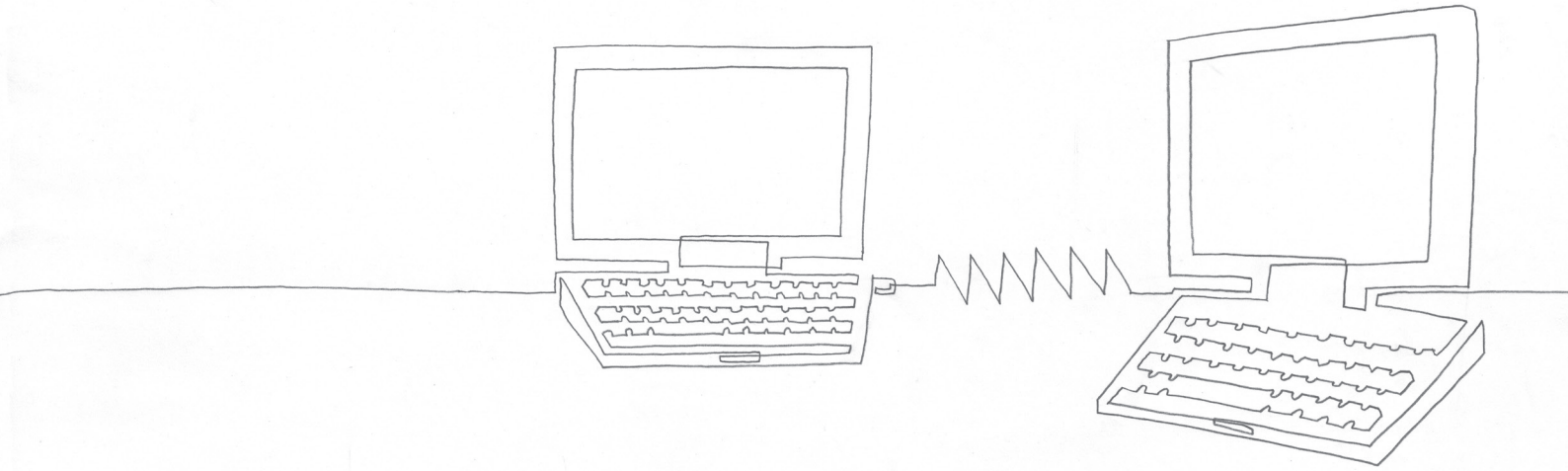
# Beazley Breach Response
## A Proven Solution for Data Breach Events



# Beazley Breach Response
## A Proven Solution for Data Breach Events

**Beazley Breach Response, a unique services-based data breach insurance offering, now protects over five hundred organizations. Since the launch of Beazley Breach Response in 2009, Beazley's breach response team has helped our clients handle many dozens of data breach events successfully.**

Data breaches take many forms. Some derive from external hackers; others from malicious insiders. A third – and surprisingly large category – derives from simple carelessness.

Many pose a real threat to the individuals whose personally identifiable data has been lost or stolen. Others prove on investigation to be false alarms, but the forensic costs of establishing this can be high. Industry characteristics are critical too – a loss of medical records from a hospital poses different risks from a loss of credit card information from a retailer.

In each case we work closely with our insured to establish the best response that is tailored to their individual needs.

Examples from the dozens of breaches recently handled by our breach response teams include:

- When a healthcare insured was the victim of a rogue employee who stole the personal health information of several patients and used that stolen information to fill forged narcotics prescriptions, Beazley assisted the insured with retaining expert legal counsel and coordinating with local and federal law enforcement. Notification letters were mailed to the affected patient group, offering credit monitoring and identity fraud resolution services.
- Forensic services were immediately required when a financial institution experienced a network hacking incident. Given the possibility, albeit remote, that sensitive client information was accessed, including Social Security numbers and financial account details, the decision was made to issue notification letters offering credit monitoring services.
- A university suffered a data breach when a laptop containing payroll and other personally identifiable information for over 10,000 employees was stolen from a car. Over 30% of the affected employee group enrolled in credit monitoring services, which were offered by Beazley at no cost to the insured.

For more information go to **www.beazley.com/breachresponse**

- An exhaustive forensic examination of a healthcare provider's network after a possible malware event determined that no personal health information or personally identifiable information was accessed, requiring no further action or notification by the insured. Beazley paid over $175,000 in forensic expenses in excess of the insured's $20,000 retention.
- A non-profit discovered a vengeful employee had been secretly removing active paper files containing personally identifiable information from the office and disposing of them in a local dumpster. Beazley worked with the insured as it completed a manual review to determine the missing group of files and identify the impacted individuals. Expert legal counsel advised the insured on its notification requirements, as the impacted individuals resided throughout multiple states and Canada.
- After a computer containing personal health information of over 500,000 patients was stolen from a hospital, Beazley guided the insured through a comprehensive response, including the immediate retention of an external crisis management firm and issuance of notification letters to the over 500,000 impacted individuals, at a substantial cost covered by Beazley in excess of the insured's low retention.
- After a healthcare provider discovered an employee's theft of information, forensics were able to limit the impact of an information theft to a single database, ruling out two other databases and reducing the group of potentially impacted individuals from about 750,000 to under 15,000.
- When a managed care organization had numerous hard drives stolen from an offsite storage facility, Beazley paid $2 million towards forensics and notification costs.

As can be seen from the above, responding to a breach can be complicated and costly. Working with our experienced team, an organization is guided through and empowered with the resources it needs to implement a sound and strategic breach response plan.

## Breach services offered through Beazley Breach Response

Breach services include notification for up to 4,000,000 individuals; legal representation; expert forensic services; credit monitoring; crisis management; and fraud and healthcare record resolution services. Both internal and external expert resources ensure that our insureds are provided with timely information so they can make informed decisions on how to respond to breaches, comply with legal obligations, and minimize potential reputational damage.

CBSL204_US/UK_10/11

## Beazley Group

Plantation Place South
60 Great Tower Street
London EC3R 5AD
United Kingdom

T +44 (0)20 7667 0623
F +44 (0)20 7674 7100

## Beazley Group

30 Batterson Park Road
Farmington, CT 06032
USA

T +1 (860) 677 3700
F +1 (860) 679 0247

## Beazley Insurance Services

101 California Street
Suite 1850
San Francisco, CA 94111
USA
CA Lic. #0G55497

T +1 (415) 263 4040
F +1 (415) 263 4099

# Every breach is different.

The strange and disturbing world of data breaches

# A world of risk

Data breach risk is the product of two trends:

The proliferation of data exchanged within and between organizations. Much of this is personally identifiable information, which in the wrong hands can give rise to identity theft or to other forms of financial or reputational harm.

The proliferation of regulation. A host of state and federal regulations have come into force in recent years to protect individuals in the event that private information concerning them is lost or stolen.

Bring these two trends together and the result is a massive increase in the number of data breaches that are reported to affected individuals. Take healthcare. Until 2009 there was no federal requirement for healthcare providers to notify affected individuals of the loss or theft of personal health information. In 2010 alone, this new obligation resulted in nearly 15,000 healthcare data breach notifications being mailed out, on average, every day.

## Expect the unexpected

For businesses, a particular challenge of data breaches is that they can come from almost any angle. Take the incident depicted on the cover of this brochure. In April 2012, the *Boston Globe* reported that a local hospital had notified 6,831 patients that their billing information – including credit card numbers and security codes – could have been compromised after paper records were found blowing through a field in Charlestown, several miles from the hospital.

Data breaches take myriad forms. According to the largest database in existence, a record of publicly disclosed breaches in the US affecting more than half a billion personal records maintained by the Privacy Right Clearinghouse (*www.privacyrights.org*), the biggest single cause by number of records breached (56%) is hacking or malware attacks.

Clearly in such cases the risk of identity fraud is far higher than when data is simply mislaid: it is already by definition "in the wrong hands."

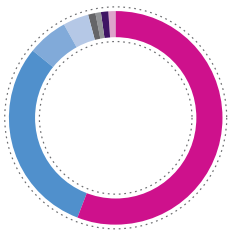
The second largest cause of breaches, according to the PRC database, is from the loss or theft of personal devices, such as laptops, PDAs, smartphones or memory sticks. This accounts for 30% of the breached records on the database.

The third biggest cause of breaches, representing 6% of the records held on the PRC database, is insiders – individuals with legitimate access who intentionally breach personal information. Although 6% may not seem a large slice of the pie, the vast size of the PRC database means that it still accounts for nearly 340 million records.

## The biggest risk

But for many organizations, the biggest risk does not come from hackers. It does not come from the breach itself at all. It comes from the organization mishandling its response to the breach – and thereby forfeiting the confidence and trust of customers and other stakeholders. What is really at stake in a data breach – particularly a large scale data breach – is reputation.

## Records breached



Total
563.9 million
Since 2005

*Source:* Privacy Rights Clearinghouse, 10/18/2012

| | |
|---|---|
| **Hacking or malware** – Electronic entry by an outside party | 56% |
| **Portable device** – Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc | 30% |
| **Insider** – Someone with legitimate access intentionally breaches information – such as an employee or contractor | 6% |
| **Unintended disclosure** – Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax or mail | 4% |
| **Stationary device** – Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility | 1% |
| **Payment card fraud** – Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices | 1% |
| **Physical loss** – Lost, discarded or stolen non-electronic records, such as paper documents | 1% |
| **Unknown or other** | 1% |

March 2012. Data cartridges containing 800,000 social security records are lost in transit

# Our experience

Experience is critical in many lines of insurance, but in none more so than in tackling data breach risk. In 2012 alone we helped clients manage more than 350 real and suspected data breaches.

In 2012 we also established BBR Services, a business unit dedicated to helping clients that have suffered a data breach manage the consequences swiftly and effectively. BBR Services is responsible for the seamless provision of all the response services a BBR policyholder may require following a data breach.

Claims are a moment of truth in the relationship between insurer and policyholder. When an insurer has a high client retention rate, it indicates that it is charging a fair price and is providing good claims service. Retention rates vary across lines of business, but most insurers would regard a 90% retention rate for most lines of business as very good. Since we launched Beazley Breach Response in July 2009, our annual client retention rate has exceeded 95%.

The data breaches we handle are extremely diverse. Many – and among the most expensive – derive from determined and often persistent attacks by external hackers. Others derive from insiders motivated either by the prospect of financial gain or a desire to take revenge for real or imagined grievances. Finally, the capacity of human beings to make simple mistakes – such as sending an email to the wrong address or losing a laptop or a flashdrive - is almost limitless. And in a world awash with personal data that is subject to extensive regulation, these mistakes can prove very costly – even if the data does not fall into the wrong hands.

Data breaches present a major challenge for organizations because they are both infrequent and complex events. Beazley has been helping clients manage these events since 2007, when the market for cyber liability insurance was in its infancy.

# How we help

Beazley has helped clients handle more than 500 data breaches, including many involving hundreds of thousands of records. Our service is designed to meet three critical needs: speed, thoroughness, and coordination:

## Speed

*"I read about it in the press before I heard about it from you,"* is not something you ever want to hear.

## Thoroughness

Balancing the need for speed is a need for thoroughness in investigating the causes of the breach and in determining an appropriate course of action. A number of organizations have rushed to notify thousands of customers of a data breach, only to discover afterwards that no data actually escaped.

## Coordination

A data breach can only be successfully managed through smooth coordination among a number of parties. A little like a relay race, there is a risk of the baton being dropped at each handover.

### 1.

The insured registers at **www.nodatabreach.com** an online information security and privacy information service.

**Purchase Beazley Breach Response policy with coverage for up to five million notified individuals.**

### 2.

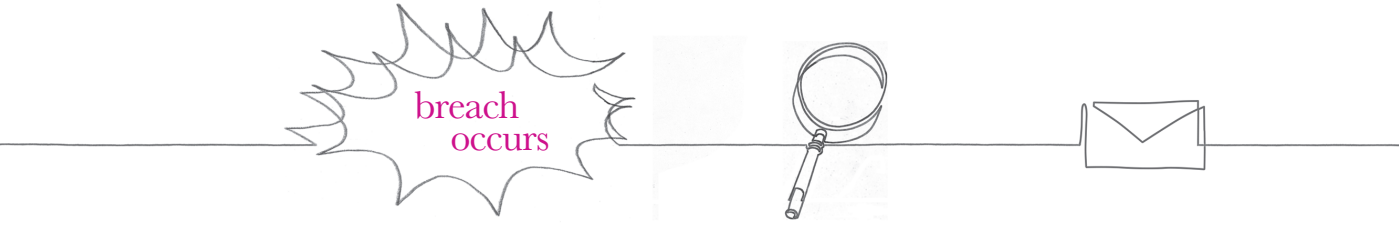
Notification to Beazley claims office via phone or email:
+1 866 567 8570
bbrclaims@beazley.com

### 3.

An attorney from BBR Services, our dedicated unit focused on helping clients manage breaches successfully, contacts the insured. He or she will help the insured select a lawyer with expertise on applicable laws and regulations and, if needed, a forensic expert able to investigate and report on the scope of the breach. An action plan is drawn up.

### 4.

The insured, with advice from legal counsel and continuing guidance from BBR Services, decides whether and to what extent notification is required. If notification is required, a notification service provider is chosen to mail out notifications in line with applicable regulations.



Data breaches – or suspected data breaches – are challenging events in the life of any organization. Many things need to be done quickly. If the left hand does not know what the right hand is doing, an already bad situation can deteriorate fast.

## 5.

The insured and attorney approve notification letters for mailing and a call center service provider is selected. Q&A scripts for call center employees are prepared.

## 6.

The notification service provider sends letters, which include an offer of either a credit monitoring or identity monitoring package to affected individuals.

## 7.

Individuals who are potentially affected by the breach receive letters and may enroll in the monitoring services. Credit monitoring enrollment is either online or offline through the call center. Those enrolled are also eligible for identity theft resolution or fraud support services should they become a victim of identity theft or fraud caused by a covered breach.

## 8.

The insured receives reports on the progress of the mailing and credit monitoring enrollment for continuous monitoring of the event. BBR Services maintains close contact with the insured and the service providers throughout the process to ensure the breach is handled as effectively as possible.

# About Beazley Breach Response

Beazley Breach Response is a unique insurance, loss control and risk mitigation service that provides a comprehensive service to notify and protect the customers of policyholders that have suffered a data breach.

## Coverage highlights

- The limit of coverage is available for up to 5,000,000 notified individuals per policy period. Other limit options are available
- Flexible limits for forensic expenses to determine the existence and scope of a breach
- Limits up to $250,000 for crisis management and public relations
- A separate sublimit of coverage for fines and penalties resulting from non compliance with published Payment Card Industry (PCI) data security standards. Coverage includes a separate sublimit of $50,000 for PCI re-certification expenses following a breach
- A key feature of privacy breach response services is that they are provided with per incident retentions starting as low as $5,000 for legal services
- Credit and identity monitoring services start at breaches over 100 or 250 notified individuals, depending on company size.

For more information, go to **beazley.com/bbr**

## Comprehensive service

Beazley has partnered with a network of organizations, all of which have extensive data breach management experience, to provide the most comprehensive service possible:

- **Forensic** (to provide computer security services in the event of an actual or suspected breach incident)
- **Legal** (to determine the applicability of, and actions necessary to comply with, breach notice laws)
- **Breach notification**
- **Call center**
- **Credit monitoring and data monitoring services**

# 563million

records reported leaked since Privacy Rights Clearinghouse began tracking US data breaches in 2005.

July 2005. Hackers lift millions of credit card numbers off a retailer's wireless network

## Beazley Group

Plantation Place South
60 Great Tower Street
London EC3R 5AD
United Kingdom

T +44 (0)20 7667 0623
F +44 (0)20 7674 7100

## Beazley Group

30 Batterson Park Road
Farmington, CT 06032
USA

T +1 (860) 677 3700
F +1 (860) 679 0247

## Beazley Insurance Services

101 California Street
Suite 1850
San Francisco, CA 94111
USA
CA Lic. #0G55497

T +1 (415) 263 4040
F +1 (415) 263 4099


Visit our dedicated microsite
everybreachisdifferent.com

Follow us
twitter.com/breachsolutions



beazley

April 2012. Thousands of hospital patients require notification after paper records containing personal financial data – including credit card details – are found blowing through a field several miles from the hospital

# Beazley Breach Response Checklist

| | Insurer 1 | Insurer 2 | Insurer 3 |
|---|---|---|---|
| Insurer/Policy Form | **Beazley Breach Response** | | |
| A.M. Best Rating | **A*** | | |

| **Breach response cost coverage** | | | |
|---|---|---|---|
| Breach response costs coverage includes notification of up to _____ individuals? | **Yes** | | |
| Credit monitoring offered to notified individuals? | **Yes** | | |
| Coverage includes credit restoration service? | **Yes** | | |
| Dedicated breach response costs limit that is in addition to third party liability aggregate limit? | **Yes** | | |
| Forensic and legal expenses also in addition to policy aggregate limit (sublimit of $_____ )? | **Yes** | | |
| Insurer has panel of service providers? | **Yes** | | |
| Insured may select legal counsel from panel? | **Yes** | | |
| Free risk management program included with coverage? | **Yes** | | |

| **Security and privacy liability coverage** | | | |
|---|---|---|---|
| Limit | | | |
| Retention | | | |
| Duty to defend | **Yes** | | |
| Coverage includes both non-public personally identifiable information and confidential corporate information? | **Yes** | | |
| Coverage extends to information in the possession of independent contractor? | **Yes** | | |
| Coverage includes events and claims anywhere in the world? | **Yes** | | |
| Coverage includes acts by rogue employees? | **Yes** | | |
| Coverage includes failure to comply with own privacy policy? | **Yes** | | |
| Coverage includes failure to administer an identity theft prevention program required by law or take necessary actions to prevent phishing/identity theft? | **Yes** | | |
| Coverage for failure to timely disclose a security breach as required by law? | **Yes** | | |
| No exclusion for failure to maintain security? | **Yes** | | |

| **Regulatory defense and penalties coverage** | | | |
|---|---|---|---|
| Fines and penalties covered where insurable by law under most favourable venue? | **Yes** | | |

| **Crisis management and public relations coverage** | | | |
|---|---|---|---|
| Coverage includes crisis management expenses? | **Yes** | | |



*Beazley's Syndicates at Lloyd's A15; Beazley Insurance Company, Inc. A8