CYBERRISKS&LIABILITIES_

Understanding and Responding to a Data Breach

No company, big or small, is immune to a data breach. Many small employers falsely believe they can elude the attention of a hacker, yet studies have shown the opposite is true. According to Verizon Communication's *2012 Data Breach Investigations Report*, 72 per cent of the 855 data breaches analysed were at companies with 100 or fewer employees.

Data breach response policies are essential for organisations of any size. A response policy should outline how your company will respond in the event of a data breach, and lay out an action plan that will be used to investigate potential breaches to mitigate damage should a breach occur.

Defining a Data Breach
A data breach is an incident where personal data is accessed and/or stolen by an unauthorised individual. Examples of personal data include:

- National insurance numbers
- Credit card information (credit card numbers – whole or part; credit card expiry dates; cardholder names; cardholder addresses)
- Business identification numbers; employer identification numbers
- Biometric records (fingerprints; DNA; or retinal patterns and other measurements of physical characteristics for use in verifying the identity of individuals)
- Payroll information
- Medical information for any employee or customer (doctor names and claims; insurance claims; prescriptions; any related personal medical information)
- Other personal information of a customer, employee or contractor (dates of birth; addresses; phone numbers; maiden names; race; religious belief; sexual orientation; commission or alleged commission of an offence; etc.)

Data breaches can be costly. According to the Ponemon Institute's *Cost of a Data Breach Survey*, the average per record cost of a data breach was £79 in 2011; the average organisational cost of a data breach was £1.75 million.

Responsibilities upon Learning of a Breach
The Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 and subsequent amendments establish requirements that organisations must follow concerning data protection. A breach or a suspected breach of personal information must be immediately investigated. Since all personal information is of a highly confidential nature, only personnel necessary for the data breach investigation should be informed of the breach. The following four elements should be included in any breach management plan:

1. Containment and Recovery
Establish procedures to isolate and contain the breach in order to limit the damage. Consider whether there is anything you can do to recover any of the breached data or equipment. Once basic information about the breach has been established, management should make a record of events and people involved, as well as any discoveries made over the course of the investigation to determine whether or not a breach has occurred.

2. Assessment of the Risks
Once a breach has been verified and contained, perform a risk assessment that rates the:

- Sensitivity of the personal information lost (customer contact information alone may present a smaller threat than financial information)
- Amount of personal information lost and number of individuals affected
- Likelihood personal information is usable or may cause harm
- Likelihood the personal information was intentionally targeted (increases chance for

fraudulent use)
- Strength and effectiveness of security technologies protecting personal information (e.g., encrypted personal information on a stolen laptop, which is technically stolen personal information, will be much more difficult for a criminal to access.)
- Ability of your company to mitigate the risk of harm

3. Notification of the Breach
Responsibility to notify individuals, the Information Commissioner's Office (ICO) or appropriate regulatory body depends on the sector your organisation is in, type of data accessed, and the individual circumstances of the data breach. Any information found in the initial risk assessment should be turned over to the appropriate legal professional of your company who will review the situation to determine if, and to what extent, notification is required. Notification should occur in a manner that ensures the affected individuals will receive actual notice of the incident. Notification should be made in a timely manner, but make sure the facts of the breach are well established before proceeding.

In the case that notification must be made:
- Only those that are legally required to be notified should be informed of the breach. Notifying a broad base when it is not required could raise unnecessary concern in those who have not been affected.
- A physical copy should always be mailed to the affected parties no matter what other notification methods are used (e.g., phone or email).
- A help line should be established as a resource for those who have additional questions about how the breach will affect them.

The notification letter should include:
- A brief description of the incident, the nature of the breach and the approximate date it occurred.
- A description of the type(s) of personal information that were involved in the breach (the general types of personal information, not an individual's specific information).
- Explanation of what your company is doing to investigate the breach, mitigate its negative effects and prevent future incidences.
- Steps the individual can take to mitigate any potential side effects from the breach.
- Contact information for a representative from your company who can answer additional questions.

4. Evaluation and Response
It is important for you to investigate the causes of the breach and the effectiveness of your response to it. Identify and review your existing policies and procedures to see where improvements can be made to prevent future data breaches.

For more information on how to respond to a data breach, please visit the Information Commissioner's Office at www.ico.gov.uk.

Insurance is Important
Chances are your company doesn't have funds saved to pay for data breach remediation. Fortunately, there are insurance options available to make recovery easier. Cyber liability insurance policies can cover the cost of notifying customers and replace lost income as a result of a data breach. In addition, policies can cover legal expenses a business may be required to pay as a result of the breach.

We're Here to Help
A data breach can be very costly and even has the ability to shut a business down. Contact Crendon Insurance Brokers Ltd today for resources to help support your cyber security efforts. We have the know-how to ensure you have the right cover in place to protect your business from a data breach.