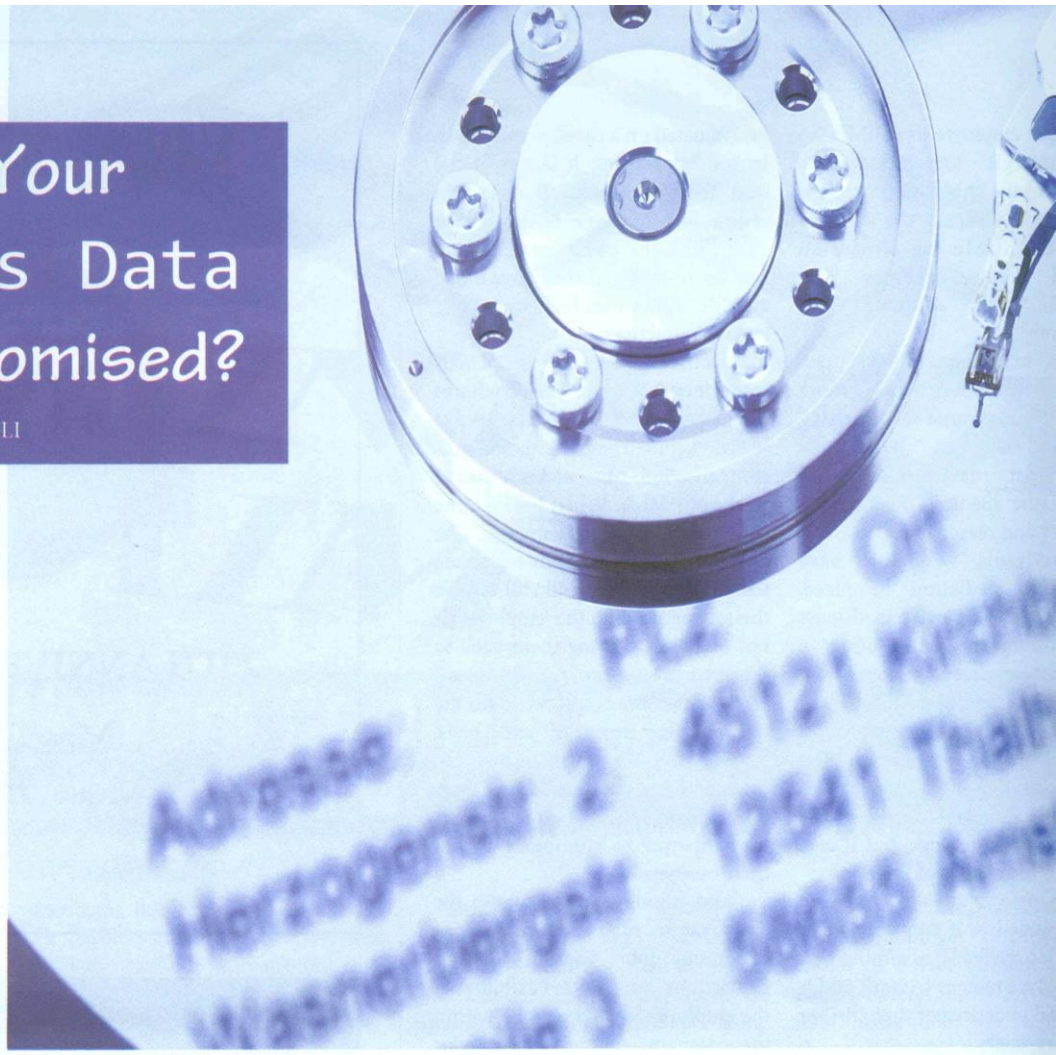
What If Your Business's Data Were Compromised?

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 in place is like pouring th pillow straight into a pillowcase. You might lose feathers, but you can put your back together.

Physical and virtual data s requires constant vigilance part of every employee organization. The majority breaches are inside jobs, t committed by disgruntled emp About 59 percent of employe data prior to exiting a position

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

There are usually warning signs rofiling this type of employee. Jnfortunately, those signs are shared fter the breach has already happened. f you see red-flag warning behavior think: angry, complaining, antisocial, ossibly threatening), say something. Better to be paranoid and wrong ather than silent and correct.

There are also inside jobs at the ands of careless employees. Train our employees on smart data uardianship, and issue periodic eminders. Systemically, this includes ntivirus software updates, ncryption software, installing urrent patches, and employees who ctively research and combat the latest hreats.

For all employees, this includes but is certainly not limited to) strong asswords that aren't written nywhere, protecting business-ensitive data the way they would treat heir bank account information, and ocking down hardware and emovable 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, preve measures are preferable to tryi recover feathers that have al escaped the pillowcase. BW