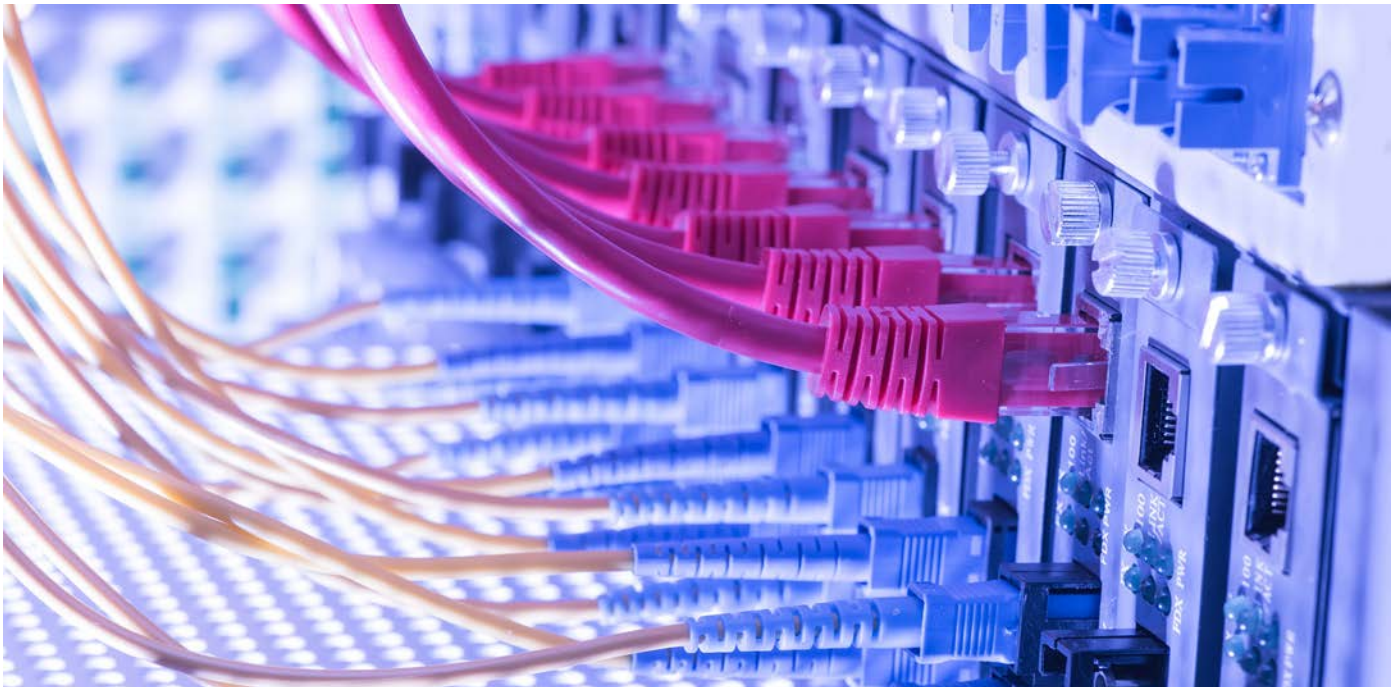

Information Security: Best Practices for Small Firms

Bailey Jung, Owner of Silver Bullet Shredding

Data breaches are occurring with more regularity than ever before. In many cases, human error and specifically, a lack of proper training is to blame. Every organization, regardless of their size, has sensitive business information as well as personal information from employees and clients. Without adequate training and in the absence of proper policies and procedures, organizations put themselves at risk of a privacy breach every day.

High profile breaches involving large organizations make the front pages of newspapers and attract a lot of media attention, albeit unwanted negative attention. While a breach occurring at a small law firm involving personal client information might fall under the media's radar, such an incident can still have serious consequences for the firm involved. The loss of trust, damage to a firm's reputation, a visit from investigators from the Privacy Commissioner's Office, and even lawsuits can result from a privacy breach. Small firms are often more vulnerable to security breaches than larger firms as the latter can dedicate greater resources and better training towards information security. At large firms, a Chief Privacy Officer or a Privacy Manager is responsible for overseeing the firms' privacy program governance. Smaller firms often lack the necessary personnel trained in information security management and as a result, expose themselves to greater risk of a privacy breach incident. In many cases, an Office Manager who hasn't been properly trained is responsible for dealing with privacy related issues.

This article cannot begin to cover all the necessary elements of putting together a proper privacy program to reduce the risk of a privacy breach incident, but it can start the conversation by offering some basic tips and advice. Here are my top five tips for reducing the risk of a privacy breach incident at your firm:

EDUCATION AND TRAINING

At the core of every firm's privacy policy is education and training. Privacy protection and compliance must start at the top. When senior management is committed to ensuring that an organization is compliant with privacy legislation, the program will have a better chance of success, and a culture of privacy will more likely be established. Education plays a critical role in preventing privacy incidents. At the most basic level, every employee should be familiar with the 10 Privacy Principles under Personal Information Protection Act (PIPA). These principles define fundamental privacy rights for individuals and obligations for businesses. Training doesn't start and stop with a company employee handbook. It is an ongoing process that is always changing and evolving.

POLICIES, PROCEDURES, & PROTOCOLS

Every employee should know the firm's policies and procedures for handling personal and sensitive business information. He or she should be familiar with the type of information that falls under current privacy legislation and how that information needs to be protected. Begin by conducting an information audit of your firm. What information do you collect? Why do you have it? Where and how is the information stored? Are proper safeguards in place to protect the information? What are the weak links in your firm's information management system? Does everyone understand proper protocols in the event of a privacy breach? Who takes the lead in the event of a breach? Once-a-year policies and procedures should be reviewed to ensure best practices are being

...continued on page 16

continued from page 15

followed and to address any new threats or vulnerabilities that may have been identified.

LIMITING ACCESS

Access to personal information, sensitive client information, or confidential business information can be a tricky issue particularly at smaller firms where everybody works together in close quarters and security measures tend to be a little looser. Role-based access control is one of the best ways for organizations to limit who has access to what information. In accordance with "need to know" principles, employees should only have access to the minimum amount of personal information they need to perform their duties within the organization. For example, a Human Resource Manager would certainly have a different level of access to personal information than the person responsible for Marketing or Office Services. Limiting access through role-based access control is one of the best practices recommended by information security experts.

ADEQUATE SAFEGUARDS

British Columbia's PIPA states that "an organization must use reasonable, physical, administrative and technical safeguards to protect personal information from unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks (section 34)". Data breaches can often be attributed to human error, carelessness such as leaving a laptop containing personal client information on the front seat of your car, or hackers who have identified a weak link in an organization's infrastructure. You can reduce the risk of a privacy breach at your firm by ensuring proper safeguards are in place. Physical safeguards could include simply locking file cabinets up at the end of the day. Administrative safeguards could include conducting periodic or annual privacy audits to ensure employees are adhering to the firm's privacy policy. Technical safeguards could include using password-protected computer screen savers so unauthorized personnel or visitors cannot see personal information. Another example might be encrypting personal information stored on mobile electronic devices such as laptops and USB flash drives.

DESTRUCTION & A DOCUMENT'S LIFECYCLE

Organizations should have a policy regarding the disposal or destruction of records. Clients

...continued on page 17

SAVE THE DATE

BCLMA Lunch & Learn - Instagram + Twitter 101
Wednesday, January 27, 12 pm – 1:30 pm
Borden Ladner Gervais, Vancouver

BCLMA Biennial 2016 Conference
Conference Kick-off event / Cocktails, Conversation & Creativity
Wednesday, March 2, 2016, 7:00 pm – 9:30 pm
River Rock Casino Resort, Richmond, BC

Conference Day
Thursday, March 3rd, 2016, 7:45 am – 9:00 pm
River Rock Casino Resort, Richmond, BC

BCLMA Annual General Meeting
Friday, April 8, 2016, 12:00 pm – 1:30 pm

BCLMA Annual Summer Social Reception (New Date)
Thursday, June 2, 2016, 5:15 pm – 7:30 pm
Bridges Restaurant, Granville Island

BCLMA Upcoming Survey Schedule
Member Value Survey
Distribution: January 2016 – Publication: February, 2016

Associates Salary Survey
Distribution: March 2, 2016 - Publication: April 1, 2016

Law Firm Economic Survey
Distribution: April 1, 2016 - Publication: June 17, 2016

Biennial Disbursement Survey
Distribution: June 1, 2016 – Publication: June 30, 2016

For more information, visit www.bclma.org

Call for Submissions

Do you have an idea for an article that you think would benefit BCLMA members? Are you itching to put pen to paper (or more likely fingers to keyboard) or do you have an article that you have already written that you'd like to share? We are always looking for submissions!

If you have an article or story idea you would like to submit, please email Sunita March at smarch@cfmlawyers.ca. Please note that our prescribed article length is 750 words. All submissions will be subject to review by the editorial board.

continued from page 16

have the expectation that an organization will dispose of their personal information when it is no longer needed. It is important to keep in mind that each document has its own lifecycle and retention period. Some are two years, others may be five years, and still others may be seven years or even longer. To minimize the risk of a privacy breach, a comprehensive document destruction program involves two components - the destruction of documents whose retention period has expired and the destruction of documents that are generated daily in the normal course of business that often ends up in recycling bins.

No "one-size-fits-all" program exists to prevent data breaches from happening. Data breaches can occur even when the best laid out plans and risk mitigation strategies have been established and implemented. The tips and advice contained in this article is a good starting point for reducing the risk that your firm will be on the six o'clock news.

Bailey Jung is the owner/founder of Silver Bullet Shredding, a Burnaby-based document shredding firm. He can be contacted at 604.708.4200 or bailey@silverbulletshredding.com.

BCLMA thanks our conference sponsors for pledging their support!

Platinum

DYE & DURHAM CORPORATION

SHAWSABEY

Gold

ARLYN • RECRUITING

Worldox

ZSA LEGAL RECRUITMENT

Silver

PORCHLIGHT FINANCIAL

dyrand systems

bmcnetworks inc. TECHNOLOGY SERVICES

RICOH imagine. change.

#bclma2016