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

Data breach risk is the product of two trends:

The proliferation of data exchanged within and between organizations. Much of this data is personally identifiable information. 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.

Expect the unexpected:

For businesses, a particular challenge of data breaches is that they can come from almost any angle and can take myriad forms.

932.7 million records breached since 2005

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%

Source: Privacy Rights Clearinghouse (www.privacyrights.org)

The biggest risk:

The biggest risk for most organizations 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 is reputation.

How we help:

Data Security services has helped clients handle more than 1,500 data breaches, including many involving hundreds of thousands of records. Service is centered to meet three critical needs:

Speed
Thoroughness
Coordination

Purchase a Data Security policy with coverage for up to one hundred thousand notified individuals. The insured registers with a Data Security services website designed to provide online security and privacy information services.

Below is an example of events that take place for business following a breach:

1) Notification to Data Security services claims office via phone or email is provided for claim reporting.
2) An attorney from a 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.
3) The insured, with advice from legal counsel and continuing guidance from Data Security services, determines 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.
4) 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.
5) The notification service provider sends letters, which include an offer of either a credit monitoring or identity monitoring package to affected individuals.
6) Individuals who are potentially affected by the breach receive letters and may enroll in the monitoring services. Credit monitoring enrollment is either direct 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.
7) The insured receives reports on the progress of the mailing and credit monitoring enrollment for continuous monitoring of the event. Data Security services maintains close contact with the insured and the service providers throughout the process to ensure the breach is handled as effectively as possible.

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

BSR