

MIDLANDS

Data Breach Technology E & O Coverage

Midlands provides industry-leading coverage for emerging data security & privacy exposures facing your insured. Available through **A.M. Best Rated Carriers**.

TARGET RISKS:

Retail • **Healthcare** • **Financial Institutions** • **Schools/Universities** • **Law Firms** • **Insurance Agents** • **Car Dealers**

Key Events That Trigger This Coverage:

- Lost/stolen portable computers or media
- Lost/stolen back-up tapes and drives
- Improper disposal of paper records & computer equipment
- Computer hacking
- Employee misuse
- Vendor negligence

Why Your Insured's Need This Coverage:

This coverage offers multi-faceted protection for both the expense & the legal liabilities associated with data security privacy breaches, **exposures not typically covered by traditional insurance policies**.

Even when your insured's have done nothing wrong, they can face significant legal fees defending themselves against allegations, costs \$50,000 or more.

Premium Example:

\$1,750 Minimum Premium for a \$1M Limit with a \$2,500 Deductible.

Limits up to \$20,000,000

Business Vulnerabilities:

Customers or employees who entrust a business with personal or private information such as credit card or social security numbers put businesses at risk. This coverage helps mitigate the financial impact of data breaches associated with:

- Credit card information
- Personal financial information
- Personal health information
- Business information of others (trade secrets)
- Customer data (confidential information)

Coverage Provides:

- Broad coverage for the expenses associated with an incident, including:
 - Compliance with data breach notification laws
 - Securing legal counsel to advise on incident response
 - Providing credit file monitoring to victims
 - Hiring forensic experts to investigate the breach
 - Paying regulatory defense and penalties from privacy law violations
- Extensive coverage for legal liabilities including those arising from failure to comply with state or federal breach notification laws or privacy policies and/or to administer a government-mandated identity theft prevention program ("Red Flag Rules").

For additional information, please contact:
Midlands Management Corporation
ProfessionalLiab@midman.com
Phone: 800.800.4007 • Fax: 405.840.5432
Send Submissions To: Submit@midman.com

www.midlandsmgt.com



DATA BREACH ~ 4 POINT INSPECTION CHECKLIST

-  **Encrypt data stored on portable devices. Keep TRACK of your business laptops & create best practices to keep them safe.**

Stolen laptops constitute 20% of the total number of data breach incidents. Replacing a laptop lost by an employee may cost \$1,000 but can escalate to \$50,000 factoring in the loss of intellectual property or customer sensitive data. Use locks on laptops, & refresh password & encryption protocols.
-  **Ensure your DATA storage system has appropriate safeguards, & conduct periodic vulnerability scans.**

Use backup tapes/third party vendors/servers to keep data safe. Ensure any vendor in charge of storing your customer data has a tightly-buttoned security program in place. Ensure any software protection vendor engaged by your company conducts regularly scheduled vulnerability scans to detect missing security patches, configuration errors, & other weaknesses that allow unauthorized access.
-  **Safeguard against insider negligence. Make sure your employees are well-TRAINED.**

Although not intentional, insider negligence accounts for a large portion of data breach incidents. Ensure employees do not transfer sensitive information to work from their home computers, & that they properly dispose of paper records & computer requirements. Make sure they are not opening emails from unknown sources that could lead to virus issues. Implement data privacy policies & training for all employees to ensure they know how to properly handle your sensitive information.
-  **Be AWARE that customer information in your care could leave your small business vulnerable.**

Hacking attacks were responsible for the majority of personal identity records exposed in 2009. Credit Card/Social Security Numbers/Personal Health Information/Trade Secrets/Business Information of others - all leave your business vulnerable. Make sure your network security software is updated with the latest available patches. Ensure your insurance protects following a breach for credit file monitoring & other "post event" services.