

Est. 1864

Risk Mitigation for Data Security Breaches Isn't Optional Anymore

It's not IF, but WHEN, your business will be a victim of Cyber Crime

According to CNN Money, cyber crime's easiest prey is small to medium sized businesses, which account for more than 72% of all data breaches. The Federal and State governments (differ by state) have developed laws and standards (PCI) to protect the public regarding personal and financial information (credit cards). In North Carolina and all other states except Kentucky, New Mexico, Alabama and South Dakota, data must be secure and there are consequences if there is a breach.

EXAMPLES OF RECENT BREACHES:

July 29, 2013 — Walmart in Oklahoma*

Two men were indicted for their role in a skimming plot. They were accused of fraudulently obtaining \$400,000 by placing skimming devices at gas pumps at Walmart stores for up to two months at a time. They then created counterfeit credit cards by using the legitimate card information obtained through skimming. The skimming ring ran from April 2012 through January 2013.

June 28, 2013 — ABC Stores in Greensboro and

Winston-Salem, NC*

Greensboro and Winston-Salem stores discovered that the software used in their cash registers had been hacked. The malware was discovered after customers complained about fraudulent charges on their debit and credit card accounts. The ABC stores stopped accepting debit and credit cards while investigating the issue.



For more information contact:

Lisa Cunningham

Commercial Account Manager Scott Insurance 4700 Falls of Neuse, Suite 320 Raleigh, NC 27609

919.844.7719 lisacunningham@scottins.com

March 2, 2015 — Piedmont Advantage Credit Union of Greensboro, North Carolina*

Piedmont Advantage Credit Union notified customers of a data breach when one of their laptops containing personal information of its members could not be located. The information included names, addresses, dates of birth, member account numbers, and Social Security numbers. According to the credit union the laptop included password protected authentication.

If there is a breach of credit card information from one of your locations, you may be obligated to do the following:

- Notify your entire customer base with a description of the loss
- Describe the type of Personal Information that may have been breached
- Describe the steps your company has taken to prevent further unauthorized access
- Provide a telephone number for effected parties to contact
- Provide credit monitoring services for the customer

Data breaches are expensive. Can your company financially handle a breach based on the following? (Data from 2011-2013**)

- Average number of exposed records 2.4M
- Average cost per record \$956.21
- Average total cost per incident \$3.7M
- Average cost of legal defense \$698,797
- Average claim payout \$733,109
- PCI Fines range from \$11,000 \$120,000
- Average cost for forensics, notification, call center, credit monitoring \$983,000

Because of the demand for such coverage, insurance carriers offer Cyber Liability Insurance which will help you protect your business. Typical insurance policies exclude cyber and privacy liability.



Scott Insurance, a division of James A. Scott & Son, Inc., has offices in Charlotte, Greensboro and Raleigh, North Carolina; Knoxville and Nashville, Tennessee; and Lynchburg, Richmond and Roanoke, Virginia, and captive insurance operations in Grand Cayman and Vermont.