MAY 2010

Privacy Law Alert

from the Privacy & Information Security Group of Poyner Spruill LLP

Bad Behavior = Bad Press

Employee Behaviors That Spell Trouble for Your Information Security Compliance Program

by Elizabeth Johnson

In the world of privacy and information security compliance, your employees can either be your greatest source of risk or your first line of defense. How so? A well-trained employee can be the difference between a significant data breach and a near miss. Recent headlines reveal how employees' inadvertent mistakes led to these widely publicized information security breaches:

- Properly trained, your employees will not inappropriately download and take home with them files that include the Social Security numbers of millions, only to have their laptops stolen. Actual headline: "VA Loses Data on 26 Million Veterans: Employee Claims Laptop With Sensitive Data Was Stolen."
- Properly trained, your employees will not use peer-to-peer file -sharing programs on their work computers, potentially exposing files they did not intend to share. Actual headline: "Widespread Data Breaches Uncovered by FTC Probe: FTC Warns of Improper Release of Sensitive Consumer Data on P2P File-Sharing Networks. (More than 100 organizations were affected.)"
- Properly trained, your employees will not print identification numbers on external mailings that inadvertently expose the recipients' Social Security numbers. Actual headline: "Citi Apologizes for Envelope Gaffe (It affected 600,000 customers)."
- Properly trained, your employees can help ensure that malware does not infiltrate and expose personal information by avoiding suspicious emails and attachments. Actual headline: "U of C Warns Patients After Computer Virus Hits Medical Records."

These headlines reveal a small sampling of the types of incidents that can result in a legal obligation to notify affected individuals of a security breach. These incidents also result in bad press, unwanted attention from regulators, lawsuits, and lost productivity as your organization responds to the breach. Tens of thousands of these incidents have been reported since 2005, when California became the first state to require breach notifications for affected individuals. Forty-five other states, the District of Columbia, Puerto Rico, and the Virgin Islands have since enacted similar requirements, often requiring notice not only to affected individuals but also to state attorneys general or other regulators.

The Federal Trade Commission and state agencies have been very active in taking enforcement actions based on such incidents, alleging that the inadequate security evidenced by the breach notice letters constitutes an unfair trade practice in violation of federal or state unfair and deceptive trade practices statutes. A common result in FTC cases is a consent order that requires implementation of a comprehensive, fully documented information security program with a third-party audit of that program every other year for 20 years.

So what to do? Unfortunately, there is no easy answer. The best and most effective response is to maintain a comprehensive information security program and fully implement it. It's not enough to have written policies and procedure -- training, including refreshers and reminders, is a critical aspect of an effective information security program.

You can also be on the lookout for the following characters, all well-meaning, and all of whom regularly and unknowingly create risk for their employers. A comprehensive security program with meaningful training will address these behaviors.

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

RALEIGH CHARLOTTE ROCKY MOUNT SOUTHERN PINES WWW.POYNERSPRUILL.COM

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

Telecommuters and Overachievers. These are the employees who take work home, either because they work from home or because they can't get enough of it in the office. Without discouraging either behavior, consider how you can provide them with secure methods to remotely access personal information if necessary to perform their duties. They should not be downloading it to their personal computer, toting it around on portable devices (laptops, thumb drives, CDs, etc.) or in hard copy, or emailing it to their personal email account in order to access it online from home.

The Facebook Junkie. By now, most people realize that social networks are rife with malware, scammers, and hackers. These are sufficient reasons to be cautious in your personal use of social networks (which is done in the office more frequently than might be ideal). But what about legitimate professional use of social networks? If your employees take to the Web, of their own volition or yours, to promote your organization, the FTC has stated that they must disclose their connection to your organization. The rationale is that the employment relationship, if not apparent in the context of a chat room, blog, or social network, may constitute a material fact that would affect a consumer's evaluation of the promotional comment your employee has offered. In addition, organizations are increasingly using social networking as a tool to evaluate potential hires, current employees, and even consumers applying for credit. Depending on the situation, this activity could raise issues under the Fair Credit Reporting Act, the Stored Communications Act, or state privacy tort statutes.

The Marketing Whiz. The best marketers are often the most creative and risk-tolerant. Making your marketing team aware of the overlapping and sometimes inconsistent requirements imposed on direct marketing will help them design a campaign that takes into account your downstream legal obligations. After all, who wants to spend thousands on a campaign to collect mobile phone numbers, only to discover that follow-up text messaging is not an option because the proper consents were not obtained at the time of collection?

The Procurement Specialist. It might be low-cost, quick, and efficient in the short term, but relying on a purchase order to govern your relationship with vendors is not appropriate when they handle personal information on your behalf. Your business is responsible for the privacy and security practices of its service providers, including any security breaches caused by them. When these vendors have access to mass quantities of information (e.g., payroll processors, data hosting services, records storage providers, tech support, employee benefits providers, shredding services, etc.), the risk increases exponentially. A recent study by the Ponemon Institute reveals that 44% of information security breaches are caused by vendors, and the average cost of these breaches was 23% higher. As a result, it's prudent to do some diligence before you hire a provider that will handle personal information. Specific contractual provisions are also a must; a mere representation of compliance with the law will not necessarily address concerns related to confidentiality, secure disposal of information, security breaches, or appropriate security measures. In addition, some federal regulations and certain states require specific contract language, depending on your operations and the nature of the information you provide to vendors.

The Pack Rat. This employee keeps all her files and correspondence, including email, forever. In addition to increasing your company's costs for storing hard copy and electronic records, this behavior increases costs related to discovery in the event of a legal dispute. Accumulating records containing personal information also increases risk of a security breach and, if one occurs, increases the potential magnitude, since a greater number of people may be affected. An effective and fully implemented records management program will minimize this risk. That program should feature, at minimum, an overarching policy, training for your employees, a legal hold overlay to implement litigation-related preservation requirements, a schedule with retention periods that comport to any legal obligations to maintain certain records, and a disposal policy that complies with state laws mandating destruction procedures for certain records.

In order to effectively implement a comprehensive security program, you need to make sure these and other risks are addressed. You then need to ensure that your program has been communicated to employees, preferably via both written policies and procedures and training.

Elizabeth Johnson's practice focuses on privacy, information security, and records management. She may be reached at 919.783.2971 or ejohnson@poynerspruill.com.