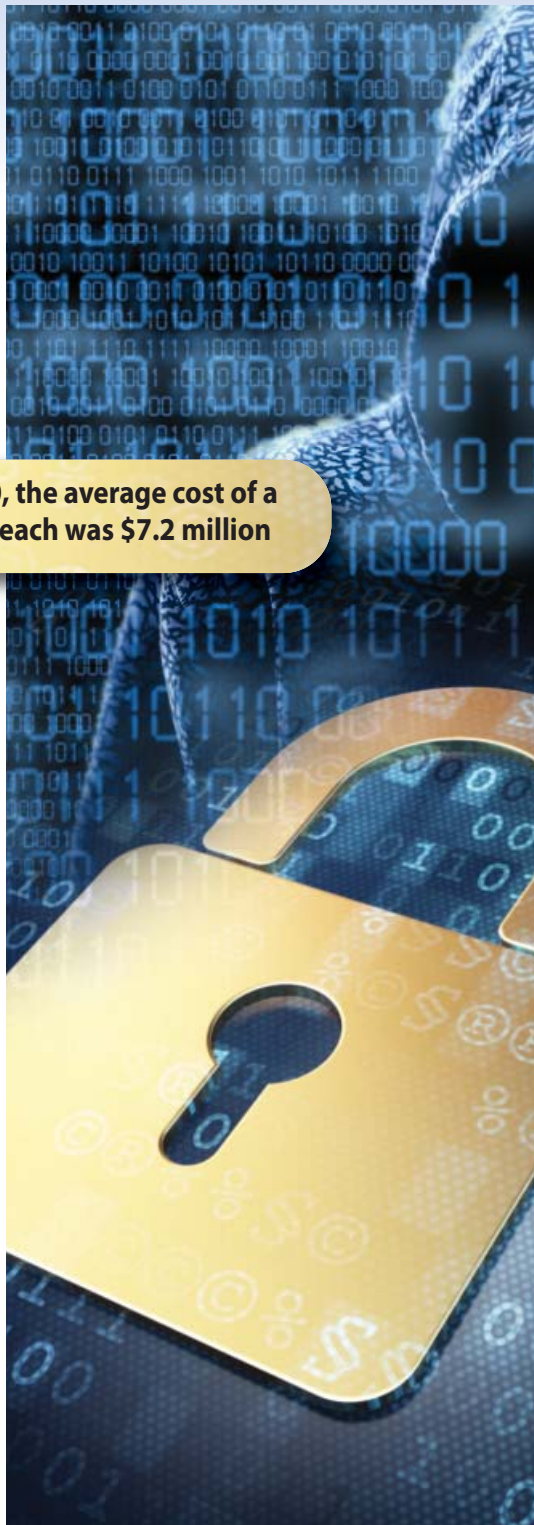
Special feature:

Expert advice on improving

PA Chamber member companies Dell SecureWorks and Marshall Dennehey Warner Coleman & Goggin weigh in with expert advice and a number of different options for businesses of all sizes on how to improve their IT security and prevent data breaches.

How to minimize the threat of the dreaded data breach

By **David J. Shannon**



Every day we are bombarded with reports of new data breaches. Hackers here and abroad seem to be around every corner and invading every computer system. In addition, laptop and/or tablet computers are lost, stolen or misplaced on a daily basis. Add in the everyday employees who unwittingly click on virus phishing emails, and a business owner has to wonder—how can I win?!

The short answer is: with proper planning. Data breaches are an ongoing daily risk for every business and company; no different than the risk of a union strike, or a warehouse fire or customer lawsuits. In 2010, the average cost of a data breach was $7.2 million, and a more recent 2013 Ponemon Data Breach Study found the average cost to be $9.4 million and $188 per lost or stolen record. Such expenses include computer forensic investigations, credit monitoring, affected third party notifications, legal defenses, regulatory fines, public relations and future audit and security programs. However, like every risk, a good business owner can put in place a proper data security plan to effectively minimize data breach threats and secure a company's data and its customers' personal identifiable information (PII).

More than 10 percent of small businesses have had funds stolen from their bank accounts

Whether you are a large business with hundreds of employees, or a small business with less than a dozen employees, the prepared CEO will work with his or her IT, HR and executive management team to develop a strategic, concise, data security plan. Data security must involve commitment from all parts of a business, with personnel identified from each area to serve on a data security team. With this team in place, a good data security plan will identify and address the following issues.

In 2010, the average cost of a data breach was $7.2 million

Data security is everyone's job

When selecting a group of employees to act as your data security team, a common response is, "isn't that the IT Department's responsibility?" No, it is not. Data security is everyone's responsibility. IT must purchase and monitor server firewalls. HR must implement password and computer use procedures. C–suite level managers must monitor the use and retention of customers' data. Managers must ensure that the proper level of knowledge of data security is provided to everyone. Legal personnel must see that all state and federal data security laws are known and followed. In short, everyone plays a role in preventing a data breach.

Old data is bad data

In this day and age, your business collects and retains a tremendous amount of electronic data

continued on page 38

How to minimize the threat

continued from page 36

—all of which contains PII. Many businesses neglect to delete, destroy or properly archive old data, which is one of the worst things a business can do. A data breach is bad and expensive when your 2013 customer PII is lost. A data breach is really bad and really expensive when your customers from 1999 through 2013 have their PII lost or stolen. Develop a plan to routinely purge your servers and paper files of old, non-essential data.

Encryption, encryption, repeat after me, encryption

Every good data security plan starts with a proper encryption plan for all computers, servers and other data-holding devices. The servers in your business must be encrypted. The computers on your desks must be encrypted, and the laptops or tablets in your salesman's car must be encrypted! While encryption is not a guarantee of protection, it does limit your business's exposure if a data breach occurs. Most state data breach statutes, including Pennsylvania, have safe harbor exemptions that will limit a company's liability if it can be demonstrated that the data was encrypted.

Play like your practice

Sports coaches are always telling their teams that a good week of practice will ensure a win on Saturday. The same goes for data breach prevention. IT staff should conduct regular analysis of your servers' vulnerability and determine if PII can be accessed by outside hackers. Department managers should have regular meetings to ensure data security is a priority and protocols are being followed. Are there any missing laptops? Are all passwords secured? Is old data being shredded? These topics should be addressed on a routine basis. Management also needs to ensure that vendors are complying with data security policies and procedures as well.

25 percent of small businesses said they have "little to no understanding of cybersecurity."

Do I need data breach insurance?

While the steps above will provide a blanket of protection, even the most comprehensive data security plan cannot prevent all data breaches from occurring. Human error cannot be discounted as it leads to lost laptops or the penetration of viruses. Hackers can almost always exploit weaknesses in your firewalls before a patch is provided. In every case, a company's risk will be significantly reduced if a cyber insurance policy is in effect. A cyber policy provides a business with coverage for breach notification costs such as attorney fees, letter notification, postage, forensic fees, and regulatory fines. Additional benefits include immediate access to experienced legal and forensic professionals to assist in the data incident response. Coverage for business interruption, third party liability and other losses can also be added to a cyber policy, providing a company with further insulation against liability.

Conclusion

In today's electronic age, businesses must look at data breaches not from the "if," but from the "when" perspective. By treating data security in the realm of ongoing risk prevention, a business owner can reduce exposures to devastating and costly data breach and cyber liabilities and be prepared to respond when the call comes with those five dreaded words, "We've had a data breach."

David J. Shannon *chairs the Technology, Media and Intellectual Property Practice Group, and is co-chair of the Privacy and Data Security Practice Group at civil defense litigation firm, Marshall Dennehey Warner Coleman & Goggin. He devotes a substantial portion of his practice to privacy law, data breaches, IP, copyright infringement and technology litigation. His blog, Data Breach Legal Watch, provides perspectives on data security issues facing businesses. He may be reached at djshannon@mdwcg.com or 215 575-2615.*