NYMITY

Toronto / Washington DC / Brussels
www.nymity.com

Privacy Interviews with Experts
September 2010

Annie Searle

Principal
ASA

Data Protection: Five Simple Mitigation Strategies to Minimize Personal Information Loss

Over the past decade companies have down-sized, outsourced, off-shored, stream-lined and trimmed their staffs and challenged them to do more with less. Today, companies continue to struggle to innovate, rebuild and grow revenue while they also face an incredible responsibility to protect the personal information they hold on behalf of their employees and customers. The stakes are high.

Personal information loss is expensive. It affects the brand, customer and employee retention and the stock price.

Annie Searle identifies five personal information challenges and suggests very simple mitigation strategies that companies can use today to address some of their risks. Some of these may have even been core components of compliance programs that companies have let lapse. Others are new techniques now required because companies have changed the way they do business. Others are a return to old business practices, because the risks are too high. While accountability, metrics and monitoring are seeping into regulations and laws, they have yet to return or be enhanced in many business environments today.

Annie, now principal of ASA Risk Consultants, built and ran an award-winning computer hardware company for 15 years. She went on to spend ten years at Washington Mutual, first as its chief technology architect and then as senior vice president for Enterprise Risk Services. She left JPMorgan Chase in the spring of 2009 to found ASA, whose six practice areas include global response, business practices, information technology, business continuity, corporate and information security. ASA helps companies build resilience to keep operating through crises and natural disasters (www.anniesearle.com)

Nymity: To your horror, you discover your company and some of its leaders are being discussed by employees on Facebook. What do you do?

Searle: First, it's great that someone has brought this to your attention. Most companies do not have social media policies in place, nor is there always corporate guidance given young employees on what is appropriate to discuss in any public context. This is an easy one to fix. Write a comprehensive policy that includes all forms of social media, including sites such as Twitter, Facebook, and My Space. Review your corporate policy on blocking such sites on the corporate network – often access to more business-like sites like Plaxo and Linked In are allowed, which tends to confuse some employees. At Washington Mutual, every employee was required to recertify annually on several computer-based training programs that included the code of conduct (where matters like this would have been handled) to information security tips on personal data protection and the protections that surround any customer's data. Particularly with new and younger employees, it's important to indicate how high a value the company places on employee discretion, including an understanding that internal work discussions remain internal. In today's rather viral environment, it's important that the HR department is providing adequate guidance to those just beginning their corporate careers.

Nymity: In upgrading your online banking program, you find that developers are using non-obfuscated (live) customer data in the test environment to get all the bugs out. What actions do you take?

Searle: A quick look up of Federal Financial Institutions Examination Council (FFIEC) guidance on customer data indicates that data protection standards have been breached. Thus it's entirely possible that examiners will cite this as a longstanding practice that must be changed. Obfuscation programs that mask personal information so that it can be used in a non-production environment are

expensive. If you can't afford such a program, which is the easiest way to automate such a control, your best bet is to set up appropriate controls of the test environment, including careful checks and balances, perhaps even certifications, around testers.

Nymity: A review of employee access privileges turns up suspicious activity by a low level employee with authorized access taking place during regular work hours. Upon investigation you find that credit card fraud has taken place, using confidential customer data. What are your next steps?

Searle: The Carnegie Mellon Computer Emergency Response Team calls this employee an "inside threat," and has written substantial white papers on prevention and detection of such employees (www.CERT.org). Especially in today's anxious work environment where layoffs always seem to be pending, employees may be motivated by financial difficulties or anger and frustration at their work environment. CERT has also identified other types of inside threats to include selling customer information to an outside criminal entity for material gain. A comprehensive security program that allows logging and monitoring to take place when managers identify unusual behavior of employees is advisable. From the customer end, a well-publicized location for customers to report discrepancies or irregularities they detect in their accounts is also advisable.

Nymity: One of your business partners terminates an employee, but fails to terminate all his access. As a result, administrative passwords and event logs relating to customer databases are deleted.

Searle: CERT points out that when you suspend or terminate anyone, employee or contractor, you must remove all access. First, ensure that your company has the appropriate policy and procedure in place to be able to terminate access immediately and at all levels when necessary. Enacting the policy would usually be a function of an information security group, who would act upon the request that would normally come from an HR department. Since this case involves a business partner's employee, it's important to ensure contractually that your vendors perform to the same level of termination controls that your company will in the future. This is best negotiated in the vendor contract itself, or an addendum if the contract is already in place when this is discovered. The vendor policy on termination should mirror the one in place at your company.

Nymity: A disgruntled employee forwards plans of impending layoffs to the media. Later you find that the employee has also been selling confidential customer information.

Searle: Assuming that you already have policies and standards on confidentiality in place, either of these actions would be ground for dismissal. But it is worth it to put into place an education program that teaches managers how to recognize signs that could be associated with such behavior, but which often are not correlated – unexpected absenteeism, conflicts with supervisors or coworkers where a disproportionate amount of anger and/or resentment is being exhibited in the workplace. If managers watch for such signs, then logging and monitoring can be utilized. And I believe managers can be trained in how to detect signs of such behavior.

Nymity: Some of the situations above are ones that most companies knew collectively how to handle within their organization and management structure, however, when layers of staff were eliminated during the downsizing era such knowledge disappeared. How do you recommend returning it to the organization without re-staffing?

Searle: This is a difficult question. The formal answer is that there must be policies and standards in place as well as training for all employees. Assuming that you could bring in a contractor to write the policies and standards, there still needs to be a business owner to oversee the controls set up in those documents and to be held responsible for programmatic integrity around the controls. A legal department can assume responsibility for the compliance-based pieces of the situations I've discussed here. I'm not sure that's enough when we are talking about personal information. Some of the situations described here would be the province of an IT security team. I can't imagine a company not having an IT security team, either in house or on contract.

Nymity: Also, now that some of these crises have been addressed, what are the next steps to avoid being in constant crisis management?

Searle: I think that anxiety in the workplace is likely to be with us for some time, as the improvements to the world economy are incremental at this time. It's incumbent on leaders to try to motivate their employees to see past the anxiety and take pride in the work they do to grow the company in a difficult environment. The steps that would do the most to avoid crisis response mode would involve automating as many controls as possible; and, in the absence of automation, spelling out procedures clearly so that there can be no room for misunderstanding or misinformation where personal information and privacy is concerned.

Nymity: Finally, now that some of these crises have been addressed, what are the next steps to ensure that innovation and data protection as partners, is not only encouraged, but becomes seriously imbedded as part of the core culture?

Searle: It's hard to imbed innovation and data protection without putting authentic and credentialed leaders in charge of the programs that protect personal information. To operate without leaders in areas that involve privacy is to court disaster. That being said, many programs appear to be mediocre and could benefit from rewarding innovation.

Nymity: In closing, what have we not asked that you would like to share with our customers?

Searle: The piece I have not talked about here is from the other side: educating internet users in particular on how to create and store passwords in a responsible fashion; and to understand when they may be the victims of inappropriate data mining efforts.