Risk to Entities Regarding Data Breaches
Lessons From a Brief Case Study

With the expansion of technology, especially the Internet, organizations have reaped many benefits. But these advancements come with some risk and threats, both to individuals and organizations. One of those threats is referred to as cybercrime, where bad guys do not wield guns and force to rob you, but use technology, stealth and cunning. One popular crime among cybercriminals is identity theft, which has become rampant. Costs of cybercrime in 2011 were an estimated US $1.52 billion in the US alone and US $221 billion globally. These criminals find a bonanza if they can successfully perpetrate a data breach in which they break into a system and database to steal personally identifiable information (PII) (e.g., addresses, social security numbers, financial account numbers), or better yet, data on credit/debit cards (a more direct way to perpetrate identity theft) for a large number of individuals. The recent data breach at Target is an example of such a crime.

**THE PROBLEM**

Even large, sophisticated organizations, such as Target, can have their systems penetrated and lose thousands, even millions, of people’s PII or data on credit/debit cards. There are safety measures that can help prevent this crime, or at least detect it early. But the truth is, many organizations are susceptible and do not know it.

In 2011, 174 million data records were stolen, in 885 different incidents. There were five attacks in 2011 in the US in which more than 10 million identities (PII) were stolen, at a cost of US $194 per capita. In 2012, the Ponemon Institute surveyed 56 organizations about the cost of cybersecurity, and results show the average cost of a data breach for those organizations was US $8.9 million. The same survey found that those entities experienced 102 successful attacks per week.

Organizations of all sizes are at risk. *PC World* says that data breach is a fairly common occurrence among companies of all sizes. In addition, Symantec’s 2013 *Internet Security Threat Report* says that 50 percent of all targeted malicious attacks in 2012 were aimed at entities with fewer than 2,500 employees, and the largest growth area was entities with fewer than 250 employees (51 percent of all attacks).

**CASE STUDY**

A good example is a recent data breach conducted on the Department of Revenue for the state of South Carolina (USA) and its data records in those systems. According to reports, about 3.6 million records were compromised in the data breach. The cybercriminals got Social Security numbers and other PII that can be used to perpetrate identity theft crimes. Thieves also accessed data on 387,000 credit/debit cards. Stolen records contained data from 1998 to present. Fortunately, the state used encryption on recent credit/debit cards, and only 16,000 records were unencrypted. However, cybercriminals are tech-savvy and there is a chance that they could take the time to break the encryption on those records.

The cybercriminal attacked the systems of South Carolina in August 2012 from a non-US Internet address and again in September 2012—this time gaining access to tax returns back to 1998. The attack went unnoticed until 10 October 2012, when the US Secret Service electronic crimes task force detected the crime. It took 10 days for South Carolina to lock down its systems from the intruder and secure its data. To date, no arrests have been made nor has the intruder been publicly identified. It is important to note that South Carolina did not discover the crime itself—there was outside detection. Thus, it is possible the crime would have gone undetected for much longer.

According to South Carolina Governor Nikki Haley, the crime was “creative,” bringing up an important point about data breaches and similar cybercrimes. Cybercriminals, as stated previously, are tech-savvy and, therefore, are fully capable...
of conducting sophisticated, crafty and creative attacks to steal data. A second point, cybercriminals often target their victims specifically. Third, often these attacks are associated with cybergangs that live in countries external to where the perpetrated organizations reside and that may act as safe havens for the cybercriminal. Data breach and resulting identity theft are the new international crime wave.

THE RISK
There are a number of risk factors that might be proprietary to a particular entity. The following are the more common risk factors (albeit the list is not exhaustive):

- Resources to conduct IT repairs, mitigation activities
- Costs associated with protecting PII of customers
- Loss of public image and relations

Obviously, the initial costs are associated with mitigating the vulnerability (loophole) that allowed the breach to occur. IT professionals have to figure out how the cybercriminal got into the organization's system, how to patch it and how to prevent it from happening again. Remember, it took South Carolina 10 days to do all of that. These costs likely include technologies and other purchases as well as the time of many professionals. Sometimes, a consultant or subject matter expert (SME) may be needed to fix the loophole.

Monetary costs related to customers typically involve the organization providing credit monitoring, usually for one year, and sometimes an insurance policy, often for as much as US $1 million, to cover future fraud based on stolen PII. Think about an organization that has 3.6 million such customers/clients and calculate the total costs of these two provisions.

Then, there is the effect of a publicized data breach on the reputation and public image of the victim organization. While it is difficult to put a specific monetary figure to this situation, almost everyone would agree there is some level of cost in this intangible circumstance. It appears Target has suffered some of that loss in its recent data breach.10

Finally, there can be legal fees. If individuals sue the victim organization for not protecting their PII, the victim has to pay to defend itself because it is a victim of a cybercrime—a paradox to say the least. Settlement costs can be significant, and if the case goes to court and the organization loses, there may be stiff costs associated with the court's decision.

EXECUTIVE SUMMARY
Executives need to understand that the risk is not just that their organization can become a victim of a data breach or may end up in court. The risk goes beyond that. There is a new expansion of legal risk.

Over the last few years, about 46 US states have passed a security (data) breach law.11 On 25 August 2013, the new breach notification regulation of the European Union (EU) came into force for electronic communication service (ECS) entities.12 Businesses in the US that fall victim to a data breach may also be found guilty of a violation of one or more state security breach laws. A few years ago, Choicepoint.com had a breach that cost it millions of dollars in fines and mandatory security audits for years.

In June 2012, the US federal government crafted a bill and is attempting to pass a federal security breach law similar to those enacted by those 46 states. The bill, which should ultimately replace state laws, contains language to specifically define a breach and set a national standard in the US for data breach notification to the victim's clients. It would also set maximum damages the victim would have to pay its clients.

But more than the pending US federal law is the legal risk of existing laws and the way courts are interpreting them. Until a couple of years ago, courts dismissed a lot of claims of damages from data breaches similar to the one in South Carolina. Victims had to show specific damages and often the data would have been stolen, but the cybercriminals had not used any of the data...yet.

Now judges are allowing class-action suits related to data breaches. They are also considering the fact that there is a lag between the theft of PII and the use of PII to conduct identity theft crimes that do involve monetary damages, but not until weeks or months after the theft. Now judges consider lawsuits that can show a real possibility of future damages. Organizations will need to make sure their insurance is adequate to handle this rare, but possible, event.

Although it is impossible to prevent all data breach attacks, the courts have taken a stance on reasonable protection. The metric for that reasonableness is best practices in cybersecurity to protect against a data breach. That is, the more the entity has adopted those best practices, the less likely the court is to settle on behalf of the plaintiff or the lower the settlement. Conversely, the less the defendant has employed best practices, the more likely the judge or court is to rule in favor of plaintiffs and award higher settlements.
According to a study by Temple University Beasley School of Law (Philadelphia, Pennsylvania, USA), in the case of a lawsuit associated with a data breach, the average settlement award is US $2,500 per plaintiff and the average attorney fees are US $1.2 million.\(^\text{13}\) As can easily be seen, the potential legal costs are a significant risk that no executive wants to have to address as the result of a data breach. These costs are additional to the ones mentioned in the last section.

**SOLUTION**

IT auditors need to be informed and capable of assisting organizations in preventing data breaches, as much as possible. That prevention must start with an evaluation of the risk associated with a data breach. If an organization maintains PII of individuals who are basically customers, then the higher the number of such customers, the higher the inherent risk. In the previously discussed case of South Carolina, the initial risk assessment is quite large, with millions of customers. In such cases, the IT auditor must assist management in evaluating its level of security over PII. It could be that the entity has sufficiently addressed the risk by employing the necessary best practices, but a security audit by the IT auditor should help make a relatively definitive assessment. But if the entity has not done an assessment, it is likely to be quite vulnerable and susceptible to large costs of a data breach, and it is likely they have not employed a sufficient level of best practices. In this process, the organization should assess the need for the assistance of an IT auditor knowledgeable about data breaches.

**CONCLUSION**

IT auditors need to be aware of the basics regarding data breaches. This begins with a risk assessment based on size, assets that are high-profile targets and having security controls in place. It also includes a basic understanding of the best practices in security: vulnerabilities assessment, patching them, weaknesses in a perimeter and encryption. These special skills, knowledge and abilities are needed more than ever.

Entities that maintain large databases of individuals and their PII should be prepared for a data breach by doing due diligence, as defined by cybersecurity professionals. That includes such preparation as ensuring that an adequate level of best practices have been employed, and an incident response plan is in place to handle all of the aspects of risk and costs mentioned herein. IT auditors should be key resources to accomplish these tasks.

**ENDNOTES**

7 Op cit, Symantec, p. 4
8 Most of the facts on the case study were taken from Bonner, P.; “S.C. Taxpayers’ Social Security Numbers, Credit Cards Hacked,” Journal of Accountancy, 1 November 2012, www.journalofaccountancy.com/News/20126778.htm
11 The only US states without a data breach law are Alabama, Kentucky, New Mexico and South Dakota. Puerto Rico and Washington DC also have data breach laws.