COMPUTER AND TECHNOLOGY SECTION

Circuits

Newsletter of the Computer & Technology Section
of the State Bar of Texas

Volume 2: Fall 2014

TABLE OF CONTENTS

Every Company is an Internet Company Now

By Jason Smith

So you think you're not in the online business? Think again. Whether it's directly offering products and services over the Internet, telecommuting employees or just communications on mobile devices, today, every company, large or small conducts business online. While the security around online-based businesses and telecommuting employees is quite mature, the mobile ecosystems remains a virtual wild west.

Mobile devices can be defined as cell phones, tablet computers, portable hard drives, USB flash drives, laptops, etc. The obvious benefits of portability, flexibility and accessibility have driven the growth in use of such devices in corporate America. For instance, an 8 GB flash drive that is smaller than a business card can hold the equivalent of 640,000 boxes of paper. A portable hard drive which is a little larger than a cell phone can store more than 40 million boxes of paper. Unfortunately, portability provides opportunities for loss of important data on a much larger scale than simply misplacing a confidential file folder. This article will highlight the risks of the mobile ecosystem that should be keeping GCs awake at night.

Risk #1: Hackers targeting your corporate systems

From 2010 to 2013, the number of corporate data breaches had more than tripled from almost 600 to over 2,100.[1] The number of records affected by those breaches skyrocketed from 18.6 million to over 800 million. Hacking accounted for almost 60% of incidents, and over 70% of leaked records. At an average cost of $204 per record, the estimated total hard cost of these breaches was more than $163 Billion, and only for those breaches that were reported. Of course, the potential soft cost of these breaches is immeasurable. It was hard enough to defend these attacks in a central location, but with the growth of the mobile ecosystem, the company walls are dissolving into a borderless virtual world.

While a company's responsibility for protecting data is governed by general business principles and the financial implications, there are also laws governing the level of security a company must implement as well as actions that must be taken in the event of a data breach. Texas is among 46 other states which impose a duty to notify on any person who conducts business in the state in the case of an unauthorized disclosure of personal information. Chapter 521 of the Texas Business and Commerce Code establishes a reasonableness requirement for the procedures that companies must take to avoid disclosure of sensitive personal information of

[1] http://ow.ly/Dt1pl

customers and clients. Initially, notification was required to be given to any "resident of the state" but effective last September, the statute was changed to require notification to "any individual" affected – regardless of jurisdiction. So far, Texas has not yet followed the five New England states that have added a duty to notify the state's Attorney General during law enforcement investigations. Texas' breach/notification law affords the Attorney General injunctive relief and painful fines for companies that lose sensitive personal information.

Developing a comprehensive data security policy must include every electronic system, including mobile devices, to be effective and executives must understand that the laws require certain data breaches to be thrust into the public spotlight. But your data security is only as good as your weakest link.

Risk #2: Hackers targeting law firms

On November 1, 2009, the FBI issued an advisory warning[2] to law firms that they were being singled out by hackers with 2011 seeing an increase in law firm breaches reported by more than 80 firms.[3] In addition to the cases of identity theft from family law, probate and tax firms, the biggest threat appears to be corporate espionage targeting firms that represent companies on securities, intellectual property and mergers and acquisitions deals. Firms are being specifically targeted because hackers realize that law firm computers typically house the most high-value data of its client companies -- and not in a corporate-secure data center. Worse, today's hackers are usually professionals sponsored by sovereign states.[4] While lawyers are additionally governed by ethical rules, you should certainly consider extending your technology and privacy policies to your next version of Outside Counsel Guidelines.

In fact, many of the largest U.S. financial institutions are now mandating that the law firms representing them assume stronger cybersecurity measures. From complete background checks on lawyers that handle personally identifiable information and on-site audits to determine the level of access to information to other more stringent compliance procedures. The ABA is getting involved as well. In May of this year, they passed Resolution 109[5], advising attorneys to implement a cybersecurity plan to protect client data.

---

[2] *Preventing Law Firm Data Breaches*, ABA Law Practice Magazine Vol. 38 Num. 1 – John W. Simek and Sharon D. Nelson, Esq.

[3] Mandell and Schaffer, *supra.*

[4] *China-Based Hackers Target Law Firms to Get Secret Deal Data* – Michael A. Riley and Sophia Pearson, February 2012

[5] http://www.insidecounsel.com/2014/10/27/financial-institutions-instructing-law-firms-to-be

Risk #3: Your employees and the destruction of company files

Not all of the threats to your corporate information are inbound. The strongest firewalls and toughest encryption techniques are no match for loss of sensitive corporate data by an employee. With mobile devices, this threat is growing exponentially.

The use of portable mass storage devices to easily carry work product while traveling have given employees the flexibility to take the entire office filing cabinet with them on a plane on a device as big as a house key. And like your house keys, these portable mass storage devices can be easily lost or damaged, taking with it mountains of critical corporate data. Sometimes destruction of the information can do as much damage to a company as disclosure or theft. Many companies already have backup routines built into their Information Technology policies, but the growth of the mobile ecosystem, and the expanding space required to house data that's so easily created, is impacting the timing and method for these backups.

Bring your own device ("BYOD") policies are gaining traction to balance the ease of allowing employees to connect personal mobile devices to corporate systems with the IT policies that govern company-owned devices. But these policies may still be vulnerable if that mobile device becomes entangled in a lawsuit or investigation. In one of the most cited cases on the subject the United States Court of Appeals for the Ninth Circuit held that the Fourth Amendment to the United States Constitution does not require government agents to have reasonable suspicion before searching laptops or other digital devices at the border, including international airports.[6]

It has also been reported that the Department of Homeland Security policies now allow federal agents to "take a traveler's laptop computer or other electronic device to an off-site location for an unspecified period of time without any suspicion of wrongdoing." Further, "officials may share copies of the laptop's contents with other agencies and private entities for language translation, data decryption or other reasons."[7]

As more cases like these arise, the balance between flexibility and protection will shift more towards company IT policies becoming more conservative to hedge against the many unforeseen opportunities for destruction or disclosure of sensitive information.

---

[6] United States v. Arnold, 523 F.3d 941 (9th Cir. 2008)

[7] (Nakashima, Ellen (2008-08-01). "Travelers' Laptops May Be Detained At Border: No Suspicion Required Under DHS Policies". Washington Post.)

Risk #4: Lack of visibility

Not all of the risks lie in the disclosure or destruction of the data. With the proliferation of mobile devices that can store and transmit corporate information to and from anywhere on the planet, the field of view becomes much broader for leadership. How can GCs and others in the executive suite, who are required to sign certifications on internal financial controls, be completely certain of their certification if executed contracts are scattered across smartphones and tablets of global sales staff? How can they aware of the risks and obligations facing the company if critical proposals are stored on flash drives under an employee's car seat? What about the important documents related to a pending merger housed on a laptop at a lawyer's vacation house? Implementing a strategic information lifecycle management program, including systems that focus on workflow and storage of business information will help narrow the field of vision for executives looking to maintain visibility into the affairs of the corporation.

Conclusion

To compete in the fast-paced, plugged-in global marketplace, companies have to embrace the mobile ecosystem while recognizing that the threats are growing as fast, if not faster, than the technology world itself. Executives must maintain vigilance while keeping pace with the brave new world. Sure, there are a growing number of dangers in an always-connected world, but when harnessed properly, the advantage can mean exponential growth to the business. The companies that succeed won't necessarily be the ones who outpaced their competitors in the marketplace, but those who outpaced the threats in the mobile ecosystem.

About the Author

Jason Smith is Senior Director and Legal Counsel for Apttus. He is the former chair of the State Bar of Texas Computer and Technology Section and currently sits on the Social Media Committee for the Corporate Counsel Section. He is a frequent speaker on cybersecurity, data privacy and legal technology issues. You can follow him on twitter @TJSmithEsquire. He can be contacted at jsmith@apttus.com.