Could Your Agency Weather A Data Breach?

A full 80 percent of businesses that experience a data breach go out of business as a result.[1] The right insurance can keep your agency from becoming part of this startling statistic. If that is not enough reason to consider purchasing data-breach protection for your business, here are six more:

1. **Data breaches are common among smaller businesses.** Some 55 percent of small businesses responding to a recent survey have experienced a data breach and 53 percent have reported multiple incidents.[2] If you collect sensitive information from policyholders, you are at high risk.

   Data held by small businesses is low hanging fruit... hackers know these enterprises lack the security resources of their larger counterparts. Only 38 percent of breaches in the latest Verizon study impacted larger organizations.[3]

2. **Responding to a breach is not only costly (running an estimated $200,000), it's complex.** Experts from multiple disciplines (from forensic investigators, to public relations firms, to privacy counsel) may be needed to mount a coordinated response to even a small incident. Botch the response and your reputation can be irreparably damaged. There is also the specter of regulatory fines and penalties and legal liability. A single laptop left on a commuter train or stolen at an airport can cost an agent nearly $50,000 – most of that being expenses to respond to data breached (or potentially breached).[4]

3. **Package policies are not up for the task.** Your commercial package policy may have a cyberliability extension, but take a hard look at the coverage provided. Endorsements typically carry low limits and few options. If first-party coverage is provided, limits may be inadequate for the exposure. For third-party liability, coverage may fall short in key areas, such as responding to acts of rogue employees. Does it address regulatory fines and penalties? Does the insurer have the duty to defend?

4. **You are obligated to protect data you collect.** This sensitive data might include everything from personal information, (addresses, Social Security and driver's license numbers of employees, policyholders or prospects) as well as corporate information (sensitive financial information on commercial clients). If you handle employee benefits, you may have personal health information in your care.

WHAT AMPS UP AN INSURANCE AGENCY'S EXPOSURE?

Answering yes to any of the following questions:

- Do you have employees?
- Do you keep employee records?
- Do your client records include third party corporate information (such as company financials)?
- Do you handle personal lines?
- Do you offer premium financing?
- Do you have computers, back-up tapes, a copier, a fax machine?

State and federal regulations dictate proper handling of private information. If this information is breached, agents must navigate the different laws in 46 states that mandate how victims must be notified. [5]

5. **Even if you outsource data handling, your exposure stays in house.** You may feed data into third-party agency management or document-management systems or outsource data storage to a cloud provider. Still if your agency's data is breached, you are obligated to respond.

   Nearly 70 percent of small businesses report that breaches are more likely to occur when outsourcing data.[6]

6. **The exposure is not just from hackers intruding on electronic systems.** Breaches are caused by everything from lost/discarded/stolen laptops, smartphones and portable memory devices to innocent procedural errors and acts of disgruntled employees.

Of 563.9 million records breached since 2005:

56% Hacking or malware – Electronic entry by an outside party.

30% Portable device – Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.

6% Insider – Someone with legitimate access intentionally breaches information, such as an employee or contractor.

4% Unintended disclosure – Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax or mail.

1% 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/ other.

Source: Privacy Rights Clearinghouse, 10/18/2012

How costs add up in a breach

Every data breach is different. Generally speaking, however, in considering the cost of a response you can expect to pay from $10,000 to $100,000 just for a forensics expert to get to the root of a breach and contain it. Creating and mailing notification letters to victims is in itself costly. Once you do that, you typically must also set up a call center to respond to inquiries from victims and offer credit monitoring to help mitigate damages. Smaller businesses are less likely than larger ones to have the internal resources and expertise to handle a breach response, so they are more likely to have to pay outside experts (including specialized privacy counsel, consultants, crisis management and public relations professionals) to assist. Then there is the cost of any regulatory actions, penalties or lawsuits that could arise from the incident.

Being protected = Being prepared to respond

It could be a lost flash drive or a persistent attack by hackers a world away. Every breach is different, and every one requires a smart, strategic response. With Beazley Breach Response, your agency can secure comprehensive coverage for the expenses incurred to respond to a breach and have experts standing ready to deliver the well coordinated response you need to mitigate financial damages and protect your reputation. It encompasses everything from forensic investigation, legal, compliance and public relations services to breach notifications, call center servicing and ongoing credit and data monitoring. To learn more, contact Laura Cornell with IIABSC Agency (803.760.1227 or lcornell@iiabsc.com) or visit www.iiabsc.com.

1. *Privacy Rights Clearinghouse: Chronology of Data Breaches*
2. *Ponemon Institute.*
3. *Verizon2013 Data Breach Investigation Report, p. 5*
4. *California Attorney General/Privacyrights.org*
5. *http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx*
6. *Ponemon Institute.*

POLICYHOLDER SERVICES

NEW SERVICES INCLUDE

- Training and Awareness Programs
- Animated Staff Training Programs
- Expanded HIPAA Compliance Tools

DATA SECURITY RISK MANAGEMENT

NoDataBreach.com provides risk management policies, procedures, training, and other tools to help insureds prevent a breach of confidential data.

As a Beazley Breach Response® policyholder, you have unlimited access to:

ON-LINE COMPLIANCE MATERIALS

Federal and state compliance materials regarding data security, data breaches, and data privacy, including:

- Quick Tips on many subjects; Summaries of federal/state laws
- Links to statutes & regulations; Sample policies & procedures
- Continuing updates and electronic notification of significant changes to the on-line materials

QUARTERLY NEWSLETTER & "INSTANT ALERTS"

Sent by email, learn about changes in federal and state laws regarding data security, data breach, and data privacy issues; Instant Alerts sent by email for events require immediate attention.

EXPERT SUPPORT ON-LINE

Experts support from consultants/attorneys on data security issues; including:

- Health care & HIPAA compliance issues
- Data breach prevention issues
- Data Security best practices
- Computer forensic issues

STEP-BY-STEP PROCEDURES TO LOWER RISK

Procedures and on-line forms help you:

- Understand the scope of "personal information" ("PI")
- Determine where PI is stored
- Collect and/or retain the minimum amount of PI as required for business needs
- Properly destroy PI that is no longer needed
- Implement an Incident Response Plan

TRAINING MODULES

- Comic Strip training
- Online training programs; Employee training bulletins
- Webinars for privacy compliance and IT staff
- Audio and PodCast training for managers and/or employees

HANDLING DATA BREACHES

Guidance provided to:

- Help prevent data security incidents
- Respond to a data breach

NoDataBreach.com

Powered by ePlace Solutions, Inc.

For a quote, contact:
Laura Cornell
IIABSC Agency
803.760.1227
lcornell@iiabsc.com