Data Security is an affinity program of your State and National Rural Water Association

Could your business weather a data security breach?

Small and midsize businesses are the top targets of cyber criminals, actually suffering breaches more often than their larger counterparts, according to the Verizon 2014 Data Breach Investigations Report.
While hackers are not slowing down (indeed, their methods only get more sophisticated), your business can survive after a breach if you are prepared with the proper insurance in place. Need more reasons to consider data breach protection for your business? Consider this:

1) If you collect any sensitive information from customers, employees or others, you are at high risk.

The data held by small businesses is low hanging fruit. Hackers know that smaller enterprises hold the same sensitive data as their larger counterparts, but lack the same security resources. Only 38 percent of breaches in the latest Verizon study impacted larger organizations.

2) Responding to a breach is not only *costly*, running an estimated $200,000, it is *complicated*.

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 company's reputation can be irreparably damaged. There is also the specter of regulatory fines and penalties that vary state to state as well as legal liability.

3) Package policies are not up for the task.

Your commercial package policy may include a cyber liability extension, but take a hard look at the coverage it provides. These endorsements typically provide low limits and few options. If first-party coverage is even provided, limits are likely to be inadequate for the exposure. On the third-party liability side, coverage will probably fall short in key areas, such as responding to acts of rogue employees. Does the extension address regulatory fines and penalties? Does the insurer have the duty to defend? Unlikely.

4) You are obligated to protect data you collect.

State and federal regulations dictate proper handling of private information. This could include personal information of employees or customers, such as addresses, Social Security numbers and driver's license numbers as well as personal health information if you offer employee benefits. If Data Security is breached, you must navigate different laws in 47 states that mandate how victims must be notified.

5) Even if you outsource data handling, your Data Security exposure stays in-house.

Your data may be compromised when it is in the hands of a third party - such as the cloud provider you hired to expand data storage. Or, a hacker may simply be intruding on your network and data in route to capture data held by your large clients. Either way, your organization can be responsible for providing notification and responding if the data is breached. You can outsource your responsibility but you can not outsource your Data Security liability.

6) The exposure is not just from hackers intruding on electronic systems.

Breaches are caused by everything from lost, discarded, or stolen laptops, PDAs, smartphones, portable memory devices and paper files, to innocent procedural errors and acts of disgruntled employees.

What increases your exposure?

Answering yes to any of the following questions:

Do you have employees?

Do you keep employee records?

Do you run credit checks?

Do you require Social Security numbers or drivers license numbers to provide services?

Do you offer credit card payment options or other financing?

Do you have computers, laptops, tablets, smartphones, back-up tapes/drives, copiers, and/or fax machines?

Do your client records include third party corporate information (such as company financials)?

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 Data Security services, your small business 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 forensic investigation, legal services, compliance & public relations services, breach notifications, call center servicing, and credit & identity monitoring.

Bailey Special Risks, Inc.
800.768.7475
submit@bsrins.com

BSR