Boy Scouts

IN THIS ISSUE:

WHAT ARE YOUR RESPONSIBILITIES IF YOU GET HACKED?

What are the damages to your reputation? How will you respond? This article will address some of the main concerns of data breach and how a hacker's fun quickly becomes your responsibility.

If a company is hacked, they can be held responsible for proving what was hacked and when and what records may have been accessed. Even if data is encrypted, the burden of proof can still fall on the company to know if it was actually encrypted at the time of the data breach. They are also responsible to notify anyone who may have had their personal information accessed. Let me state this again. Any record of any person who has personally identifiable information on your database must be notified and provided credit monitoring at the company's expense.

What is Personally Identifiable Information (PII)? The US GSA states: "The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, **it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual."**

Even if you store data on a cloud or contract your IT services, you are still at risk and will be held responsible in the event of a breach. Here are some facts surrounding Cloud Exposures.

- Increasing use of cloud services can increase the probability of a $20 million data breach by as much as 3 times
- 36 percent of business-critical applications are housed in the cloud, yet IT isn't aware of nearly half of them
- 30 percent of business information is stored in the cloud, yet 35 percent of it isn't visible to IT*

Perhaps you don't store data on a cloud, you can have information hacked by any one of a million ways. Internet access, theft of laptops, computers or even paper. You can have 999,999 airtight securities in place, but it only takes one flaw for a hacker to get in and leave you to clean up.

The average cost per record that is hacked: $201**. If you have 100 employees and 1,000 online purchases, you could be looking at a cost of $221,100. That's a lot of popcorn.

What you should do:

1. Add securities, encryption and firewalls. Contact a security expert in data breach prevention.
2. Consider storing less data. Making sure to dispose of data properly.
3. Contact USI or have your agent contact USI to purchase a product that will pay for your expenses if breached. Make sure it includes stolen laptops and paper as well.

Even if you store data on a cloud or contract your IT services, you are still at risk and will be held responsible in the event of a breach.

**Ponemon Institute LLC, Data Breach: The Cloud Multiplier Effect, 2014*

***Ponemon Institute LLC, Cost of a Data Breach Study: Global Analysis, 2009, 2014*

FOR MORE INFORMATION CONTACT:

USI Colorado LLC Program Administrator, Leah Gearhart | leah.gearhart@usi.com | 800.873.8500 | bsa.usi.com