



PAY NOW OR PAY (A LOT MORE) LATER

TEXT BY Todd Newton

As the tax deadline approaches, some people look forward to getting a refund because they managed to pay more on the front end. For others, there's the dreaded news of owing Uncle Sam because they didn't pay enough. When it comes to taxes, it's a "pay me now or pay me later" reality. The same is true for businesses and how they handle one of their most precious assets: their data.

In today's workplace, we keep vast amounts of information about customers and employees on our computers and on storage devices, which allows us to work faster and more efficiently.

From the smallest of "mom and pop shops" that keep their customers' credit card numbers on file to the larger companies that keep sophisticated and detailed records on individual customers, personal information is literally everywhere. And as the newspapers and cable news shows constantly

remind us, computer intrusions are happening with frightening frequency, exposing consumers to the threat of identity theft and businesses to potential liability for failing to take adequate steps to protect their customers' information.

For many businesses, the decision is, unfortunately, only about the bottom line. In other words, if it costs "too much" to protect the data, then those steps may not be taken because that money could be put to better use "growing the bottom line." Or so the argument goes.

What that mindset fails to consider, however, is the fact that the loss of data to a hacker (or even worse, as the result of a negligent employee who left his laptop at the local coffee shop) can often result in costs far greater than just the cost of upgrading a network or implementing standard security features.

Negligence can often result in costs far greater than just the cost of upgrading a network or implementing standard security.

First, there's the cost of responding to a breach, trying to figure out what was stolen (or lost), by whom, and how to stop the bleeding.

Second, there are the costs of notifying the persons whose information was stolen within a short period of time or else facing the possibility of fines for failing to follow the appropriate notification standards (more on that later).

Third, there could be the costs of settling with government regulators such as the Federal Trade Commission who take a dim view of companies with weak (or non-existent) security policies.

Fourth, there could be the costs of defending the company in the event of a lawsuit, including the costs of an unfavorable judgment. **Fifth**, and arguably the most important, the loss of the company's good name. But it doesn't have to be this way.



Companies can (and should) take proactive steps to protect themselves and their customers from the horrific nightmare of identity theft or money drained from compromised financial accounts.

First, companies should consider hiring an outside computer security company to perform an audit of their network. Just think of it like you would a routine check-up at the doctor: it's worth your time and money to have a trained physician check you out before anything goes wrong. After all, that little pain in your chest could be the sign of something worse just around the corner.

Second, companies should undertake their own audit to determine the types of information they retain, where they retain it, and how it's protected, if at all. By knowing this information, a company that is victimized by a hacker can more quickly respond when it gets the news that it's been hacked. And by knowing the type of information that was compromised, the victimized company can more quickly comply with its obligations to notify its affected customers.

What obligations, you may ask?

Very simply, a majority of states have victim notification laws that provide specific instructions on what companies must do if their data is stolen, and many of those states provide for fines for companies that fail to comply. Trying to wade through that swamp after a breach has occurred is almost a guaranteed way to get bitten.

Third, companies should prepare for the worst before it ever happens. By planning in advance for a breach, companies can effectively respond to a breach when it happens by promptly notifying any affected customers, contacting any governmental authorities that may have regulatory oversight, etc.

These are just a few of the steps that companies should take to protect themselves and their customers. By doing so, companies can avoid the nightmare scenario of paying a lot more later.



Todd L. Newton is counsel in the Little Rock office of Mitchell, Williams, Selig, Gates & Woodyard, P.L.L.C., and is a member of the firm's Information Management and Security Team which advises clients on data security and electronic discovery issues. Prior to joining the firm, he served almost seven years as an Assistant United States Attorney in Little Rock, handling a variety of cases involving cybercrime, public corruption, and asset forfeiture.