Data Liability: Challenges Facing Employers

PARKER | SMITH | FEEK

August 2011

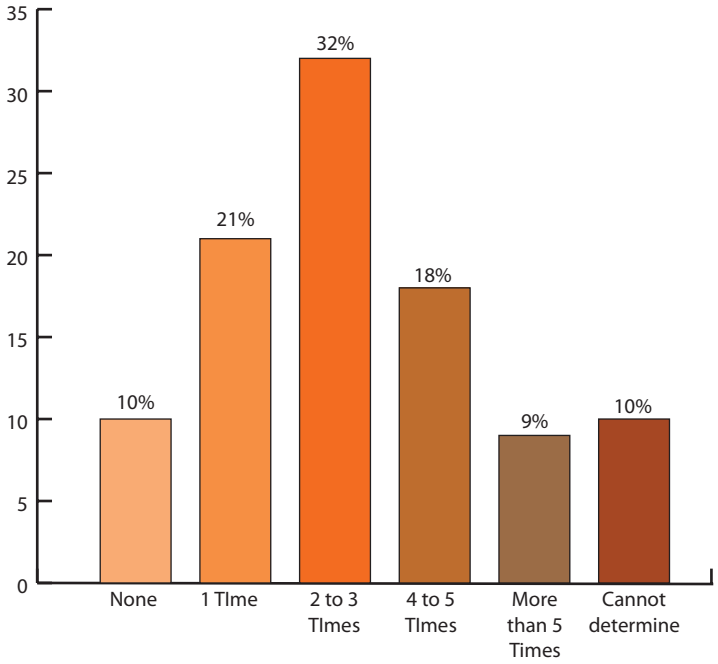
By Cliff Rudolph, Technology Practice Group Leader

In a recent article titled Hack Attack published in Time Magazine, the author, Bill Saporito, provides a glimpse into the world of hackers and outlines the motivations of LulzSec, the group responsible for the much publicized Sony breach. In the article he points out that "Hackers have discovered that small and medium-size businesses are far more vulnerable than major corporations."

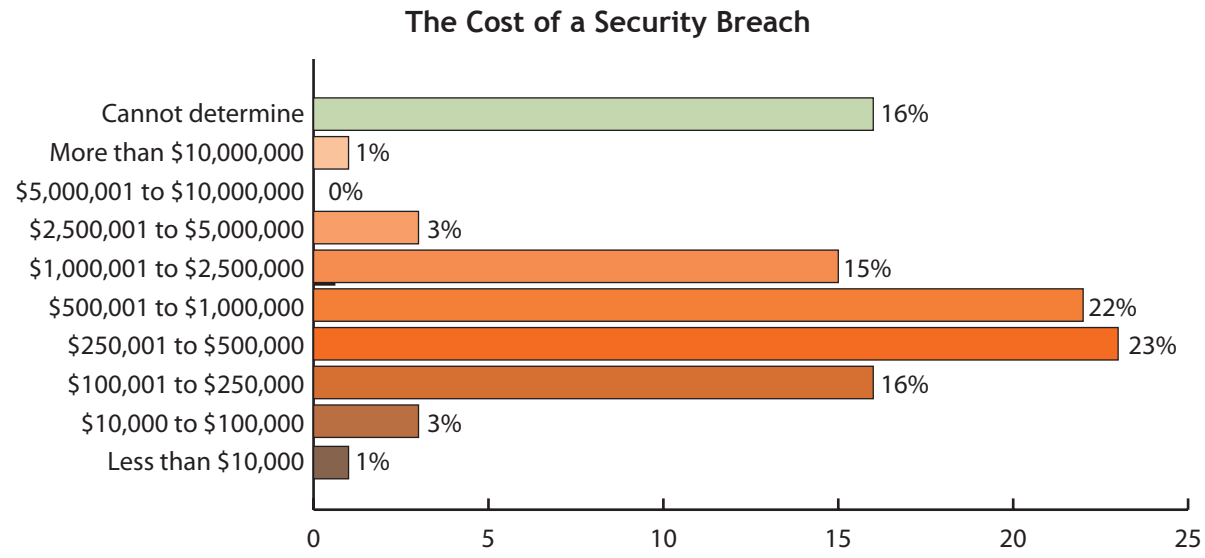
Recent surveys conducted by Verizon and Ponemon Institute would support the idea that small to mid-size businesses are increasingly at risk. Based on figures from the Verizon survey, 50% of reported breaches occurred to organizations with less than 1,000 employees and 27% of breaches were experienced by companies with less than 100 employees. And while less data has been lost through cyber attacks, the cost and number of malicious attacks are increasing rapidly. This would highlight a trend of attacks shifting from large breaches to smaller breaches, which are difficult to stop as they generally go unnoticed.

To gain a deeper understanding of the risks that small-to-midsized businesses face we can look to an additional report published by Ponemon Institute in June of 2011, Perceptions about Network Security. Ponemon surveyed 583 IT and IT Security practitioners in the U.S. and found that 90% of respondents had been breached by hackers at least once in the past 12 month; more than one-third of respondents do not have confidence in their IT infrastructure to prevent further network security breaches.

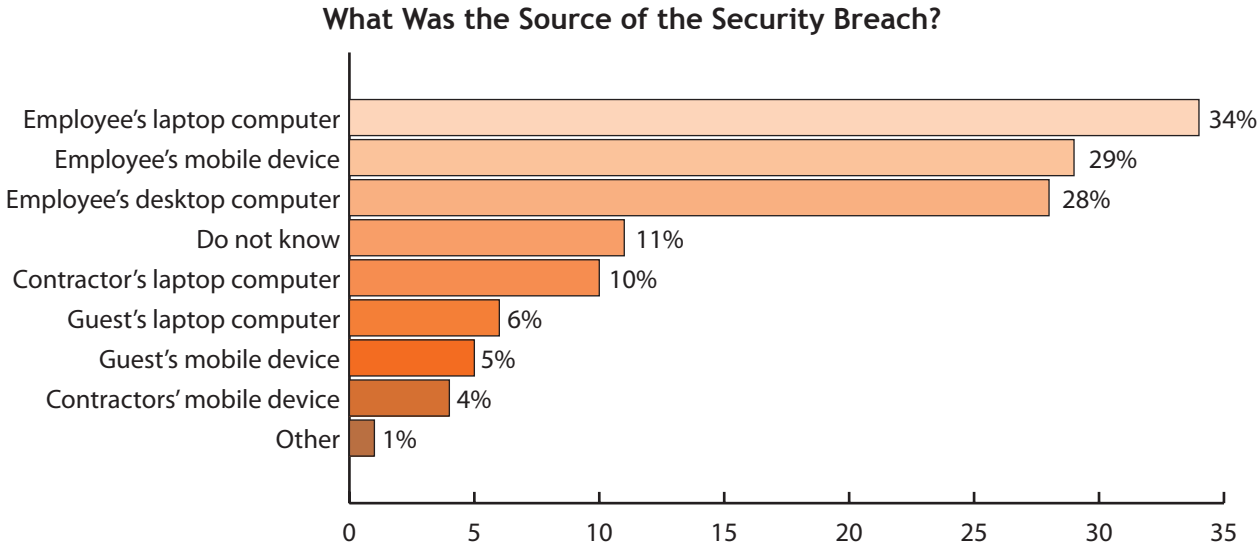
Number of Successful Network Security Breaches over 12 Months



The cost of a security breach can be expensive. Of those that were breached, over 78% reported a financial impact greater than $100,000. Another 16% of respondents were unsure of the financial impact, an indication that the full impact of a breach cannot always be immediately assessed. Only 4% identified a financial impact less than $100,000.



Ponemon's survey also tracked the sources of security breaches and reported multiple vulnerabilities. While we all know of someone who lost a laptop or inadvertently opened an attachment with a virus, the survey found that those methods are not a company's primary problem. As indicated in the graph below, the use of mobile devices and non-employee access greatly increases a company's risk. Twenty-nine percent of cyber attacks occurred through an employee's mobile device and over 25% resulted from a guest's or contractor's laptop or mobile device.



What Should You Do to Protect Your Organization?

Protection of sensitive, private data should be a major concern for organizations of any size. Almost all organizations have exposure to loss of Personally Identifiable Information (PII). At the very least, companies have what would be considered PII for their own employees. PII is often defined as information that can be used to uniquely identify, contact, or locate a single person or information that can be used with other sources to uniquely identify a single individual. In Washington, PII is defined as an individual's first name (or initial) and last name combined with one of the following: Social Security Number, driver's license number, Washington Identification card number, bank account number, credit card number, or debit card number (credit card numbers require that the security code, access code or password also be included) when either the name or the data elements are not encrypted.

Whether your business is located in Washington or elsewhere, you need to be aware of Privacy laws in all states in which you do business. Today, 46 states have legislation regarding security breach notification laws. If you have a breach and private data of individuals located in other states are affected, you must comply with each state's laws. Perkins Coie does a fantastic job of aggregating this information on their website; you can find it here.

In addition to the frequency and severity of hack attacks, organizations face increased costs for solutions that can mitigate their risk exposures. One effective method that companies should consider is financial risk transfer through the procurement of a comprehensive Data Privacy/Cyber Liability insurance policy.

David Navetta, a partner in the law firm InfoLaw Group, recently discussed the importance of cyber insurance in a Fox News interview. According to Navetta, "A lot of companies spend a lot of money trying to stop hackers and bad guys from getting in, yet it still happens. There is no way to perfectly secure a company." He considers cyber insurance "a good option because it puts the risk on insurance companies, and you don't have to pay a lot of money out of pocket." You can watch the complete interview here.

Until recently, Data Privacy/Cyber Liability insurance was typically carried by financial institutions, large healthcare organizations, and related industries. However, as more and more organizations increase their reliance on electronic data, the risks are no longer limited to a handful of industries. Your exposure to loss may include retention of employee data; the use, storage or transfer of PII; or the loss of client data while on a worksite.

Many insurance carriers now offer some form of Data Privacy/Cyber Liability coverage to their business clients. Chartis, Ace, Beazley, Hiscox, and The Hartford currently provide some of the most comprehensive coverage options. Insurance carriers can tailor coverage for organizations of all sizes and diverse exposures to loss. Basic Data Privacy/Cyber Liability programs are relatively inexpensive. However, keep in mind that not all programs are equal. Typically, lower cost means less comprehensive coverage.

Here are a few things that you should look for in a comprehensive Data Privacy/Cyber Liability program:

- Business Interruption coverage for any network outage, including extra expense
- Cyber Extortion coverage
- Enterprise-wide data privacy and unauthorized access coverage to include both electronic and non electronic information
- E-Media coverage for advertising injury
- Broad definition of data privacy wrongful act to include failure to prevent identity theft or credit card and debit card fraud
- Coverage for unsolicited electronic communication (Spam)
- Broad definition of insured to include Directors and Officers
- Employee unauthorized access to include actions by a rogue employee
- Regulatory fines, fees, and penalties, as well as expenses related to an investigation included in coverage
- Breach notification costs that include credit card monitoring, attorney fees, and forensic investigation costs
- Coverage for breaches resulting from a service provider or guest

Today's cyber criminal is targeting small-to-midsize organizations. While prevention, detection tools and internal policies and procedures help mitigate this risk, a comprehensive Risk Management program would also include risk transfer. Data Privacy/Cyber Liability insurance policies are relatively inexpensive and readily available in the marketplace. If you are concerned about your loss exposures and interested in learning more about this coverage, consider talking with one of our Data Privacy/Cyber Liability specialists.