Data Breaches and How to Avoid Them - The Boeing Example

March 1, 2017 - Whether your company is big or small, if you have more than one or two employees, the chances are good that you also have a spreadsheet somewhere that contains all of their personally identifiable information. That means you are vulnerable to having a data breach, much like one recently experienced by Boeing. As you will see, a couple of very simple mistakes were all that it took to allow the breach, and with a little planning the breach was entirely preventable.

Boeing's troubles last month began when an employee sent a spreadsheet to his spouse via email. The employee was experiencing formatting issues on the spreadsheet and asked his wife for help, even though the spreadsheet contained data on 36,000 Boeing employees.

Even though the decision process for sharing the spreadsheet is questionable, sharing the document probably wouldn't have triggered state data breach laws if it hadn't contained hidden fields. But it did. Hidden data in the spreadsheet included dates of birth and SSNs.

When the company discovered what had happened, in January, it began to notify affected employees. It also had to make notification to States Attorney General offices in Washington, California, Massachusetts and North Carolina; the states in which the employees live.

Ironically, Boeing makes a software program to scan documents for sensitive information before they are distributed. But the company doesn't apparently use that program except when it is working on classified information. Had it been in use company-wide, it would have prevented transmission of the spreadsheet.

While small businesses may not be able to afford software such as Boeing's, there are still precautions that they can take to prevent a similar breach. For starters, they can install a local search engine on their computers and conduct wildcard searches for things like SSNs. A wildcard search looks for specific formatting rather than for a word or phrase. The question mark (?) symbol is used in these searches to represent any character and the star (*) symbol is used to represent any string of characters. So if you want to find any SSNs on a computer, you would search for "???-??-????" which should return any results that are formatted like a SSN.

Learning how to conduct this type of search on your own computer is a good idea for anyone. For small companies, it is

really essential because it will find data in files that may be hidden. Conducting a search like this on all of your computers can also help to ensure that only employees with an actual need to know will have access to sensitive information. There are a number of reasonably priced software programs on the market that you can use to conduct this type of search.

Most small companies have very little idea what is stored on the hard drives of employee computers. And if your computers have been used by multiple employees over many years, it is likely that they have a lot of information on them that the current users don't even know about. That's dangerous.

In addition to finding out what information is stored on computer systems, companies also need to train their employees. Although we don't know that Boeing's policies forbid employees to share data in the way that this particular employee did, it is quite likely that they do have such a policy. In that case, it is also apparent that the employee involved in this data breach wasn't adequately trained. Every company needs to have cybersecurity policies in place and made sure that their employees understand that violating those policies could result in discipline, right up to loss of job. But you can't enforce a policy that you haven't put in place. And you can discipline an employee whom you haven't bothered to train.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS