

It's important for lawyers new to in-house to recognize that corporate executives may assume that you are an authority on data security and privacy or, that you "have it covered." And yet, if you are like many in-house counsel, your expertise may lie solely in litigation, labor law, or transactional areas.

## Data Security in a Digital World

BY ADAM PALMER and TIM S. McCLAIN

Does your company maintain personal information on clients and employees? If you just answered "no," maybe you need to rethink your definition of personal information. Personal information can be as simple as a name, address, driver's license number, social security number, or bank account number. If you are in-house counsel at a company of any size, you may be aggressively protecting your brand name and intellectual property. Chances are, however, that you are not applying the same aggressive protective measures to all of the private data within the control of your company. In today's digital internet age, huge amounts of personal information can be lost in an instant of carelessness or theft. If your company maintains files with personal information, you must ask yourself, "Am I prepared to respond when we have a data breach or loss?" Notice the word "when" rather than "if." Chances are high that your company will experience a data breach/loss of some sort within the next three years.

The nightmare can be real. In May 2006, Tim McClain was general coun-

sel of the US Department of Veteran's Affairs (VA) when he received a phone call in the middle of the night informing him that a laptop computer holding personal information of about 26.5 million "clients"—American veterans served by the VA—had been stolen and potentially compromised. While this incident has become the poster child of data breaches, in the intervening 15 months, more and more companies have found themselves similarly at risk. For inside counsel, the stakes continue to grow.


Companies often have negotiated contractual obligations to protect confidential and trade secret information of customers, vendors, and business partners. Companies aggressively guard against theft or loss of intellectual property, however, the loss of sensitive employee and customer information can be just as damaging. Lose trust with your customer and you may lose the customer. Additionally, the media and public are paying increased attention to privacy breaches. Companies risk significant public embarrassment—not to mention potential litigation—if they fail to appropriately safeguard private and confidential information. Courts nationwide are also taking an increasingly intolerant view of companies that fail to take reasonable efforts to protect sensitive employee and customer data.

The digital age has significantly increased the risk of data losses. The internet remains the Wild West of security with hackers, often using highly sophisticated methods, trolling for systems with weak security and easily available data that can be stolen. Employees may blog or allow file sharing programs open ac-

cess to wrongdoers who can download confidential information. Vast amounts of personal information can be released onto the internet where it becomes a very difficult task to recover the data.

As was demonstrated with the VA data loss, laptops are portable and easily stolen or lost. Worse still are the powerful flash memory cards, often carried casually on key chains, potentially containing vast amounts of confidential information.

It might be easy to conclude that data security is just about risk management. However, a well-designed and well-managed privacy and data protection program may actually improve your company's bottom line revenues. A culture of privacy and security is simply good business. Business-to-business and business-to-consumer companies in today's environment are seeing sales directly influenced by their privacy reputation and performance.

If you have not already adopted an aggressive plan for preventing data security losses or handling a loss, it may be worthwhile to rethink your data security. Consider your internal policies and IT solutions to controlling data such as monitoring internet traffic that may contain early leaks of sensitive information. You may want to also consult outside counsel to develop a comprehensive data retention and security plan. You also should maintain awareness of what Congress is doing to address data security and privacy. This is definitely an area where it pays to be proactive before there is a problem that lands your company in the headlines, or results in a lawsuit or a serious loss of customer trust. 

*Have a comment on this article?*  
Email [editorinchief@acc.com](mailto:editorinchief@acc.com).



ADAM PALMER is general counsel and chief security counsel for Cyveillance, the world leader in cyber intelligence. He is the vice chair for the New to In-house Committee. He can be contacted at [apalmer@cyveillance.com](mailto:apalmer@cyveillance.com).

TIM S. McCLAIN is a lawyer with Womble Carlyle Sandridge & Rice PLLC, in their Washington, DC office. He was a former general counsel of the US Department of Veterans Affairs. He can be contacted at [tmclain@wscr.com](mailto:tmclain@wscr.com).