TULSA WORLD

Business Viewpoint with Tom Vincent: Early investments can pay off in protecting company information

By Tom C. Vincent II Business Viewpoint | Sunday, September 11, 2016

A breach of a company's information security, and the theft or loss of sensitive data, can be very expensive. These costs can often be reduced, however, by making investments in the security of the company's information – and that of its customers – before an incident occurs.

Tom Vincent II of GableGotwals

The sixth annual Benchmark Study on Privacy & Security of Health Care Data, published by the Ponemon Institute in May of this year, estimates the average cost of a breach for health care organizations at more than $2.2 million. Direct costs may result from damages to individuals whose information is compromised, with additional costs coming from ransom paid to free company data. Ransomware – programs that encrypt system files and lock out users until a ransom is paid – is expected to result in payments of over $1 billion in 2016.

But what about the indirect costs of a breach? As anyone who has experienced a breach of their own personal information can attest, there are often hours of time spent reviewing financial account statements, electronic communications and contract terms to determine what your liability and recourse is – and that doesn't include any affected third parties that must be contacted as well. Compounding the cost is the impact that all of this activity may have on your normal day-to-day schedule – whether resulting in time off from work or delaying other productive activities to get back to normal.

The same can be true for the business that suffers a breach, but on a larger and more costly scale. Pulling employees away from their regular duties to focus on damage control and "what happened when" reduces individual productivity and company profits. Forward-looking efforts may give way to remedial tasks – from building your brand to saving your reputation.

Just as with your financial assets, your information is valuable – but not all information is valued the same. A first step for any company is to know what the most valuable information in the company is and protect it accordingly. Depending on the information, it may be subject to federal and/or state requirements both before and after a breach. Development and implementation of appropriate technical and personnel safeguards in line with these requirements may reduce the liability of the company, and appropriate contract language may provide recourse to the company via indemnification and limitation of liability provisions.

It's also important to know not only where your information is but where it goes. Your most valuable information should be the least mobile in the company to reduce the risk of loss and/or theft (by an outsider or employee). Structuring your network to reduce access – and providing independent data backup not accessible from the network – can help to limit the effectiveness of ransomware that gains entry into your systems.

Also, tracking information on the movement of this information (for example, through access logs) may speed the determination of a breach and reduce the need to backtrack should a breach occur. Advance development of a plan in the event of a breach can further reduce the time it takes to notify customers (which in turn may reduce any damage to your reputation).

In addition to technical safeguards, your workforce can provide a line of defense when aware of their roles, from the overall corporate policy to each individual position, in protecting the company's data. The more that information security is seen as important to the survival of the company, the more likely it is that employees will see poor information security as detrimental to their individual welfare within the company.

Incorporating information security in job goals and performance reviews – both positive and negative – gives employees a personal stake in the issue that can translate into both awareness and action to support the company's security efforts.

Finally, by educating its customers in appropriate measures for their personal and business information, companies can increase their customers' information security and the safety of communications from those customers, resulting in greater overall security for the company.

By implementing tactical, targeted measures, companies can help to reduce not only the ultimate direct expense of a breach but also the resulting indirect costs. The earlier such measures are put

in place, the more easily they may be integrated into regular company processes and the less expensive they may turn out to be.

Tom C. Vincent II is an attorney with the law firm of GableGotwals and a former bank compliance officer. His practice areas include banking and financial services compliance and data security.

http://www.tulsaworld.com/business/businessviewpoint/business-viewpoint-with-tom-vincent-early-investments-can-pay-off/article_2eb77ecc-dfc2-553e-a6c4-d9034e882f0d.html