

# What If Your Business's Data Were Compromised?

By GINA NAPOLI

One of the most critical undertakings for any organization is proactively protecting its data. It's important to treat your data-security approach as a continuous strike against electronic hackers and social-engineering infiltration.

For businesses that rely on accurate data sources to manage their everyday workflow, a security breach equals disaster in terms of work stoppage, privacy, and finances.

"Costs can vary greatly depending on the size of the breach and the type of information lost," said Anthony Dagostino, vice president, ACE Professional Risk.

When personally identifiable information (PII) is lost, a business is vulnerable to identity theft. Identity theft in 2012 alone cost companies and individuals \$1.5 billion. PII includes non-public information, like a person's name in combination with birth date, Social Security number, or address. It can also include data like credit card numbers, bank account numbers, and private medical information.

Corporate-confidential information, like intellectual property or proprietary data, may need to be protected as well, especially if acknowledged as confidential under a non-disclosure agreement or similar contract.

Having a formal data-incident response plan in place is crucial.

"We recommend a written plan that is regularly updated and tested

through tabletop exercises," Dagostino said. "Effective plans have an individual identified as the point person and identify responsibilities across numerous job functions, like legal and compliance, risk management, IT, and communications."

It's important for companies to select third-party vendors specializing in breach-response services before they have a breach. Pay attention to how the contract is structured.

Key terms would include who is legally and financially responsible for data if they are breached, who is responsible to communicate the breach to potentially affected individuals, how to recoup expenses, and liability insurance.

"Having the right companies on standby with pre-negotiated rates for response services like legal, forensics, and notification are key in handling a breach in a timely and effective manner," said Dagostino.

"A third-party vendor can help formulate and execute an incident-response plan, which should be communicated to all employees, along with each employee's specific roles and responsibilities. Treat this plan as you would a fire drill. Prepare and execute periodically."

Companies that are more prepared to respond to a breach spend less money on post-breach services. Imagine puncturing a feather pillow on top of a mountain, shaking all the feathers free, and then trying

to collect them all. Having a plan in place is like pouring the pillow straight into a pillowcase. You might lose a few feathers, but you can put your pillow back together.

Physical and virtual data security requires constant vigilance as part of every employee's job in any organization. The majority of breaches are inside jobs, typically committed by disgruntled employees. About 59 percent of employees delete data prior to exiting a position.

No security approach is 100 percent foolproof. As hackers become increasingly creative, so must your data-security plan.

There are usually warning signs of profiling this type of employee. Unfortunately, those signs are shared after the breach has already happened. If you see red-flag warning behavior, think: angry, complaining, antisocial, possibly threatening), say something. Better to be paranoid and wrong rather than silent and correct.

There are also inside jobs at the hands of careless employees. Train your employees on smart data guardianship, and issue periodic reminders. Systemically, this includes antivirus software updates, encryption software, installing current patches, and employees who actively research and combat the latest threats.

For all employees, this includes (but is certainly not limited to) strong passwords that aren't written anywhere, protecting business-sensitive data the way they would treat their bank account information, and locking down hardware and removable media.

Those anecdotes about laptops

being stolen from cars and janitors stealing thumb drives from hard drives are real. So are the people who have given data over the phone without verifying a caller's credentials.

So what are your rights if your business data is compromised?

Many regulations exist on both federal and state levels. Nationwide, federal regulations exist for some industries that have higher PII exposure, like banking and healthcare.

The Gramm-Leach-Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA) were enacted to provide consumer-disclosure protocols, and they address what type of information is collected and how it is shared.

HIPAA contains amendments to address how information is to be protected and also provides guidelines on notifying affected individuals after a breach.

Currently, 46 states have different laws in place that address notifying affected individuals after a breach.

Various bills have been introduced for

a national data-breach notification law, but no legislation has been passed as yet.

You can have the smartest data-protection plan available, and your data can still be compromised. No security approach is 100 percent foolproof. As hackers become

increasingly creative, so must data-security plan.

Defending your company's may conjure images of a *Spy* vs. cartoon, but calculated, preventive measures are preferable to trying to recover feathers that have already escaped the pillowcase. **BV**

*Join other businesswomen at monthly luncheon workshops to learn more about achieving success in business.*

December 10, 2013  
Eat the Icing First  
Debra Stock,  
CEO (retired) YWCA York

February 11, 2014  
New YCP President  
Dr. Pamela Gunter-Smith

**WBCO** WOMEN'S BUSINESS CENTER ORGANIZATION

**YORK COLLEGE** OF PENNSYLVANIA

*Educating Women on Best Practices in Business*  
[www.wbcoryork.org](http://www.wbcoryork.org)

**THE DREXEL GROUP INC.**  
TEMPORARY AND PERMANENT STAFFING

1832 Market Street, Camp Hill PA 17011 • 50 Mount Zion Road, York PA 17404

**Full Service Staffing:**  
Light industrial • Administrative/Office Staff  
Hospitality - Banquet Servers, Bartenders, Kitchen Staff,  
Cafeteria Staff, Housekeeping

Camp Hill: 717.730.984 • York: 717.718.1414  
[www.TheDrexelGroup.com](http://www.TheDrexelGroup.com)

**SIERRA CLUB-LANCASTER GROUP  
POLAR BEAR 5K  
TRAIL RUN/HIKE**

**DATE:**  
SATURDAY,  
JANUARY 18, 2014

**RACE START:**  
10 A.M.

**LOCATION:**  
LANCASTER COUNTY CENTRAL PARK,  
PAVILION 22

Prizes will be awarded to the overall top three male & female runners, and the top three male & female runners in each age category. The first three finishers with dogs will also receive prizes.

**Race fees:** \$20 if received by January 7; \$25 after January 7, 2014. All those who register before January 7 will be guaranteed a t-shirt.

Proceeds benefit the Sierra Club-Lancaster Group's environmental cleanup and education efforts throughout the county.

For more information, visit [www.lancastersierraclub.org](http://www.lancastersierraclub.org) or email [SierraClubEvent@gmail.com](mailto:SierraClubEvent@gmail.com).

**BY PARTICIPATING IN THIS RACE YOU WILL BE MAKING TRACKS FOR CHANGE!**