled to get this past the IT department, who viewed insurance as an insult to them", Beeson reflects. "It's definitely no longer the case – they now understand that there's always going to be a residual risk. You need to get the right things in terms of contracts, intrusion detection systems, and encryption – but you can still get hit. It's also become a boardroom risk in the US, not least because of what the Securities and Exchange Commission [SEC] is saying about listing cyber risks when you file reports."

In the UK, he adds, this same consciousness hasn't yet taken hold; too often managers still see the risk of data breaches as an IT problem that can be solved with money and technology. "They're not understanding that this is an enterprise-wide risk", Beeson observes.

Barn agrees. "It's always a challenge when you run the security function to get more resources or funding within the business."

In addition, as Hogg says, it's a new product that businesses aren't used to purchasing. "Any number seems like a high premium", he relays.

Data's Toxic Effects

It's no wonder that the former UK Information Commissioner, Richard Thomas, has called personal data a "toxic liability" and William Heath, the founder of Mydex, a company aimed at providing consumers with the facilities to manage their own data, favors data minimization.

Steve Eckersley, the ICO's head of enforcement, says that in the absence of mandatory reporting requirements, his office gets news of data breaches in many different ways: whistleblowers, media reports, complaints from consumers or third-party advocacy groups.

"We are always scanning the horizon to be alert to a significant data security breach", he says. Once a breach is discovered, a team investigates the circumstances and gathers evidence to establish whether a fine is appropriate. Since being granted the power to impose monetary penalties in April 2011, most of the organizations the ICO has fined have been healthcare-related organizations, usually because of human error associated with lack of clear policies or direction, or lack of training. "We have had recent cases", Eckersley recalls, "where patient files were found in a disused hospital premises".

As for commercial companies, so far, the ICO has fined only three: Welcome Financial Service (£150,000), A4e Limited (£60,000), and ACS:Law (£1,000, as the firm had ceased trading by the time the investigation was complete).

Most policies, Beeson says, typically include the aforementioned direct costs, though he notes that in the UK fines imposed by regulators such as the Information Commissioner's Office or the Financial Services Authority – the only two UK agencies that can impose such fines – are not insurable. By contrast, in the US, fines under the Health Information Portability and Accountability Act (HIPAA) or imposed by the Federal Trade Commission (FTC) can be covered.

Hedging Against Risk

Beeson's earlier point – that you can do everything right and still get hit – becomes clearer when you pick out some other pieces of the 2011 Symantec-Ponemon report: the most frequent causes of data breaches are negligent employees and malicious attacks. The IT department can do everything right and still be undermined by the employee whose work laptop is stolen from his home while he's on vacation, or data that should be protected is in the hands of a business partner.

Another issue that Hogg highlights is the importance of the network, even to businesses that think of themselves as resolutely bricks and mortar. "For example, the just-in-time models of the last 10 years depend on a highly sophisticated IT infrastructure. But people think it only matters when they're an online business."

One complication is that because this type of insurance is so new – and because it often forms part of cyber insurance, which can cover anything from malicious attacks and cyber extortion to notification costs and credit card reimbursements – policies vary a great deal. Typically, both because of the relative immaturity of the field and because of the complexity of these policies, organizations will buy through a broker who knows the field and can also examine what other coverage the organization has and identify any gaps.

Ultimately, Hogg says, it’s still up to the organization to do as much as it can to secure its systems. “Then we take the residual risk as the insurer.”

Unlike many types of insurance, this simply isn't a commoditized product. “One of the tough things”, notes Hogg, “and why a broker is still relevant, is that none of the wordings [are] the same. They cover the same things, but the nuances and wordings are different. Some only provide business interruption cover if there’s been a malicious event. Others say that’s half the story: What if there’s an administrative mistake or an operational error by employees?” He sums up the overall market in closing: “There are a lot of details to getting the best coverage.”