IMPORTANT NOTICE:
This Publication Has Been Superseded

See the Most Current Publication at

https://thesedonaconference.org/publication/Sedona_Canada_Commentary_on_Privacy_and_Information_Security

wgs

The Sedona Conference

The Sedona Canada Commentary on Privacy and Information Security for Legal Service Providers: Principles and Guidelines

A Project of The Sedona Conference
Working Group 7 (Sedona Canada)

October 2019
Public Comment Version
Submit comments by January 10, 2020,
to comments@sedonaconference.org

The Sedona Canada Commentary on Privacy and Information Security for Legal Service Providers: Principles and Guidelines

A Project of The Sedona Conference Working Group 7 (Sedona Canada)

OCTOBER 2019 PUBLIC COMMENT VERSION

Author: The Sedona Conference

Editor-in-Chief: David Outerbridge

Drafting Team:

Molly Reynolds
William Ellwood
David Outerbridge
Duncan Fraser
Sarah Millar
Martin Felsky

Staff Editor: David Lumia

wgs

Preface

Welcome to the public comment version of The Sedona Canada Commentary on Privacy and Information Security for Legal Service Providers: Principles and Guidelines, a project of the Sedona Canada Working Group (WG7) of The Sedona Conference. The Sedona Conference is a research and educational institute that exists to allow leading jurists, lawyers, experts, academics, and others to come together in conferences and mini-think tanks called Working Groups to engage in true dialogue, not debate, in an effort to move the law forward in a reasoned and just way.

I thank all of the drafting team members for their dedication and contribution to this project.

This *Commentary* builds on similar principles and guidelines regarding privacy and information security for legal service providers produced by the Sedona Conference Working Group 1 for the United States. However, these Principles and Guidelines focus on the regulatory and practice requirements of the Canadian legal profession.

We hope our efforts will be of immediate and practical assistance to legal service providers, related third-party service providers, and their clients. Please note that this version of the *Commentary* is open for public comment, and suggestions for improvement are welcome. Please submit comments by January 10, 2020, to comments@sedonaconference.org. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be.

Craig Weinlein
Executive Director
The Sedona Conference
October 2019

Table of Contents

Executive Summary

The Principles and Guidelines set out in this *Commentary* are designed specifically for lawyers, law firms, and other legal service providers ("LSPs"). They address the privacy and information security protections that LSPs should implement in order to protect themselves and their clients, and comply with legal and ethical obligations.

Advances in technology present new risks to privacy and the security of information that LSPs hold. Personal and confidential information ("PCI") is increasingly vulnerable to unauthorized access, loss and theft. Yet the ethical responsibility and legal obligation of LSPs to protect such information has not changed. Nor does an LSP's duty depend on the size or resources of the professional who holds such information.

While the duty is constant, the means of fulfilling it will vary. Effective privacy and information security does not allow for, or require, a one-size-fits-all solution. The nature of the information, the needs of the client, the circumstances in which the information is held, and other factors affect the methods that an LSP should adopt to protect PCI entrusted to its care.

Perfect security practices are not achievable. What is required are well thought-out policies and practices—rigorously and systematically implemented and updated over time—that are both reasonable and appropriate to the circumstances.

This *Commentary* is intended to help all LSPs—sole practitioners, law firms of all sizes, paralegals, law clerks, and legal support entities—determine which policies and practices are best suited for them. They aim to give practical guidance to LSPs by exploring "real-life" scenarios involving the loss of PCI, or the breach of security measures designed to protect it, commonly experienced in practice. Examples will be explored throughout this *Commentary* to illustrate the Principles and Guidelines in action.

The *Commentary* is divided into four sections.

Guiding Principles: Section I sets out six governing principles that should guide all Canadian LSPs when designing and maintaining PCI security programs.

Obligations: Section II examines the ethical and legal obligations requiring LSPs to protect PCI.

Security Risk Assessment: Section III describes the recommended elements of a security risk assessment that LSPs should perform in respect of their practice.

Best Practices: Section IV describes, in step-by-step format, recommended best practices for the development of appropriate policies and practices to protect PCI. The table of contents for Section IV serves as a high-level checklist of these best practices.

I. GUIDING PRINCIPLES

A. Introduction

Legal service providers ("LSPs") as well as the third-party service providers ("TPSPs") assisting them[1] in their legal practice rely on various forms of technology to communicate, create, share, and store information in the course of business. Technology poses risks to privacy and information security, including the confidentiality of privileged communications. This *Commentary* sets out a framework for mitigating these risks.

The focus of the Commentary is on personal and confidential information ("PCI"). Personal information is any information about an identifiable individual, such as contact information, medical or financial information, or biometric identifiers such as an individual's voice recording. Confidential information may relate to individuals or legal entities and includes any information subject to a lawyer's duty of confidentiality or a class of privilege.

Ethical rules, statutes, regulations, and the common law all impose duties on lawyers, paralegals, and less directly, on much of the legal services industry, to safeguard PCI belonging to clients and third parties. Engagement agreements may also contain requirements about the safekeeping and handling of PCI. This *Commentary* suggests some prospective and remedial measures that LSPs should consider in order to meet or exceed these obligations.

The discussion in this *Commentary* is informed by the following guiding principles:

Principle 1: **Know the law**: LSPs should know the relevant law in order to identify, protect, and secure PCI they control in their practices.

Principle 2: **Understand the PCI you control**: LSPs should understand what PCI is, and know the types of PCI in their control.

Principle 3: **Assess risk**: LSPs should periodically conduct a risk assessment of the PCI within their control. The risk assessment should consider the PCI's sensitivity and vulnerability, and the harm that would result from its loss or disclosure.

Principle 4: **Develop policies and practices**: After completing a risk assessment, LSPs should develop and implement appropriate policies and practices to mitigate the risks identified in the risk assessment.

---

[1] As used herein, the term "Legal Service Provider" ("LSP" or "provider") includes lawyers, law firms, and any other person or entity directly engaged in providing legal advice and counsel, and the term "Third-Party Service Provider" ("TPSP") includes the other professionals and organizations who play an integral part in the provision of legal services, such as auditors, outside experts, consultants, and eDiscovery service providers.

Principle 5: **Monitor regularly**: LSPs should monitor their operations on a regular basis for compliance with privacy and security policies and practices.

Principle 6: **Reassess**: LSPs should periodically reassess risks and update their privacy and information security policies and practices to address changing circumstances.

B. Principles Explored

Principle 1: Know the law

LSPs must take reasonable steps to protect and secure PCI by understanding applicable requirements for such information.

These requirements arise from many sources, including ethical rules, federal and provincial privacy laws, common law, foreign laws, court rules, and contractual requirements. On a general level, LSPs need to understand the following about the Canadian legal landscape:

- the professional obligations applicable to all members of the LSP, including privacy and confidentiality guidance established by applicable law societies;
- the federal and provincial privacy laws applicable to the LSP, such as the Personal Information Protection and Electronic Documents Act and similar statutes in British Columbia, Alberta, and Quebec;
- the circumstances under which foreign privacy laws may apply to information the LSP is handling, such as when acting on cross-border matters or representing a client based in another country; and
- the terms of any agreements the LSP has signed that govern their rights to use information (e.g., corporate client external counsel guidelines, terms of use for land titles, or drivers' license registries) or give other parties rights to information under the LSP's control (e.g., cloud storage or document review software services).

Principle 2: Understand the PCI you control

LSPs should understand what constitutes PCI.

The following are types of personal information often collected by LSPs**:**

- "know your client" information, such as identity cards, contact details, and billing information
- medical or financial assessments obtained in the course of litigation or estate planning

- due diligence information gathered under a nondisclosure agreement in a corporate or real estate transaction

- employee information, such as Curriculum Vitae (CV), payroll information, and performance reviews

- financial or social security information belonging to customers of the LSP's client

Confidential information controlled by LSPs can include:

- all information provided to the LSP by clients or potential clients;

- information obtained from third parties during the course of providing legal services to a client, such as corporate information about an acquisition target or records relating to an opposing party in litigation; and

- information subject to a confidentiality agreement or undertaking.

LSPs should also understand how this PCI comes into their control, where they store it, who has access to it, and how sensitive it is. LSPs should keep in mind that as technology evolves, the types and methods for collection and storage of PCI may also need to change.

Principle 3: <u>Assess risk</u>

LSPs need to perform a risk assessment tailored to meet the specific needs of their legal environment, including information practices, storage locations, employees, work practices, Information Technology (IT) infrastructure, and client security policies, to name a few. The LSP can conduct the risk assessment on its own or, if unfamiliar with the area of privacy and information security, use a professional or consultant knowledgeable in the area.

Regardless of who conducts the risk assessment, the following steps are key to the process:

- Identify and evaluate the sensitivity of the various types of information within the LSP's control, and the potential harm that would result from unauthorized disclosure, breach, loss, or theft of that information.

- Identify specific threats and vulnerabilities that could result in unauthorized disclosure, breach, loss, theft, alteration, or unavailability.

- Assess the risk of harm posed by each threat or vulnerability.

Principle 4: Develop policies and practices

Each LSP should develop and implement a scaled and prioritized set of policies and practices to respond to any risk to PCI identified in the risk assessment. These policies and practices should:

- factor in and respond to the sensitivity of different types of information;
- respond to the threats and vulnerabilities identified in the risk assessment and minimize the risks that would result in unauthorized disclosures, breaches, loss, or theft;
- respond to client-created data privacy and security requirements while enabling the LSP to meet its day-to-day business needs;
- address privacy and security outside the office environment, in transit, or where data is accessed remotely;
- focus on individual training;
- respond to actual data loss and breaches; and
- mandate how and when information is shared with third parties, such as outside experts, consultants, other TPSPs, co-counsel, adversaries, and courts.

The goal is to keep PCI free from corruption or loss, and accessible only to those who need to use it.

In this regard, larger LSPs should consider hiring one or more full-time employees with expertise in these areas to develop and implement the LSP's policies and practices. As with the conduct of a risk assessment, it is acceptable for smaller LSPs to hire a consultant to address both information security and privacy and assist in creating the LSP's policies and practices in this area. In the end, it is important to have a senior-level person within the LSP's practice who has the authority to implement and enforce the policies and practices developed, and who is held accountable for their success.

Practically speaking, good policies and practices respecting PCI will: (1) limit access to confidential information to those with a bona fide role-based need for access; (2) provide for physical security; (3) implement information access controls (e.g., multiple-factor authentication and attribute-based access control); (4) consider intrusion detection and prevention technologies; (5) employ appropriate use of encryption technologies; (6) provide for secure backup/disaster recovery; and (7) ensure the prompt disposition of information that is no longer needed (and hence at risk of theft or loss with no offsetting potential benefit).

Any policies or practices should include a clear incident response plan to address the unauthorized disclosure, breach, loss, or theft of PCI. The incident response program should include procedures

for: (1) reporting each incident to a designated person responsible for implementing the LSP's response plan; (2) identifying the source of the breach; (3) undertaking steps to stop the breach; (4) investigating the extent of any loss or compromise of private or confidential information; (5) providing appropriate notice to the client, relevant law enforcement authorities, and insurers, as necessary; and (6) abiding by applicable data breach notification requirements.

Human beings are the weakest link in any information, privacy, or security program. A well-designed program to protect PCI will contain robust provisions for training in protecting information, and ongoing monitoring. The best and most effective training sessions are interactive and involve testing to confirm that the recipient understands the material. Accordingly, LSPs should seek to conduct or sponsor formal training at regular intervals (ideally annually) for all personnel.

Principle 5: Monitor regularly

It is important to be vigilant on a continuous basis. Security breaches can come from many sources, internal and external. Breaches may occur at any time, and the damage they cause may spread at incredible speed. Accordingly, to minimize the likelihood of any breach and to mitigate its consequences, LSPs need to engage in real-time monitoring of risk and compliance with policies and practices.

Monitoring should be tailored to the organization. Each LSP should establish a mechanism for assessing the various components of its information security environment, policies, plans, and practices, including those relating to physical security, information-access controls, intrusion prevention and detection systems, encryption technologies, and the maintenance, transfer, and disposition of information. For some providers, such monitoring may be relatively simple and straightforward. Others may need to employ, depending on their industry or situation specific requirements, standard auditing frameworks, such as SSAE 16 (formerly SAS), the ISO 27000 series standards, or another framework capable of being measured, assessed, and improved with demonstrable and documented criteria and according to a fixed schedule. Of course, as technology changes, so will these lists. Periodic auditing for any organization is important and strongly recommended.

Principle 6: Reassess

Once a risk assessment is completed and policies and practices developed, LSPs cannot place the protection of PCI on the back burner.

It is important for LSPs to update their risk assessments on a regular basis and alter policies or practices in response. Threats to security and privacy change constantly. The compliance landscape challenges organizations at every level, arising from industry-specific, provincial/territorial, and federal requirements, and obligations that affect the creation, management, transfer, or disposition of information in non-Canadian jurisdictions. These factors, coupled with constantly evolving technologies, require ongoing vigilance to ensure that the LSP's privacy and security policies and practices remain responsive to changing circumstances.

To be "reasonable and appropriate," security policies and practices should be current; and the best way to keep them current is to stay abreast of developments in the law, technology, and industry best practices. This creates a need to perform two tasks in tandem: (1) conduct *ad hoc* reassessments based on active monitoring of the LSP's actual real-time or near real-time practices; and (2) undertake regularly scheduled (ideally annual) reviews of developments that may concern the LSP's current internal practices or supported programs.

II. SOURCES OF THE DUTY TO PROTECT PRIVATE AND CONFIDENTIAL INFORMATION[2]

The duty to protect privacy and confidentiality applies to all participants in the legal services industry. The duty is multifaceted and derives from a number of sources. The principal sources of the duty are: (1) the ethical rules applicable to lawyers and paralegals; (2) federal, provincial and municipal statutes and bylaws regulating the collection, use, and disclosure of personal information; (3) foreign laws, where applicable; (4) statutory and common-law-based causes of action; and (5) agreements with and instructions by clients.

A. Ethical Rules Applicable to LSPs

The Federation of Law Societies of Canada ("Federation") has developed a Model Code of Professional Conduct ("Model Code") to synchronize professional conduct standards for the legal profession across Canada. The Model Code has been adopted by 12 of the 13 provincial and territorial law societies (in Québec, the Model Code is under review, although the *Code of Ethics of Advocates* is largely harmonized with the Model Code[3]).

This section provides an overview of obligations related to competency and confidentiality under the Model Code that may intersect with privacy considerations. It also provides an overview of applicable guidelines issued by various law societies and the Canadian Bar Association ("CBA").

Although professional standards set out by the Federation and provincial law societies apply directly to lawyers and in some cases paralegals, they also apply indirectly to nonlawyer LSPs working under the supervision of, or employed by, lawyers. Supervising lawyers are responsible for ensuring that their employees and any third parties hired to assist with a specific matter adhere to the rules.

1. Technical Competency Under the Model Code

The duty of competence is set out under rules 3.1-1 and 3.1-2 of the Model Code. A competent lawyer must apply "relevant knowledge, skills and attributes in a manner appropriate to each matter undertaken on behalf of a client."[4]

For most LSPs, legal practice is highly integrated with technology. Although the implications of the proliferation of technology are not explicitly addressed by the Model Code, implicitly, the duty of competence requires lawyers to consider what technology may assist them to practice competently,

---

2 Unless otherwise expressly stated in this *Commentary*, the term "information" includes both electronically stored information ("ESI") as well as information in paper or hard-copy form.

3 Federation of Law Societies of Canada, "Implementation of the Model Code," online: <http://flsc.ca/resources/implementation-of-the-model-code/>.

4 Federation of Law Societies of Canada, *Model Code of Professional Conduct*, r 3.1-1 online: <http://flsc.ca/interactivecode/> [Model Code].

and how to use it. For example, the use of technology may help lawyers meet their obligation to implement necessary skills competently, perform functions in a timely and cost-effective manner, manage their practices effectively, and adapt to changing professional requirements, standards, techniques, and practices. Additionally, the commentary to rule 3.1-2 stipulates that lawyers must recognize tasks that they may lack the competence to handle and take steps to ensure that the client's needs are appropriately addressed.[5]

The implied requirement to use technology may, however, be a double-edged sword, because LSPs' use of technology presents unique ethical challenges when it comes to preserving the confidential or personal information of clients and others. Computers may be accessed by unauthorized users, cellphones holding sensitive data may be lost, and even an email sent to the wrong recipient may involve inadvertent disclosure of PCI.

The Federation has recognized that technological competence—and the risks that may accompany the proliferation of technology in the provision of legal services—are burgeoning issues for legal regulators and lawyers. The Federation has suggested that lawyers should assess and mitigate risks flowing from the use of a particular type of technology.[6] Additionally, clients should be informed of any risks associated with the use of technology throughout the duration of the lawyer-client relationship.

2. Client Confidentiality Under the Model Code

Section 3.3 of the Model Code addresses a lawyer's handling of confidential information. Rule 3.3-1 imposes a general duty on lawyers to: "at all times . . . hold in strict confidence all information concerning the business and affairs of the client acquired in the course of the professional relationship and . . . not divulge any such information."[7]

The duty of confidentiality under the Model Code is broad. It covers all information obtained by a lawyer during the course of the retainer, whether directly from the client or from some other source. The source of the confidential information and the intended use attaching to the information are not relevant for determining whether information is confidential.[8] It is also implied that a lawyer may, unless the client directs otherwise, disclose client information to partners and associates in the law firm and, to the extent necessary, to other LSPs, TPSPs, and administrative staff whose services are used by the lawyer.[9]

---

5 *Ibid* at r 3.1-2, commentaries 5, 6.

6 Model Code, Preface, *supra* note 5 at 7.

7 *Ibid*, r 3.3-1.

8 *Ibid*, r 3.3-1, commentary 2.

9 *Ibid.*

Lawyers who practice in association with other lawyers in cost- or space-sharing arrangements are particularly susceptible to confidentiality breaches and should institute systems and procedures to insulate their respective practices from the risk of inadvertent disclosure.[10]

The duty of confidentiality is owed to every current and former client, regardless of whether the lawyer-client relationship is ongoing.[11] The duty extends to prospective clients seeking advice, even if the lawyer is not ultimately retained.[12] For example, a lawyer generally cannot reveal that he or she has been retained by a client or consulted about a particular matter by a prospective client, unless information about the retainer is in the public domain or there is client authorization to disclose it.[13]

Safeguarding confidential client information presents one of the most challenging ethical responsibilities in the context of technology, particularly because of the wide scope and duration of lawyers' obligations under the Model Code. It is therefore imperative that lawyers specifically consider how to approach the duty in light of the types of technology implemented in their practices. Lawyers should take measures to safeguard client information in all modes of technology employed, including computers, mobile devices, networks, technology outsourcing, and cloud computing.

Rules 6.1-1 and 6.2-2 of the Model Code incorporate lawyers' duties to supervise the work of nonlawyers and law students under their supervision.[14] Lawyers are ultimately responsible if their employee discloses confidential information without authorization.[15] Lawyers should therefore properly vet and train the professionals, administrative staff, and service providers they hire and should have reasonable checks in place to ensure confidentiality is maintained.

3. Law Society Practice Guidelines

Several law societies across Canada have issued nonbinding guidelines intended to help lawyers navigate their professional obligations relating to the use of technology in practice. The Law Societies of British Columbia ("LSBC"), Alberta ("LSA"),[16] Manitoba ("LSM"),[17] Saskatchewan ("LSS"),[18] On-

---

[10] *Ibid*, r 3.3-1, commentary 7.

[11] *Ibid*, r 3.3-1, commentary 3.

[12] *Ibid*, r 3.3-1, commentary 4.

[13] *Ibid*, r 3.3-1, commentary 5.

[14] *Ibid*, rr 6.1-1–6.1-2.

[15] *Ibid.*

[16] Law Society of Alberta, *File Retention and Document Management*, online: <https://dvbat5idxh7ib.cloudfront.net/wp-content/uploads/2017/06/14230254/TAB2_3_File-Retention-and-Document-Management2.pdf> [Alberta File Retention and Document Management Guide]; Law Society of Alberta, *To File or Not to File*, online: <https://www.lawsociety.ab.ca/resource-centre/key-resources/practice-management/to-file-or-not-to-file/>.

[17] Law Society of Manitoba, *Practice Direction 91-01: Destruction of Closed Client Files* (2004), online: <http://www.lawsociety.mb.ca/lawyer-regulation/practice-directions/91-01-destruction-of-closed-client-files>.

tario ("LSO"), New Brunswick ("LSNB"),[19] Newfoundland and Labrador ("LSNL"),[20] and Northwest Territories ("LSNWT"),[21] the Nova Scotia Barristers' Society ("NSBS"),[22] and the Barreau du Québec ("Barreau")[23] all have guidelines for protecting client confidentiality when opening and maintaining client files,[24] as well as practices to follow when retaining and destroying closed files.[25]

Three guidance documents from the LSO are representative of the types of province- and territory-specific practice resources available:

The *File Management Guideline*[26] sets out the essential features of technological and paper systems to: store information regarding clients and opposing parties; open and maintain active client files; close, retain, and dispose of closed files; and identify clients' property and place it in safekeeping. It also urges LSPs to train employees to understand the inherent risks of leaving storage media containing electronic client information unattended or unsecured.

The *Guide to File Retention and Destruction*[27] describes appropriate file handling after a client matter is closed, including regulatory requirements relating to privacy and confidentiality. Specifically, the Guide recommends that any documents retained for use as precedents should be stripped of per-

---

18 Law Society of Saskatchewan, *Retention, Storage and Disposition of Client Files*, online: <https://www.lawsociety.sk.ca/media/9995/fileretentionnov08.pdf>.

19 Law Society of New Brunswick, *Practice Advisory: File Retention and Destruction* (2005), online: <http://lawsociety-barreau.nb.ca/uploads/forms/Practice_Advisory_-_File_Retention_and_Destruction.pdf>. The Law Society of New Brunswick has also endorsed the Law Society of British Columbia's publication *Opening and Maintaining Client Files* (2006), online: <http://lawsociety-barreau.nb.ca/en/for-lawyers/code-of-professional-conduct/opening-and-maintaining-client-files>.

20 Law Society of Newfoundland and Labrador, *Practice Advisory—Concerning File Closure, Retention and Destruction* (2003), online: <http://www.lawsociety.nf.ca/wp-content/uploads/2012/11/Practice-Advisory.pdf>.

21 Law Society of the Northwest Territories, *Practice Advisory: Destruction of Closed Client Files*, online: <http://lawsociety.nt.ca/sites/default/files/documents/LSNT_PracticeAdvisory_DestructionofFiles.pdf>.

22 Nova Scotia Barristers' Society & the Law Office Management Standards Committee, *Law Office Management Standards*, online: <http://www.lians.ca/standards/law-office-management-standards>.

23 Barreau du Québec, *Retention, Destruction and Digitization of Records*, online: <https://www.barreau.qc.ca/en/ressources-avocats/services-avocats-outils-pratique/conservation-destruction-numerisation-dossiers/>.

24 Law Society of British Columbia, *Opening and Maintaining Client Files* (2006), online: <https://learnlsbc.ca/sites/default/files/LSBC_SF_FileManagement_ClientFiles.pdf>.

25 Law Society of British Columbia, *Closed Files—Retention and Disposition* (2017), online: <https://www.lawsociety.bc.ca/Website/media/Shared/docs/practice/resources/ClosedFiles.pdf> [British Columbia File Retention and Disposition Guide].

26 Law Society of Ontario, *File Management Guideline*, online: <https://lso.ca/lawyers/practice-supports-and-resources/practice-management-guidelines/file-management>.

27 Law Society of Ontario, *File Retention and Destruction*, online: <https://lso.ca/lawyers/practice-supports-and-resources/topics/managing-files/file-retention-and-destruction>.

sonal client information. Long-term storage of documents with identifying information, whether it be on-site or off-site, physical or electronic, should be done in a manner that maintains confidentiality and protects the files from loss or damage (such as through use of encryption software).

The *Technology Guideline*[28] addresses confidentiality when using electronic means of communication. The NSBS,[29] the LSM,[30] the LSNB,[31] the LSNWT,[32] the Barreau,[33] and the LSA[34] have similar guidance on how lawyers can protect confidential information when using electronic media. Lawyers can minimize the risk of loss or interception of confidential electronic communications by:

- discussing inherent security risks of particular technology (e.g., portable storage media carrying unencrypted data) with the client;
- using security software to protect information in transit and when stored;
- taking appropriate measures to secure confidential information when using cloud-based services; and
- developing office management practices that protect against inadvertent discovery or disclosure of electronic communications.

In addition, some law societies have resources regarding the use of TPSPs to electronically store or process client information. The LSBC has emphasized the need for the lawyer to ensure that the service provider's policies are in line with the lawyer's professional obligations.[35] This is especially

---

[28] Law Society of Ontario, *Technology Guideline*, online: <https://lso.ca/lawyers/practice-supports-and-resources/practice-management-guidelines/technology>.

[29] Nova Scotia Barristers' Society, *Guidelines on Ethics and the New Technology* (2001), online: <http://nsbs.org/sites/default/files/ftp/tech_ethics_guidelines.pdf>.

[30] Law Society of Manitoba, *Guidelines on Ethics and the New Technology* (1999), online: <http://www.lawsociety.mb.ca/lawyer-regulation/law-society-practice-notices/ethics_newtech.pdf/>.

[31] Law Society of New Brunswick, *Code of Professional Conduct, Appendix B—Guidelines on Ethics and the New Technology*, online: <http://lawsociety-barreau.nb.ca/en/for-lawyers/code-of-professional-conduct/appendix-b>.

[32] Law Society of the Northwest Territories, *Practice Advisory: Guidelines on Ethics and the New Technology*, online: <http://lawsociety.nt.ca/sites/default/files/documents/Practice%20Advisory%20-%20Internet%20and%20Technology.pdf>.

[33] Barreau du Québec, *Guide on the Management of Technological Documents* (2005), online: <https://www.fondationdubarreau.qc.ca/wp-content/uploads/2016/10/Guidetech_allege_FR.pdf>.

[34] Law Society of Alberta, *Computer/Network Security Checklist* (2014), online: <https://dvbat5idxh7ib.cloudfront.net/wp-content/uploads/2017/06/21224619/TAB2_4_Computer-Network-Security-Checklist.pdf>.

[35] Law Society of British Columbia, *Cloud computing due diligence guidelines*, online: <https://www.lawsociety.bc.ca/Website/media/Shared/docs/practice/resources/guidelines-cloud.pdf>. See also Law Society of British Columbia, *Cloud Computing Checklist v. 2.0* (2017), online: <https://www.lawsociety.bc.ca/Website/media/Shared/docs/practice/resources/checklist-cloud.pdf>. See also Law Society of Newfoundland and Labrador, *Loss Prevention Tip*

the case where client information will be stored electronically in another jurisdiction.[36] In such instances, the client should be fully informed.[37] The LSBC has adopted restrictions around lawyers' engagement of data storage services, in the form of amendments to the LSBC Rules.[38] Similar concerns may extend to servers physically located in Canada but subject to foreign ownership interests.

4. The Canadian Bar Association's *Legal Ethics in a Digital World*

The Canadian Bar Association has issued a guideline intended to help lawyers navigate their professional responsibilities in highly computerized practice settings.[39]

The CBA Guideline begins by suggesting that lawyers protect confidential client information through safeguards that ensure the integrity of the information, so that it is not exposed to accidental or malicious modification or alteration.[40] Backing up files is a necessary component of security policies.[41]

The CBA Guideline identifies three categories of security measures, drawn from federal privacy legislation: physical safeguards (like locked filing cabinets and restricted office access); organizational procedures (like security policies and training initiatives); and technological measures (including the use of passwords, encryption software, and firewalls).[42]

Special attention is paid to security measures that should be adopted when sensitive information is transported outside of the office, to prevent third-party access.[43] Encryption mechanisms should be used to secure the information during transport, and accessing the information via a secure Virtual Private Network ("VPN") connection should be considered in lieu of carrying electronic files on a hard drive or USB key.[44] Use of unsecured wireless networks should be avoided.[45] Particular care

---

#15: Protecting Yourself from Cybercrime Dangers: Be Careful About Putting Your Firm Data in the Cloud, online: <http://lsnl.ca/loss-prevention-tip-15/>.

36 Alberta File Retention and Document Management Guide, *supra* note 17 at 9.

37 British Columbia File Retention and Disposition Guide, *supra* note 26 at 19.

38 Law Society of British Columbia, *Law Society Rules 2015*, rr 10-3–10-4, online: <https://www.lawsociety.bc.ca/support-and-resources-for-lawyers/act-rules-and-code/law-society-rules/>.

39 Canadian Bar Association, *Legal Ethics in a Digital World*, online: <http://www.cba.org/getattachment/Sections/Ethics-and-Professional-Responsibility-Committee/Resources/Resources/2015/Legal-Ethics-in-a-Digital-World/guidelines-eng.pdf> [CBA Guideline].

40 *Ibid* at 4–5.

41 *Ibid* at 6.

42 *Ibid* at 1–2, 7–8.

43 *Ibid* at 8.

44 *Ibid* at 7–8.

45 *Ibid* at 7.

must be given when traveling internationally, as electronic devices may be subject to search or seizure by border officials. The CBA Guideline recommends that steps be taken to minimize metadata (background information about electronic documents) or to remove it from files circulated electronically, due to the sensitive information metadata may convey.[46]

Cloud computing tied to servers located in foreign jurisdictions presents a particular concern to client confidentiality, as some foreign governments have enacted legislation that allows them to access such information.[47]

B. Federal Statutory Obligations

The privacy law regime in Canada under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") applies to every organization in the country that collects, uses, or discloses personal information in the course of commercial activities.[48] As organizations engaged in commercial activities, lawyers in private practice and other LSPs must comply with PIPEDA when dealing with personal information.

PIPEDA presumptively applies to all federally or provincially regulated entities, unless the organization is otherwise subject to provincial privacy legislation that has been declared to be "substantially similar" to PIPEDA.[49] The three provinces that have enacted "substantially similar" legislation are Alberta, British Columbia, and Québec. In such cases, the substantially similar provincial law applies instead of PIPEDA, although PIPEDA continues to apply to interprovincial or international transfers of personal information.[50]

The term "personal information" under PIPEDA is broadly defined as "information about an identifiable individual." Information will be "about" an individual when it relates to or concerns the individual.[51] Individuals will be "identifiable" where there is a serious possibility that they could be identified through the use of that information, alone or in combination with other available information.[52]

---

46 *Ibid* at 9–10.

47 *Ibid* at 10.

48 Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 4(1) [PIPEDA].

49 *Ibid* at s 26(2).

50 Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick, Nova Scotia, and Newfoundland and Labrador have enacted privacy legislation as well, but only with respect to personal health information collected, used, or disclosed by health information custodians. LSPs should be aware of these provincial laws, particularly when representing clients who are custodians, as the provisions regarding agency may apply. LSPs should also be aware that some of the statutes contain specific provisions addressing exceptions that are applicable to lawyers and legal proceedings.

51 Canada (Information Commissioner) v Canada (Transportation Accident Investigation and Safety Board), 2006 FCA 157 at paras 43, 59, 61, [2007] 1 FCR 203.

52 *Gordon v Canada (Health)*, 2008 FC 258 at para 33.

PIPEDA stipulates that LSPs may collect, use, and disclose an individual's personal information only with the knowledge and express or implied consent of that individual, unless a legislative exemption applies. The level of consent required depends on the sensitivity of the information and the reasonable expectations of the individual. As an overarching principle, an organization may only collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

PIPEDA mandates protection for all personal information held by an organization. Unlike the duty of confidentiality, it applies to information regarding any individual. This means that PIPEDA may apply not only to information that LSPs collect, use, or disclose in relation to clients, but also to information about others, including adverse parties, third parties, lay witnesses, and expert witnesses. Lawyers should keep in mind that while their duties under PIPEDA overlap significantly with their professional duties, PIPEDA's application is broader and extends to nonclients.

The Office of the Privacy Commissioner of Canada ("OPC") oversees compliance with PIPEDA. The OPC has created a Privacy Handbook for lawyers, entitled *PIPEDA and Your Practice*.[53] The Handbook addresses how sole practitioners and law firms should approach their obligations under PIPEDA. The Canadian Bar Association has published ten guidelines to help law firms ensure that they are compliant with PIPEDA.[54] The comments that follow incorporate guidance from the OPC, CBA, and relevant case law.

1. Establishing Privacy Policies

For most legal practices, the starting point for compliance with PIPEDA will be an assessment of the law's administrative requirements, which include the appointment of an individual who will be accountable on behalf of the LSP for its obligations under PIPEDA (usually referred to as a "Chief Privacy Officer"). Sole practitioners will be required to assume this responsibility themselves.[55]

LSPs must understand how personal information is collected, used, and disclosed in the course of running the practice, and for what purposes. Privacy policies must address the various ways that personal information is handled, including obtaining consents as needed and developing procedures to handle complaints and requests for access to personal information under PIPEDA.[56] The Lawyers' Professional Indemnity Company ("LawPRO"), the professional liability insurer of Ontario lawyers,

---

53 Office of the Privacy Commissioner of Canada, *PIPEDA and Your Practice: A Privacy Handbook for Lawyers*, online: <https://www.priv.gc.ca/media/2012/gd_phl_201106_e.pdf> [Handbook].

54 Canadian Bar Association, *Law Firm Privacy Compliance in 10 Steps* (2015), online: <http://www.cba.org/Publications-Resources/CBA-Practice-Link/Young-Lawyers/2014/Law-Firm-Privacy-Compliance-in-10-Steps>.

55 *Ibid.*

56 *Ibid.*

has developed a Sample Firm Privacy Policy that may be used by LSPs as a precedent for developing procedures for dealing with personal information.[57]

Similarly, LSPs will need to establish (and train employees to apply) policies and practices that give effect to the requirements of PIPEDA. Privacy policies should be made publicly available by, for example, posting on a website.

The OPC has recommended that LSPs pay particular attention to the following objectives:[58]

- ensuring that third parties who conduct work on the LSP's behalf have in place a comparable level of protection while the information is being processed by the third party
- setting retention and destruction schedules for personal information the LSP holds
- establishing procedures to handle requests for access to personal information received by the LSP

2. Collection of Personal Information from Clients and Prospective Clients

LSPs often have to collect personal information from potential or existing clients throughout the retainer. For example, prior to commencing the client-solicitor relationship, a lawyer will likely have to conduct conflict checks and complete client identification in accordance with law society rules. Client consent for collection and use of this information, in the context of the specific purpose for which it is to be used, will have to be obtained. Consent may, however, be implied through a client's act of providing the requested information to the LSP in order to secure the retainer.[59]

LSPs that seek to collect personal information about a client or prospective client from a third-party source, such as via a credit check, should obtain the express consent of the individual.[60] LSPs should, within the requirements of their professional obligations and conflict checking systems, minimize the amount of personal information they keep if the LSP is not retained by the client.

3. Collection of Personal Information from Nonclients

LSPs are often engaged in the collection, use, and disclosure of the personal information of nonclients, particularly in the litigation context. The Ontario Superior Court has commented that PIPEDA does not apply to individual litigants who collect information about an opposing party through a

---

[57] Lawyers' Professional Indemnity Company, Sample Firm Privacy Policy, online: <https://www.practicepro.ca/wp-content/uploads/2003/07/2003-06-sample.pdf>.

[58] *PIPEDA Case Summary No 377, Re*, (April 5, 2007) 2007 CarswellNat 5684.

[59] Handbook, *supra* note 54 at 6.

[60] *PIPEDA Case Summary No 340, Re*, (May 2, 2006) 2006 CarswellNat 5567.

private investigator, because information collected in this context is for a personal purpose.[61] Similarly, the Federal Court of Canada has held that a party may collect, use, and disclose personal information about another party during the course of a civil action.[62] This qualifies as a noncommercial activity, and therefore remains exempt from PIPEDA. This is so even if third parties, such as LSPs or investigators, are retained to assist in the litigation.

Despite the above cases, the OPC is of the opinion that there may be instances where the collection, use, or disclosure of personal information in connection with litigation may engage PIPEDA. For example, litigation involving commercial organizations may be considered as part of their commercial activities and may be distinguished from claims involving individual litigants in their personal capacity. In a 2011 proceeding involving a commercial organization,[63] the OPC found that the organization's civil defence against a customer's claim regarding an incident that occurred on the organization's premises was sufficiently related to its regular course of business to constitute a commercial activity under PIPEDA. A decision of the Nova Scotia Supreme Court goes against this conclusion in the context of a dispute involving a large insurance company. The court in that case held that PIPEDA did not apply to information pertaining to litigation, because the relationship between the company and the other party arose in the litigation itself and was therefore not of a commercial nature. The court commented that "PIPEDA was not intended to apply to litigants in a legal proceeding."[64]

Given the unclear guidance provided by the case law, LSPs should consider their obligations, and those of their clients, under PIPEDA when engaging in litigation. Any personal information that is collected, used, or disclosed in connection with reasonably anticipated or actual litigation should be collected either with the express or implied consent of the involved parties, or under one of the exceptions provided under PIPEDA.

4. Exceptions to Consent

The exceptions to the knowledge and consent principle include collection and use for purposes related to investigating a breach of an agreement or a contravention of the law; disclosure to a lawyer (or notary in Québec) who is representing the organization; and disclosure to comply with a subpoena, warrant, court order, or rules of court relating to the production of records.[65]

---

61 *Ferenczy v MCI Medical Clinics,* 70 OR (3d) 277, 2004 CanLII 12555 (ON SC).

62 State Farm Mutual Automobile Insurance v Privacy Commissioner of Canada, 2010 FC 736 at paras 98-100, 106-107.

63 *PIPEDA Case Summary No 2011-003, Re*, (March 25, 2011) 2011 CarswellNat 6886.

64 *Hatfield v Intact Insurance*, 2014 NSSC 232 at para 27.

65 *PIPEDA*, *supra* note 49 at s 7.

The OPC has found that information collected by a client may be disclosed to its lawyer, under subsection 7(3)(a) of PIPEDA, if the lawyer or law firm is acting as the client's representative.[66]

PIPEDA also permits the nonconsensual collection, use, or disclosure of certain publicly available information from professional or business directories, statutorily created registries, or documents of a judicial or quasi-judicial body that are available to the public.

5. Use and Disclosure of Personal Client Information

LSPs that market their services using information about clients and prospective clients should be aware of how PIPEDA applies to this activity. Business contact information is outside the scope of PIPEDA only when it is collected, used, or disclosed for the purpose of communicating with an individual in relation to their business or profession.[67]

Additionally, LSPs may receive unsolicited personal information about individuals through referrals. LSPs should not assume that consent has been obtained from the prospective client until the prospective client has contacted the LSP.[68]

LSPs may sometimes find themselves subject to information requests from law enforcement authorities and regulatory agencies seeking information about their clients. Although PIPEDA permits organizations to disclose personal information about individuals without their consent upon the request of a government institution with the requisite authority, and as required by law, these exceptions have been narrowly interpreted by Canadian courts. Further, professional obligations of confidentiality may prevent this sort of disclosure.

6. Providing Access to Personal Information

Under subsection 8(3), PIPEDA allows individuals to access personal information about themselves held by an organization by submitting a written access request.[69] Upon receipt of a request, the LSP must inform the individual of the existence of their personal information and provide access to the information within thirty days.

Responding to access requests may pose a challenge for many LSPs. Because PIPEDA allows individuals to access their own personal information in the possession of an organization, LSPs and their clients may receive requests for access to personal information from individuals who are adverse to their client's interests. An LSP contemplating or engaged in litigation must still respond to

---

66 *PIPEDA Case Summary No 218, Re*, (September 5, 2003) 2003 CarswellNat 5816; *PIPEDA Case Summary No 181, Re*, (July 10, 2003), 2003 CarswellNat 5891.

67 Handbook, *supra* note 54 at 7.

68 *Ibid* at 8.

69 PIPEDA, *supra* note 49 at principle 4.9.

and process access requests from such individuals.[70] That said, LSPs should also be aware that access requests are limited to information "about" the requestors themselves. For example, the OPC has found that it was not necessary for a lawyer to grant the bulk of an access request for information related to an estate under which the requestor claimed to be a beneficiary. The requestor was only entitled to obtain information that was specifically about him.[71]

Further, PIPEDA provides a number of exceptions, such as where the information is protected by solicitor-client or litigation privilege; would reveal confidential commercial information; was collected in the course of an investigation into the breach of an agreement or of a law; or was generated in the course of a formal dispute resolution process.

With respect to privilege, the OPC has required that a party be able to prove the claims of privilege it asserts,[72] and information subject to litigation privilege may need to be provided to a requester once the underlying litigation has ended.[73]

7. Safeguarding Personal Information

The law society and CBA recommendations described above to protect confidential information are also applicable to meet the PIPEDA requirement to safeguard personal information. Limitations on access to files and retention of personal information, technological security measures, and ensuring that third-party vendors apply comparable protections are all central to remaining accountable for personal information in an LSP's control.

8. Retention of Personal Information

LSPs must reconcile their professional obligations regarding file retention with the requirements of PIPEDA. While PIPEDA requires organizations to retain personal information only as long as necessary for the purpose for which it was collected, professional regulators may require that information be retained as necessary to defend against any future proceedings or to conduct an assessment or review of the file. LSPs should nonetheless limit their retention of personal information to the minimum required in the circumstances.[74]

---

70 PIPEDA *Case Summary No 352, Re*, (September 8, 2006) 2006 CarswellNat 5578.

71 PIPEDA *Report of Findings No 2013-005, Re*, (October 2, 2013) 2013 CarswellNat 5605.

72 PIPEDA *Case Summary No.* 2008-397, *Re*, (December 18, 2008) 2008 CarswellNat 6817.

73 *Davidson and Williams LLP, Re*, 2011 CarswellAlta 2571, [2013] AWLD 399 at para 129.

74 Handbook, *supra* note 54 at 11–12.

C. Provincial Statutory Obligations

The provincial privacy statutes in Québec,[75] Alberta,[76] and British Columbia[77] that have been deemed substantially similar to PIPEDA contain similar requirements and exceptions to PIPEDA. Although the provincial statutes and PIPEDA share common objectives and are based upon similar key principles, there are some distinct obligations imposed by the provincial statutes that exceed those imposed by PIPEDA.

The main area for uneven privacy law coverage between the federal and provincial statutes is in relation to employee personal information. PIPEDA only applies to information about employees of organizations that are federal works, undertakings, or businesses. In contrast, the privacy legislation in Québec, British Columbia, and Alberta applies to employee information held by provincially regulated organizations in these provinces. Therefore, LSPs that operate in one of these three provinces should be aware that their privacy obligations may extend to their employees.

D. Foreign Statutory and Regulatory Requirements

International privacy is a dynamic area of the law in which consumers, private entities, and government actors seek to balance the considerable benefits of technological innovations with critical privacy concerns. The state of the law in the European Union ("EU") has fundamentally changed since the implementation of the General Data Protection Regulation ("GDPR") in 2018.[78] Among other things, the GDPR implements new protections concerning the transfer of EU citizens' information to non-EU countries.[79] Equally significant, stronger privacy rules have been developed in Latin America, Asia, and certain U.S. states. As a result, many multinational organizations are requesting confirmation that their Canadian legal counsel comply with these laws.

LSPs representing clients based outside Canada, or who are engaged in cross-border files, should consider the application of foreign privacy laws to the PCI they may handle in the course of an en-

---

75 Québec Act Respecting the Protection of Personal Information in the Private Sector, CQLR, c P-39.1.

76 Alberta Personal Information Protection Act, SA 2003, c P-6.5.

77 British Columbia Personal Information Protection Act, SBC 2003, c 63.

78 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 [GDPR], online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents>. A specific Directive (680/2016) on data protection in policing and justice was adopted on May 5, 2016 and applicable as of May 6, 2018: European Data Protection Supervisor *Legislation*, online: <https://edps.europa.eu/data-protection/data-protection/legislation_en>.

79 The GDPR has extraterritorial applicability to cross-border data protection matters. Accordingly, the rights and safeguards provided under the Regulation apply with respect to data transferred outside of the EU: GDPR*, supra* note 79, Article 15.2.

gagement. In some circumstances, it may be appropriate to seek foreign law advice before committing to receive or transmit data subject to international privacy laws.

E. Statutory and Common Law Causes of Action

LSPs should be aware of how security breaches or the collection, use, or disclosure of certain types of information may give rise to liability under statutory or common law privacy torts.

A number of provinces have enacted statutory privacy torts. Sections 35-37 of the *Civil Code* of Québec govern causes of action rooted in privacy rights that can be enforced in the courts. British Columbia,[80] Saskatchewan,[81] Manitoba,[82] and Newfoundland and Labrador[83] have similarly passed Privacy Acts that codify limited rights of action for the willful invasion of privacy. In Ontario, the courts have recognized common law torts of intrusion upon seclusion and publication of private facts.[84]

Additional sources of common law liability for data breaches may include: (1) legal malpractice; (2) breach of fiduciary duty; (3) breach of contract; and (4) general tort, including class action negligence claims. For example, an LSP that misuses a client's confidential information may not only be in breach of professional obligations but may also be subject to claims related to legal malpractice and breach of contractual duty to safeguard client information. Similarly, third parties that are injured following a data breach of an LSP's systems may seek legal redress for their injuries if the breach led to disclosure of sensitive personal information. One need only consider the class actions that have followed major data breaches to appreciate the business case for taking adequate steps to secure sensitive information, no matter whose information it is.[85]

As this is a rapidly evolving area of law, LSPs responding to a breach of PCI should consider whether the circumstances of the incident may give rise to civil liability and consider whether their insurance policies provide coverage for such claims.

F. Client Requirements

A broad range of information security decisions may need to be client-specific, to allow for differences in the client's business judgment and assessment of security risks and costs. When counseling clients about security alternatives, the LSP should document any advice given and ensure that the

---

80 *Privacy Act*, RSBC 1996 c 373.

81 *Privacy Act,* RSS 1978, c P-24.

82 *Privacy Act*, CCSM, c P125.

83 *Privacy Act*, RSNL 1990, c P-22.

84 *Jones v Tsige*, 2012 ONCA 32 [*Jones*]; *Doe 464533 v ND*, 2016 ONSC 541 [*Doe*].

85 See e.g. Drew v Walmart Canada, 2017 ONSC 3308; Elkoby c Google and Google Canada, 2018 QCCS 2623; Lozanski v The Home Depot, 2016 ONSC 5447.

client has access to technology experts. Upon request from the client, the LSP should clearly disclose the nature of the security measures and policies of the LSP and its vendors. Any decision by the client to forego security measures that the LSP recommends should be documented. In addition, the LSP should, when appropriate, counsel the client about potential liability insurance coverage issues and be mindful that in some situations (especially those that may expose the LSP to third-party lawsuits), the LSP should consider whether to decline to provide representation if a client is unwilling to accept recommended security measures.

III. CONDUCTING A SECURITY RISK ASSESSMENT

The touchstone of a sound information privacy and security program is its careful tailoring and scaling to the LSP and its practice. This tailored approach begins with an assessment of risk, considering both the probability and the harm or damage that could be caused by an occurrence.[86] LSPs should determine what privacy and security solutions are appropriate to the circumstances using a risk-based analysis, and subsequently develop and implement a reasonable and appropriate information privacy and security program to mitigate risks. Conducting a security risk assessment is a complex task requiring specialized expertise. The information provided below is not intended to be a substitute for a comprehensive professional risk assessment. LSPs will often need to engage a security expert to design and conduct such security assessments.

To properly assess risk, an LSP must consider the importance of maintaining the confidentiality, integrity, and availability of the information it controls. Taken together, these terms mean that information held by an LSP should be protected from unauthorized or accidental alteration, copying, or deletion. Private or confidential information should be protected from those who do not need to use it. Those who must use it must be able to obtain it quickly whenever they need it.

In security terminology, the basic elements common to almost every risk assessment are:

- Asset Identification and Evaluation: LSPs should identify the types of information they handle (e.g., social insurance numbers, payment card numbers, patient records, designs, and human resources data) and the sources of that information, evaluate the sensitivity or relative importance of each type of information, and rank by priority which types require protection and how much protection they require.

- Risk Profiling and Assessment: Analyze the specific threats and vulnerabilities that pose the greatest risk to information assets, including physical loss or damage. The risk assessment process should also examine obligations already facing the LSP: security precautions for client information may already be addressed in retainer agreements—a salutary practice—particularly if client information is to be stored off-site, including in the cloud. Security for third-party information may often be governed by contract or court order.

- Risk Mitigation and Treatment: Once the sensitivity of information assets has been determined and the sources of risks and threats identified and ranked, an LSP can make informed decisions when developing reasonable, proportional responses to the threats and vulnerabilities identified. The practices discussed in Section IV of this *Commentary* provide a guide for such risk mitigation efforts.

---

[86] See National Institute of Standards in Technology Special Publication 800-30, *Guide for Conducting Risk Assessments* (2012), online: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.

All LSPs should consider scaling and prioritizing their information security practices to fit their particular circumstances as they are known at the time. The focus should always be on what is reasonable and appropriate. To determine that, an LSP should first evaluate the type of information it has, who uses the information, and how they use it. The LSP should also consider which of its employees should have access to information, when they should have it, and whether they have put in place effective measures to prevent unauthorized access. All providers have challenges ensuring security for PCI, but ultimately all need to scale their security programs to meet their own and their clients' needs.

IV. GUIDELINES FOR POLICIES AND PRACTICES THAT ADDRESS PRIVACY AND INFORMATION SECURITY

Information security policies and practices should be scaled to the circumstances of the LSP and the needs of its clients. They may be simple or complex. This Section of the *Commentary* sets out a multi-faceted and layered approach to information security.

Not everything set out in this Section can or should be adopted by everyone. Providers should consider cost, business needs, and strategy, but ultimately the reasonableness of the solution is derived from the results of the LSP's risk assessment described in Section III.

This Section identifies a variety of policies and practices that might be used to meet the needs of LSPs and clients. In particular, it addresses the means by which members of the legal services industry may:

- consider the sources of the sensitive information they maintain and the nature of that information;
- identify those within the organization with a bona fide need for access to information and limit access to those people;
- address information security policies in three subparts: (1) information security in the office and on the network, (2) information security for information that travels outside the office or the network, and (3) information security for information that is shared with experts, consultants, other service providers, and adversaries (either in negotiations or discovery exchanges);
- plan for the disposition of information after it is no longer needed;
- institute a training program that reaches everyone and incentivizes their compliance; and
- anticipate potential breaches by developing plans for prevention, improving detection and response to incidents, preparing to notify affected parties if the information is jeopardized, and adopting contingencies for promptly resolving any problems.

<table>
<tr><th colspan="2">Illustrative Narrative</th></tr>
<tr><td colspan="2">Throughout this section are grey boxes, which contain two sides of a running fictional narrative. It is a depiction of a series of standard cyberattacks, and the simple mitigations that can defeat them. Its intent is to show that while many common attacks are not complicated, a small firm can maintain a reasonable (read, proportional) level of security without undue hardship.

The infrastructure system used in this example is Office 365, but the techniques described (both those used by the attacker, and the defensive measures used by Alex and the firm) can be implemented across many different systems.</td></tr>
<tr><th colspan="2">Introduction to the two players</th></tr>
<tr><td>Alex is a partner at Lawyer, Barrister & Solicitor LLP (LBS LLP), a three-partner law firm which handles the personal legal affairs of several high-profile celebrities.

One Friday, Alex received a phone call from a longtime friend and client, Bryce Bayne, a high-profile, high-net-worth actor who had recently been in the news following a messy breakup: Bryce's partner was alleging misconduct and threatened to take Bryce to court.

Bryce believes that there are messages on his cellphone that prove he was in the right but is concerned that disclosing any of the contents of his phone could be damaging: as an intensely private person, Bryce is sensitive about giving up the phone, even if it will prove his case.</td><td>Haxor3k is the anonymous online username of a malicious hacker that prefers the shadows. It operates internationally, using technical know-how and an ability to manipulate people over the phone and over the internet to extort money or favours from those who fall victim to its schemes.

Haxor3k noticed the recent news of Bryce Bayne's messy breakup and decided this was an opportunity to extort the celebrity, get some additional leverage for future extortions on other targets, and toy with someone from the shadows.</td></tr>
</table>

A. Step 1: Identify the Types and Sources of Information That Must Be Protected

To launch any privacy and information security program, an LSP should first evaluate the type of information it has and collects as well as how it uses that information (discussed in Section III).

Illustration #1: Determining and Gathering Personally Identifiable Information	
Alex speaks to his friend Bryce, cognizant of the intensely personal relationship between a person and one's cellphone in the modern era. As a portal to the web, a cellphone contains photos, messages, idle musings, and internet search history, which most would rather keep to themselves. Alex argues, however, that these messages should be used to defend Bryce from the unfounded accusations being leveled at him in public and private. For Alex's client, this Personally Identifiable Information is anything that could be tied back to Bryce, be it cellphone call logs (to connect Bryce to a phone number, and those of his closest friends), or a photograph of Bryce at his cottage. Bryce's cottage is remote and thus far undiscovered by paparazzi, and Bryce would prefer to keep it that way. If that cottage photograph were to get out, the background signage, layout of the bay, and architecture of the building could be used to connect the address back to Bryce, destroying his personal privacy.	Haxor3k has decided on a target, so now it shifts to reconnaissance. The job now is to gather as much Personally Identifying Information about Bryce as it can, connect it together, and determine the best way to move on with its attack. Looking at the last three years of press releases, Haxor3k determines that Lawyer, Barrister & Solicitor LLP often represents Bryce in legal dealings: contract negotiations and publicity agreements. Alex Lawyer was mentioned in a recent news article related to Bryce's messy breakup as a close friend close who lent Bryce support as he retreated from the public eye. Alex looks like a good target: access to intensely personal information, likely communications in writing or over the phone, maybe even in possession of a computer or phone with some juicy extortable material on it. Alex also has a small team so isn't likely to have sophisticated defences in play, and more people means more potential targets. Perfect. Shifting focus to Alex Lawyer and LBS LLP, Haxor3k goes to LBSLLP.ca and copies all of the contact information it can find: names, addresses, personal bios of all lawyers and staff on the team. Any cited cases on the website are fair game: it compiles a list of past clients, particularly those that have been a party to multiple newsworthy cases on the LBSLLP.ca website, because these are likely repeat customers. Haxor3k wants to impersonate one of these important customers to gain a level of trust, so it goes to the websites of the discovered clients, pulling the information of likely C-suite accountants or ranking members of the legal department who may be in regular contact with LBS LLP's team. It also runs some online queries and determines that Office 365 is the main back-office communication and storage system used by LBS LLP, and by downloading some PDFs from its website, Haxor3k can guess at the type of PDF editor used on LBS LLP systems.

B. Step 2: Determine Those Who Need Access

The LSP should determine who among its members and employees needs to have access to what information and under what circumstances should they have it—keeping in mind that all security breaches and leaks come from one of three possible sources: (1) employees (whether intentionally or inadvertently);[87] (2) lost or stolen media; and (3) intrusions from the outside. The governing information management principle should be "need to know." Only those employees with a specific business purpose requiring access to a particular type of information should have access. Policies should be drafted with this guiding principle in mind.

C. Step 3: Develop Specifically Tailored Information Security Policies and Practices

This section addresses information security policies and practices in three distinctly different contexts: security in the office and on the network; security for information outside the office or network; and security for information when it is provided to others. In each of these three situations, a fully adequate information security and privacy program can be scaled to meet the specific needs of the LSP and its clients.

1. Security in the Office and on Firm-Controlled Systems

a. Require User Authentication and Permissions

LSPs can protect PCI that is stored on networks or devices by requiring those who seek access to the information to show they have authorization to access it. This means that access to information stored on a network, a computer, or a mobile device should require user authentication through biometric means or passwords or, in the case of multifactor authentication, a password combined with a token or security question. Similarly, where the provider determines (see Step 2 above) that employee and partner access to certain information should be restricted, then users' access should be limited through permissions for designated levels of sensitive information. For example, an LSP might implement role-based access controls, by which its employees' access to information is determined by the type of information and the employee's role in the organization. Such a system might grant varying rights depending on whether a person is a partner, associate, law clerk, administrative assistant, and so forth.[88]

---

[87] One article identifies four types of employees who pose risks: the "security softie," who does things he or she should not do; the "gadget geek," who adds devices or software to the system that do not belong there; the "squatter," who uses IT resources inappropriately; and the "saboteur," who hacks into areas where he or she does not belong. The article further notes that "insider threats come from many sources: maliciousness, disgruntled employees, rogue technology, lost devices, untrained staff and simple carelessness." See Mark Hansen, *4 types of employees who put your cybersecurity at risk, and 10 things you can do to stop them* (28 March 2014), online: ABA Journal <http://www.abajournal.com/news/article/war_stories_of_insider_threats_posed_by_unapproved_data_services_and_device>.

[88] For an overview of the subject, see Computer Security Resource Center, *Attribute Based Access Control – Project Overview* (28 March 2018), online: National Institute of Standards and Technology < http://csrc.nist.gov/projects/abac>. For a more detailed review of the topic, see David F. Ferraiolo & D. Richard Kuhn, *Role-Based Access Controls,*

b. Require Sufficient Password Complexity

Illustration #2: Phishing for Passwords	
Alex started using a Password Manager two years ago, and while the transition took some time, it now saves a lot of time and headache. Alex used to use a password based on the name of his hometown, but eventually it got too hard to remember how many exclamation points were stuck to the end for his bank password, or the number of threes Alex added for the movie theater password. Better yet, with the Password Manager, each password is completely different: there's no guessable pattern to them at all.	Haxor3k knows all of the business email addresses for members of the firm, so it reaches out to contacts on the firm's website, searching for any known passwords associated with these accounts and any account credentials that were exposed during the last decade of data breaches. Finding two accounts and passwords for Alex Lawyer, it tries to log in with these credentials, with no success. It looks as if the old passwords are both based on the name of Alex's hometown, which Haxor3k found on Alex's LinkedIn profile, through Alex's high school. Haxor3k assigns one of its computers to attempt a few thousand variations on this name over the next two days. But still no luck. Since guessing passwords is hard, maybe Alex will simply give them up. Armed with its previous research, Haxor3k decides to go spear phishing.

No matter how the LSP grants or limits access to particular types of information, access to network areas and devices containing confidential information should be protected by "strong" passwords at least. The strength of a password is related to its length and its randomness properties.[89] Strong passwords should be of sufficient length and complexity that they cannot be guessed (e.g., they should contain a combination of capital and lowercase letters, numbers, and special characters).

15th National Computer Security Conference (1992), pp. 554–563, online: <https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1992/10/13/role-based-access-controls/documents/ferraiolo-kuhn-92.pdf>. An alternative, more complicated, system for limited access controls is the attribute-based access control. For an overview of this method, see *Attribute Based Access Control – Project Overview*.

89 See Meltem Sönmez Turan et. al., NIST Special Publication 800–132, *Recommendation for Password-Based Key Derivation, Part 1: Storage Applications, Appendix A.1* (2010 December), online: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf>.

Illustration #3: Alex accidentally reveals a password	
Alex receives a sharing link from his biggest client, Dr. Seo of Seo Inc., who asks for a review of a draft contract that needs to be signed by the end of the day. Alex notes that this is an unusual request, but Seo Inc. is important enough to the firm that it always gets what it asks for. Alex replies to Dr. Seo, then clicks the link and is prompted to log in to an Office 365 account so he can review the document. Alex opens the Password Manager, which usually automatically fills in these passwords, and pastes in the password.	Haxor3k knows from its PII research that Seo Inc. is a major client of LBS LLP. It also knows that Seo Inc. uses SharePoint. It sets up a fake website (www.office.com.login.downloadshared.fake) that impersonates Microsoft's login page, stealing the credentials of any account that tries to log in. Hakor3k sets up a free Gmail account, using the name Dr. Falsi Seo, the CEO of Seo Inc., and sends an email to Alex Lawyer, inviting Alex to log in and download a draft contract. Haxor3k smiles as Alex enters the password. "We're in."

c. Impose Conditional Access Rules

Although at times inconvenient for the user, a network ideally would lock out a user who has not revised a password within a prescribed interval, or who has failed to enter a correct password after several incorrect attempts. Other conditional access rules—for example, preventing new logins from non-North-American locations—can further protect systems.

Illustration #4: Haxor3k tries to login as Alex
Haxor3k opens a web browser and enters Alex's email address and the password just phished using the fake Dr. Falsi Seo email account and fake login page. Haxor3k is immediately blocked: it used the right password, but at the moment, it seems that LBS LLP users are not allowed to log in from outside of North America. Irritated, Haxor3k sets up a virtual environment in a data center in Virginia and tries to log in again from there.

d. Use Two-Step Authentication

A Two-Step Authentication system (e.g., a notification appearing on a user's token or cellphone, requesting validation before a new device is allowed access to network resources) should, when available, be used to ensure that even in the case of a lost password, a user is notified of login attempts he or she did not initiate. Combined with a Mobile Device Management solution (discussed in Section 2(a) below), these authentication systems allow the LSP to control the flow of information at the borders of its network and beyond.

Illustration #5: Alex receives an unusual alert	
Alex receives a prompt on his phone: there was a request to log in to Alex's account from a computer in Virginia, down in the United States. That's unexpected; Alex hasn't used a new computer, and the last time the login screen appeared there wasn't a Two-Factor prompt. Alex isn't anywhere near Virginia. Denying the login request, Alex now knows about the attack but isn't too worried—he is already changing the main account password, and the unknown login was already blocked. Alex is relieved that what could have been a serious breach in client trust was immediately averted.	Haxor3k tries to log in from the Virginia computer system, using Alex's username and password. Blocked again! This time it wants Alex to open his phone and authorize the new login. Haxor3k worries for the success of the attack, since Alex might now be aware that something phishy is going on. It's time to get more aggressive and exploit any opportunities available to turn this fiasco into a money-making venture. Haxor3k has invested time and effort into the reconnaissance phase, so even if this targeted attack (spear phishing) failed, it's not yet time to give up.

e. Protect Against Malware and Active Threats

Policies should consider which of the LSP's systems are regularly exposed to unknown files and applications, either through user action (downloading a new tool from a sharing website) or incoming communications (spam email). Policies should direct that antivirus software be deployed to mitigate the risk of infection and configured to automatically update and actively monitor systems to ensure that emerging threats are blocked.

Illustration #6: Alex blocks a virus	
Alex appears to be logged into the sharing site and downloads the PDF sent by Dr. Seo, but the firm's antivirus protection immediately quarantines the file: it scanned and detected a malicious file that would have taken over Alex's system. Alex is glad that the firm's antivirus is constantly updating definitions and actively monitoring activity on the network but is worried that Seo Inc. is infected or fell victim to a phishing attack.	Before it launched its phishing attack, Haxor3k set up a website to download a PDF with content that looked like a draft agreement but also contained a nasty surprise: since Haxor3k's research indicated that LBS LLP used an outdated PDF reader with known security issues, it created a malicious file that could break the program and infect the computer system. If the file succeeds, Haxor3k's virus will connect back to Haxor3k's systems asking for further instructions, and Haxor3k will be into the firm's infrastructure.

f. Require Mandatory Reporting

The LSP should consider a requirement for staff to report any suspicious activity noticed on its computer systems, involving either internal or external communications, or any observed attempts to compromise its credentials.

Illustration #7: Alex notices the attack	
Reviewing the incoming email, Alex is unsure whether the virus originated with the legitimate Dr. Seo but realizes that the Gmail address is not the one Dr. Seo usually uses and isn't associated with Seo Inc. Alex forwards the email to the firm's IT support team, which was selected because of its demonstrable experience and certifications with information security. Alex is worried that the account password may have been compromised, so Alex also alerts the office manager and then changes the password. Alex acknowledges that there will be some hassle, but thanks to Two-Step Authentication, all of Alex's existing devices already enrolled with device-specific credentials will not need to be changed, since they were not compromised, and the devices are trusted.	Haxor3k knows that the attack will be more successful if it flies under the radar. By creating a PDF with some somewhat sensible content, it hopes to delay any kind of alarm while Alex reads over the document.

g. Ensure Physical Security of the Office

Policies should provide for physical security of the LSP's office, including when doors should be locked and who has access to main entrances, offices, conference rooms, storage rooms, and other office locations. For example, a policy might specify that office locations that contain confidential information, whether desk drawers, file cabinets, or file rooms, be locked when not in use, and access should be limited to people who need access. A slightly more elaborate plan may require that all access to areas containing confidential information should be tracked, perhaps through sign-in sheets or, more elaborately, through electronic verification such as keycards. An even greater level of security might require that servers or records storage areas should have especially limited employee access, perhaps deploying security cameras inside and outside these areas, or an intrusion alert system. Biometric checkpoints may be warranted in some special circumstances.

h. Restrict the Use of External Media

While there might be valid reasons to use external media such as flash drives, transferring information to portable media can compromise security. The media could introduce viruses or malware to the network. Information copied onto peripheral media can create an additional risk point because the media can easily be transported, lost, or stolen.

Thus, policies should restrict the use of unencrypted external media. LSPs should consider policies that specify when any external media may be used, who may use it, to what devices it may be connected, and how it is to be stored, erased, reused, transferred, and designated for disposal. Such policies can take several forms, from written directives to technical measures that preclude transferring or copying information. LSPs should encrypt portable media to restrict unintended access. As discussed in Section 2(a) below, Mobile Device Management is one method for enforcing these LSP policies.

Illustration #8: "Was this our lost USB?"	
The next day, Alex comes into the office and is greeted by one of the clerks, who was hit by ransomware the previous day. The clerk found an LBS LLP USB stick in front of the building last lunch hour and couldn't get it to work on the office machines, but when plugged into a computer at home, the computer started issuing threats and demanding payment to decrypt personal files. Alex reminds the clerk about the firm's acceptable-use policy and hardware-use policy, which, in a nutshell, states that firm data should stay on firm devices—if the USB was thought to be a firm device, it shouldn't be connected to a personal computer. Further, Alex reminds the clerk that USB storage devices have been disabled on office computers—data should enter the firm either through email or the file sharing service.	Haxor3k decides that the office is the best attack vector, since all other avenues in have failed. It prepares 50 8GB USB sticks with a piece of malware, which will attempt to install itself on any computer that they are connected to, then connect back to one of Haxor3k's command and control servers for further instructions. Haxor3k orders USB sticks with LBS LLP's logo printed on the side to increase the likelihood that they would be connected to a work machine, then drops them on the ground outside of the LBS LLP office and throughout the parking lot. Haxor3k gets five successful connections, all simply consumer computers and none associated with an LBS LLP work station. Dejected, it makes the most of it by installing a standard ransomware package in an attempt to extort payment.

i. Protect Network Security

Once an LSP has a single computer connected to a server, WiFi router, or other network-enabled device, it has established a network. At a minimum, that network should then be protected against fail-

ure, and if it is connected at all to the outside world, it should be protected against intrusion. Network security requires developing secure infrastructure either in accordance with a client's specific security needs or according to a standard industry benchmark.[90] While the level of security is certainly scalable to fit the circumstances, once a provider moves beyond the most basic level, it will likely need to determine who will monitor the LSP's network for security breaches, how that monitoring will be accomplished, and how the monitors will be monitored. Policies should describe procedures for regularly monitoring and analyzing network logs and events, and for identifying and addressing potential security breaches.

LSPs that offer WiFi access in their office should ensure that the network is protected through over-the-air authentication and encryption, and their policies should provide protocols for managing and monitoring the WiFi network. Logging features should be enabled so that there is a record of everything that is copied, in the event that data is wrongfully accessed. Wireless networks should be encrypted, and LSPs should not overlook the security of their wireless network (current WiFi Protected Access II (WPA2) provides the highest level of router protection). This includes a program for regular network device patching to mitigate newly discovered threats. Guest WiFi should be provided through a separate network, with no ability to access the rest of the network.

Illustration #9: The virus doesn't spread to office computers

The Clerk who found the USB brought a personal computer into the office to ask the firm's IT staff about the computer.

Alex is alarmed that the infected device was brought to the office, since if the computer had been connected to the standard office network the ransomware could have spread to other systems at the office. However, the firm has an isolated guest network separate from the rest of its resources, so the virus is contained.

---

[90] Industry certifications can represent a useful benchmark, but LSPs should generally not consider certification, or lack of it, to define the level of security. In addition, providers relying on these or other industry standards to determine third-party security should inquire as to exactly which parts of the third party's business are certified and which are not certified.

International Standards Organization ("ISO") is the largest developer of standards in the world. Its membership is drawn from the National Standards Bodies of multiple countries. The International Electrotechnical Commission oversees the development of electrical and electronic Standards for participating countries. The 27000 series has been reserved specifically for information security matters. ISO 27001 is a standard describing the best practices for an Information Security Management System, often referred to as "ISMS." An ISMS is "part of the overall management system, based on a business risk approach, to establish, implement, monitor, review, maintain and improve information security. The management system includes organizational structure, policies, planning activities, responsibilities, practices, processes and resources." ISO/IEC 27000: 2012.

SSAE-16 (Statement on Standards for Attestation Engagements No. 16) is also a commonly used security standard for data centers, as set forth by the Auditing Standards Board of the American Institute of Certified Public Accountants.

j. Provide for Secure Backup and Disaster Recovery

Information security policies should provide for secure backup of provider information and include disaster/recovery plans, including procedures for restoration. LSPs should consider off-site storage of encrypted backup media, and if they back up client information separately from their own information, these backup processes should also have disaster/recovery plans. Such plans would ideally include specific procedures for backup and restoration that are understood, agreed upon, and maintained in compliance with a written agreement among the clients, providers, and third parties (as appropriate). Conducting regular test restores is highly recommended.

Illustration #10: Backup

Unfortunately, the clerk didn't have a proper backup for her home computer and is wondering what to do. Alex can't offer any suggestions except that sometimes ransomware is cracked and the decryption keys are released for free.

Alex decides to check the firm's backups, ensuring that they are working properly and saved to a separate storage device, which is protected from the rest of the devices on the office: no users can edit or delete them except for the allowed backup user.

k. Limit Remote Access to Firm Network

Many LSPs permit employees to access their network from locations outside the office. This access may be through encrypted connections such as a Virtual Private Network ("VPN") or remote access programs in order to maintain privacy and security. Remote access with authentication via Two-Step Authentication and deployment of access controls through role-based access control or attribute-based access control should ensure that those with permission to access certain information are the only people who can access it.[91]

l. Avoid Use of Third-Party Computers or Networks

LSPs should train employees to avoid publicly available computer systems, such as computers at hotels, when accessing the LSP's network. Once the firm's computer system is accessed from an untrusted computer system controlled by an outside party, any restrictions on further use and dissemination become problematic, and accountability for the information is compromised. Even if the employee is trustworthy and loyal, the LSP should consider whether the employee should be allowed to use the devices of friends and family members to access the provider network or use public networks in locations such as cafes or airports. LSPs should set guidelines regarding the circumstances, if any, when an employee may use public WiFi to transmit client information. Unencrypted client information sent through public WiFi, including paid or free hotspots, can be easily compromised.

[91] See Turan, *supra* note 89 and accompanying text.

Therefore, LSPs should clearly specify when use of public WiFi is and is not permitted and what additional protections are required.[92]

m. Provide for Adequate Monitoring and Audits

Oversight is appropriate to ensure that policies are executed correctly to identify remaining areas of risk and to quickly identify breaches. Policies should address who is responsible for audits and how and when audits will be conducted and reported. Monitoring should include all areas of the LSP's business and all processes involving confidential information, although they need not all take place at the same time. Checklists can serve as a useful guide to ensure thoroughness of past and future audits.

In addition, real-time tracking and accounting of client information is necessary to identify breaches quickly and help mitigate problems caused by data loss. Immediate notification of appropriate LSP partners and affected clients, as well as any third parties, such as law enforcement authorities or insurers involved in the transport or loss of information, is essential.

LSPs should also require periodic data inventories, e.g., determining what information the LSP has and where it resides. Regular checks on data logs and data inventories provide quality assurance of information security.

n. Track the Receipt and Creation of Confidential Information

Although sometimes difficult to achieve in practice, LSPs should consider implementing detailed procedures to track client information from receipt until destruction. Such procedures might establish a central point for receiving and tracking client or case-related information and implement a process for logging information received from the client, no matter whether it arrives on an electronic device or external media, through an online transmission (email, FTP site, web file sharing service, etc.), or in hard copy. Logging the date, sender, recipient, and contents of received information facilitates managing the information. Attaching a label with a unique ID to each piece of any media, device, or hard-copy file received may also help manage them throughout the representation. Logging confidential information allows LSPs to begin a chain of custody that reflects access, copying, transfer, and deletion of the files.

LSPs should also consider whether there is a need to distinguish between client-created information that is sent to them and work product that is generated by the LSP. Although LSPs should treat both types of information as confidential, the LSP may find it easier to create distinct life cycles for provider-created information and client-created information for the purpose of chain of custody and work management, as well as disposition at the end of a matter.

---

[92] Options for additional protections may include use of virtual private networks (VPNs), which route data through a private connection. When possible, encrypted connections are also preferred through use of secure "https" addresses instead of "http" for websites and use of a Secure Sockets Layer (SSL) security protocol for applications.

The flow of information into the LSP may also pose a threat: the LSP should consider inserting banners onto messages received from outside of the firm or known to be from other trusted senders, to prevent impersonation or fraud.

Illustration #11: Alex is impersonated over email	
The next day, Alex decides to work from a favourite café, down the street from the LBS LLP office. When Alex drops by the office before heading out, Gray Monie, the firm's administrator, stops Alex for a moment and asks about an unusual email that just came in, purportedly from someone at the firm. Gray noticed the unusual nature of the request: LBS LLP has a standard process for moving trust account balances and doesn't move large sums of money without proper authorization from a partner. Gray also notes that the firm's email system had added a red banner to the bottom of the incoming email: "Be careful with this message, it was sent from an external source."	Haxor3k decides to go after the law firm's bank accounts: perhaps it can trick the firm's administrator to wire some funds from the firm's trust account. Creating another fraudulent email, this time impersonating Alex Lawyer, Haxor3k crafts an email to Gray Monie, LBS LLP's office manager. The email uses LBS LLP's standard email signature (which was copied from Alex's reply to the earlier spear-phishing attempt) and a name of a prominent LBS LLP client with simple instructions: "Real Estate Agent LLC has moved one of their files to another firm: transfer the remainder of their trust account to bank routing number 012345678, account 0123456." Haxor3k is again disappointed: it never receives a response from the office administrator.

2. Security Outside the Office and Network

Whenever information moves, it is vulnerable to being diverted, damaged, lost, stolen, or altered. This is true whether a move entails a ride in a cab to the courthouse or a trip around the globe for a meeting. Information security programs should address the movement of information and the potential risks. Where information is subject to special requirements, the LSP should set forth a mechanism for alerting the relevant personnel to those requirements.

Illustration #12: A stolen laptop	
Alex arrives at a favourite coffee shop, setting a bag and phone down at a table to secure a prime spot. Returning from the counter, Alex is alarmed when both are missing. Alex knows that the phone has a password and fingerprint reader, so at least it is secure. The laptop, too. It was automatically encrypted right after it was purchased: as soon as Alex logged into the system with LBS LLP account credentials, LBS's Mobile Device Management policy configured device encryption and auto-lock requirements. Alex checks at the counter, but no one in the busy shop saw who took the bag. Alex returns to the office and asks that the lost phone and laptop be remotely wiped. The phone can't be located, but the wipe command is issued: the next time the phone comes online, the contents of the device will be securely erased.	Haxor3k is now emotionally invested in the attack. Haxor3k flies to Alex's city to physically monitor the front of LBS LLP's office and observes as Alex arrives and then immediately departs the office, heading for a coffee shop. Reviewing Alex's public social media accounts, Haxor3k identifies three Instagram photos tagged with the name of a coffee shop near LBS LLP's office, the same shop Alex just entered and set down a bag at an empty table. Haxor3k wanders into the coffee shop and brushes past the unoccupied table, surreptitiously picking up the bag and cellphone. It walks back to its car, opens the laptop and tries the password phished from Alex the previous day. No luck. The laptop remains locked. Turning to the cellphone, it is again frustrated by a password on the phone. Haxor3k turns off the laptop and extracts its storage drive, connecting it to another computer. Unfortunately, the device is encrypted and thus unreadable. Attempting to evade capture, Haxor3k turns on Airplane mode on the cellphone before its location is traced.

a. Provide for Remote Management of Mobile Devices

Mobile devices, such as laptops, phones, tablets, and PDAs (personal digital assistants) are a practical necessity for LSPs. However, their portability and access to information also make them a target for information theft, even when they are "safely" located within an office environment. The primary tools for protecting the devices from theft and intrusion consist of strong passwords, encryption, auto-locking defaults, device-tracing applications, and applications that allow the devices to be wiped remotely.

Through Mobile Device Management, the LSP can also remotely monitor and update devices (phones, tablets, and laptops). Mobile Device Management technologies can assist with the upkeep of asset inventories and the application of LSP-wide security policies. These systems maintain a list of trusted devices, associated with their primary user, and can enforce strong passwords, encryption,

and other information transmission limits. It can thus install remote applications, configure settings, ensure security by updating and running malware detection software at predetermined times (or on demand), enable device firewalls, disable public file sharing, avoid automatic connections to public WiFi, and even track and wipe lost or stolen devices. They can also facilitate a secure Bring Your Own Device ("BYOD") program by separating LSP and client data from the user's personal information.

Centrally managing trusted devices facilitates other advanced security initiatives, such as transparent external storage device encryption (all firm machines may be permitted read or write access to USB media encrypted by the firm, but not to unencrypted external media) or document-level digital rights management, which transparently decrypts a document's contents only when an authorized user on an authorized device attempts to open the file and logs that access to a central monitoring service. These technologies dramatically improve the security of information and the accountability of those with access to it, but they can impede access—they should be deployed only if the results will align with the LSP's security needs or those of its clients, and perhaps only for a subset of files.

Policies should instruct employees to notify the LSP immediately if a mobile device is lost or stolen so the LSP can wipe or disable the device, as appropriate.

Consider the LSP's Hardware Acceptable-Use policies: what is a user's expectation of privacy on a BYOD system, and is a user obligated to permit capture and discovery of the device?

Illustration #13: Remote access, denied and destroyed	
Alex is having a bad 24 hours, so he heads to a local bar with some friends after work.	Haxor3k continues to monitor Alex's movements: after returning, dejected, to the office and completing the rest of the work day, Alex heads to a local bar to relax. Haxor3k follows Alex in, impersonates a server and takes away Alex's empty glass, hoping to extract a fingerprint. Using the fingerprint from the glass, it gains access to Alex's phone: unfortunately, it is still in Airplane mode, and there is little actionable content on the phone itself, independent of the firm's network resources. Disabling Airplane mode in an attempt to connect to the firm's files, the phone immediately wipes itself. Another attack, foiled.

b. Encrypt Transferred Data

LSP policies should generally require encryption when private or confidential information is transferred. Unless email is encrypted, LSPs may wish to consider alternative ways to transfer particularly sensitive PCI. Encryption is more than a useful and convenient information security tool. It is critical for protecting client information, especially when the information is stored on mobile devices, transmitted, or stored remotely. Typically, encryption applies an algorithm to convert data to an unreadable code unless it is decrypted using a password. Provided only the sender and recipient of data know a password, the data will be protected against third parties even if the data is lost or intercepted. Encryption keys should be stored separately from the encrypted devices or media to ensure security.

Many operating systems and their supporting hardware can be configured to use encryption for all files or for files selected by the user.[93] Several different products are available to provide various levels of encryption capabilities. LSPs need to be knowledgeable enough about the different encryption capabilities available to select the appropriate options for their needs. Third-party software for encryption is also readily available. Email applications can be set up to encrypt and automatically decrypt emails. Users simply need to exchange public keys and have their private key applied to decrypt messages; however, this key exchange process is burdensome within most standardized email environments and may lead to inconsistent application. There are third-party services that provide additional capabilities that make key exchange transparent and much easier to use. Mobile devices have encryption options—which can be managed through the device settings—that protect information when the device is locked.

Once information has been encrypted, it may then be securely transmitted through Secure File Transfer Protocol (SFTP), email, or cloud document management services. If information must be transmitted physically, the delivery method should reflect the sensitivity of the information. Highly sensitive information may need to be carried by a private courier or an LSP employee. The method of transport should be considered in avoiding unintended access due to the media being confiscated, lost, or stolen. If information is mailed, it should be sent in a manner so that it can be tracked at all times. Unencrypted sensitive information should never be placed in the mail or turned over to a courier for delivery. All too frequently, packages are lost, opened, or stolen in transit.

c. Educate Regarding External Use Security Considerations

When working outside controlled environments, employees should be instructed to use screen guards to prevent laptop screens from being viewed by the public, and to avoid discussing sensitive

---

[93] Encrypting files is a critical practice in many circumstances. LSPs should be mindful, however, that in some circumstances encryption may mask the introduction of malware into the network or obscure the theft of information. See Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Crown Publish Group 2014), ch 14; see also Karen Scarfone et. al., *Special Publication 800–111*, *Guide to Storage Encryption Technologies for End User Devices* (2007 November), online: National Institute of Standards and Technology, Computer Security Research Center <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf>.

information in public. Employees also should be made aware of the vulnerabilities of bluetooth technology and the potential for eavesdropping.

d. Implement BYOD and Personal Device Policies and Practices

Losing a client's business information, trade secrets, or privileged information can get an LSP in trouble with its client and perhaps with the law society as well. Losing sensitive client information that is subject to special regulatory restrictions, such as health related information, may generate regulatory involvement. Personal devices present one of the most significant risks to client information. These devices include home computers as well as mobile devices such as laptops, smartphones, and tablets. The best defence against the loss or theft of trade secrets, business information, privileged materials, and other sensitive information may be a strong and strictly enforced policy banning the use of personal devices to transact business or store such information. If an LSP permits its employees to use their personal devices to access private or confidential information, the LSP should consider taking the following steps to lessen the risk of using such devices:

- Allowing the use of *only* those devices that are specifically approved by the LSP's security professionals.

- Requiring strong password and encryption policies.

- Limiting the employee's ability to create or store LSP or client information directly on the device, by providing access only through secured portals to provider-protected networks. LSPs may also consider "sandboxing" mobile device applications that contain confidential information to shield provider applications from access by other applications or malware on the device.[94]

- Designating types of client information that should not be accessed, transmitted, or stored on a personal device. This may include information that is subject to specific statutory protections, information that is otherwise highly sensitive, and information that clients have requested not be accessed by BYOD devices.

- Addressing employee home WiFi networks and devices used to create personal hotspots by requiring that these networks be secured with strong passwords that are not shared and are changed regularly.

e. Limit Carriage of PCI when Traveling Abroad

LSP personnel should avoid traveling across borders with client information or devices capable of accessing the LSP's IT systems, unless appropriate precautions and safeguards have been taken to

[94] Sandboxing effectively allows a device to host applications or data from multiple sources while blocking the flow of information or data from one part of the device to another.

account for increased security risks. Because this is a specialized area, LSPs might consider consulting or hiring third parties with expertise in network security involving traveling and transporting data outside the country.

LSPs should specifically address travel to high-risk geographic regions. It may not be possible or advisable for employees to directly access firm systems from high-risk areas. It also may not be advisable to allow employees to carry their normal devices or media with them into high-risk areas, lest they be used to infiltrate the provider's systems. LSPs may also consider requiring employees to travel only with devices that do not contain sensitive information and adjusting default device settings on those devices. In addition, LSPs should consider whether WiFi connections are especially risky and adopt a policy of wiping devices both before traveling through foreign customs and before reconnecting them to the provider's network when they return home.

3. Security Among Third-Party Service Providers

The best information security program in the world can be nullified if the information is vested in the hands of another service provider who does not have adequate safeguards in place. For that reason alone, LSPs have a strong incentive to make sure the information they share with their experts, consultants, litigation support specialists, and other providers is well protected.

LSPs, like their clients and other businesses, increasingly rely on Third-Party Service Providers or TPSPs to process, store, and manage information and IT systems. These TPSPs can include cloud storage providers, online human resource management companies, paper storage and destruction companies, eDiscovery service providers, enterprise-class online productivity services, Software as a Service (SAAS) cloud providers, and providers of outsourced IT staffing and services. Regardless of the TPSP or type of service offered, LSPs should consider following a set of best practices when engaging the services of such a TPSP on its own or on behalf of a client. Key privacy and information security requirements should always be reflected in the contract between the LSP and the TPSP.

a. Understand the Type of Information the TPSP Will Handle

Before entering into an agreement with a TPSP, LSPs should carefully consider the type(s) of information that the TPSP will handle. For example, the following questions should be asked about the information to be accessed, processed, or stored by a TPSP:

- Will the TPSP handle client information, or only information belonging to the LSP itself, such as its own human resources information?
- Will the TPSP handle PII, sensitive financial information, trade secrets, or privileged communications and materials?
- Are there any legal or regulatory restrictions imposed on the handling of the information?
- Are there any contractual obligations related to the information?

b. Ensure Compliance with Applicable Legal and Regulatory Requirements

LSPs should understand the legal and regulatory requirements applicable to the type of information that will be accessed, processed, or stored by the TPSP, and ensure that the TPSP is not only capable of meeting these requirements, but also is contractually obligated to do so.

c. Understand Geographic and Technical Risks Associated with the TPSP

LSPs should understand where their information will be stored and whether their information will be commingled with information belonging to other customers of the TPSP. TPSPs may store information in a variety of geographic locations, including overseas. The physical location of its information can subject LSPs to litigation and regulatory oversight in the jurisdiction where information is stored. LSPs must therefore understand and approve where its information will be stored. TPSPs may also commingle the information of their other customers. This is generally not a recommended arrangement for LSPs, because their information will be too sensitive to make the risks attendant with commingling acceptable. Thus, LSPs should avoid any arrangement in which information transferred to a TPSP will be commingled.

d. Conduct Due Diligence

A TPSP's viability is critical, and LSPs should therefore obtain information about the TPSP's potential conflicts and its financial stability. LSPs should also know the scope and policy limits of the TPSP's insurance coverage and ensure that the TPSP performs background checks on its employees and requires employees to sign confidentiality agreements.

e. Review and Approve the TPSP's Own Information Privacy and Security Policies Prior to Executing a Contract

No TPSP should be retained unless it has an appropriate information security and privacy policy. The TPSP's level of security and privacy protections should generally match or exceed those of the LSP. As a general matter, TPSPs should be retained only if they agree to meet an established standard, such as ISO 27001 and 27002. At a minimum, the LSP retaining a TPSP should consider contractually mandating each of the following:

i. Physical Security Controls

TPSPs must ensure the physical security of facilities housing sensitive information or from which such information can be accessed, including offices, off-site facilities, and locations of servers. Access to these facilities should be logged. These same recommendations apply to TPSPs that access, process, or store information belonging to the LSP or its clients.

ii. Information Access Controls

TPSPs need to have appropriate preventative controls on accessing information, including, but not limited to, multifactor authentication utilizing complex passwords, compartmentalization of information on the TPSP's systems, and access restricted to "need to know" individuals.

iii. Intrusion Detection Systems

If the information provided to the TPSP is highly sensitive and contains significant private or confidential information, LSPs should consider requiring the TPSP to employ an intrusion detection and monitoring system.

iv. Encryption Procedures

Information sent to a TPSP should be encrypted while in transit to and from the TPSP. LSPs should also consider whether the sensitivity of the information warrants a requirement to encrypt information while it is stored ("at rest") by the TPSP.

v. Secure Disposition of Information

If the TPSP will store information for the LSP, it should agree that it will only use secure methods for disposing of that information or any hardware or media on which that information was stored.

f. Review and Approve the TPSP's Employee Training Program for Information Privacy and Security Prior to Executing a Contract

For both LSPs and TPSPs, proper employee and contractor training programs are essential to maintain information security and privacy. Before entering into an agreement with a TPSP, the LSP should inquire about the TPSP's employee and contractor training programs related to information security and privacy to ensure they are adequate. If the TPSP's training program is inadequate, the LSP should consider mandating the necessary improvements in its contract with the TPSP or finding another TPSP.

g. Ensure Appropriate Safeguards for Intellectual Property

Contracts with TPSPs should protect the intellectual property rights of the LSP and those of its clients. Use of a TPSP should not alter or adversely affect intellectual property rights.

h. Require Records Management Compliance

If a TPSP will store any information belonging to the LSP or its clients, the LSP should consider requiring the TPSP to adhere to the relevant existing records management and retention policies.

i. Mandate Appropriate Information Disposition Upon Termination of the Relationship

The TPSP contract should require the TPSP to adhere to the records policies of the client and to securely dispose of, or return, all the LSP's information in a useable form, in a timely manner, and upon termination of the relationship. Contractual clauses in which nonpayment on the part of the LSP or its client justify refusal or delay in returning or providing access to information are generally not acceptable.

j. Consider Bankruptcy Protection

Careful consideration should be given to what will happen if the TPSP becomes insolvent or enters into bankruptcy. This scenario can be specifically addressed in the contract to ensure there is no dispute regarding ownership of the information or the media holding the information. Indeed, in certain situations, LSPs may wish to consider purchasing the physical media on which its information will be stored at the outset of the relationship, so there can be no question regarding the right or ability of the LSP to recover media containing PCI.

k. Conduct Due Diligence on Information Backup, Disaster Recovery, Access Continuity, and Incident Response

Before sending information to a TPSP, the LSP should be satisfied that the TPSP has adequate plans and equipment for disaster recovery, backup of the LSP's information, and response to incidents such as data breaches. The LSP should also ensure that the TPSP is contractually obligated to provide access to its information without excessive down time and will have an appropriate level of technical support available when needed.

l. Require Assistance in Discovery

In the event that information under the control of the LSP is in the possession or custody of the TPSP and becomes subject to a litigation hold or discovery obligation, a TPSP should be contractually required to render timely assistance in preserving and collecting information, as appropriate. Accordingly, the TPSP contract should include a clear benchmark for "timeliness" to avoid confusion regarding the degree of delay acceptable in implementing a litigation hold and preserving and collecting the needed information. Similarly, the agreement should clearly set forth procedures to be followed by the TPSP if it directly receives a warrant, subpoena, or other civil or law enforcement request for the LSP's information. In most circumstances, the TPSP should be required to immediately notify the LSP and cooperate fully with it in responding.[95]

[95] In some situations involving requests from law enforcement authorities, immediate notification may be prohibited.

m. Limit Subcontracting and Onward Transfers

A TPSP generally should not be permitted to allow a subcontractor or other third party to access, process, or store the LSP's information without express prior approval for using the particular subcontractor(s) or allowing the onward transfer(s) of information. Likewise, LSPs should not approve any such arrangements without first confirming that the subcontractor(s) will be legally bound to comply with the same contractual provisions as the original TPSP.

n. Encourage Accountability Through Shared Liability

The contract between the LSP and the TPSP should consider proper incentives for compliance by imposing some form of liability on the TPSP for harm resulting from any failure to comply with its obligations under the agreement. LSPs should also consider requiring some form of indemnification of the LSP by the TPSP in the event of a data breach or other contract violation that exposes the LSP to liability. There are many potential mechanisms for imposing such liability, including liquidated damages, insurance, or indemnification of the LSP by the TPSP.

o. Provide for Inspection and Monitoring

The contract should also give the LSP a right to audit the TPSP's compliance with its information, privacy, and security obligations, or to receive copies of the reports of an independent auditor. If the TPSP is concerned about giving the LSP access to its facilities or systems to test it for conflicts and security concerns, the agreement should allow for use of a mutually acceptable third-party auditor. It is also critical that at least one thorough inspection actually be performed, and not merely permitted in theory. Additionally, parties should negotiate terms that contemplate updates to information privacy and security obligations as related technology and processes evolve.

p. Ensure Appropriate Access Controls for TPSP Personnel Given Access to LSP IT Systems

Where the contract calls for TPSP's personnel to have access of any sort to the LSP's own IT system, the LSP must make sure that it has appropriate safeguards in place. At a minimum, TPSP personnel who will have the ability to access the LSP's IT system should be subject to a background check, monitoring, and logging for unusual activity, and should have access to only the systems necessary to facilitate the purpose for which the TPSP was engaged. The contract should also address the TPSP's responsibility and role with respect to providing notice and remediation in the event of any loss, theft, or breach of information caused by TPSP personnel.

D. Step 4: Establish Processes for Timely Disposition of Records and Information

LSPs should consider establishing policies, procedures, methods, and technologies suitable for deletion and destruction of client and third-party PCI. Deletion of client information is necessary when directed by a client or triggered by the LSP's information retention policy. In general, information should be deleted when it is no longer needed. This means that LSPs should also ensure timely and

thorough deletion of confidential information on devices of departing employees and on retired drives and devices during technology upgrades.

To ensure deletion policies are clearly understood by clients, LSPs should consider, when appropriate, including a standard addendum to engagement letters that addresses the retention and disposition of client and third-party information. Such attachments should address standard policies and practices for the LSP handling the deletion of client information at the end of a matter and provide instructions for the client to communicate its express wishes for the disposition of its information. Mid-matter deletion of certain unneeded documents may also be advisable, if a matter involves particularly sensitive information and is not subject to a preservation obligation. If the provider plans to retain work product containing confidential client information after a matter has closed, because it has precedential value, the provider should clearly disclose its intention and obtain client consent. Standard policies and practices shared with clients about deletion of the client's files may address:

- whether the provider holds unique copies of documents potentially subject to a legal hold in other matters and whether the client would benefit from the LSP's retention of certain files from the closed matter;

- the level of sensitivity of the client's information held by the LSP;

- whether the client requires the LSP to retain certain documents, and whether other unnecessary files can be segregated and deleted;

- whether the client wants the LSP to send it a copy of the files to be deleted; and

- whether the client wants the LSP to keep copies of certain documents for safekeeping, and, if so, how those files will be stored.

The client engagement letter, or a related addendum, should also address the disposition of information if a client becomes unavailable after the close of a matter. In that circumstance, the agreement might allow the client's information to be disposed of following a designated waiting period and in compliance with the LSP's applicable legal and ethical obligations.

The waiting period should be set forth in the LSP's policies and made available to the client in the engagement letter. The addendum and a notice of the commencement of the applicable waiting period should be sent to the client after the matter closes. At the end of the applicable waiting period, the LSP should direct that the client's information be disposed of in accordance with the LSP's legal and ethical obligations, unless the LSP becomes aware of a reason to continue to hold the information, e.g., it becomes potentially relevant to other proceedings involving the client. Policies should set forth procedures for a legal hold of the LSP's information in the event the LSP has an expectation that the files may be relevant in future litigation.

LSP policies should account for whether the LSP may have any legal or other obligation to retain files after a client's matter concludes and whether it may need to retain a copy of any files as a record of the work it did for the client. LSPs may therefore wish to create a deletion schedule where the LSP's work product is held for a longer period than client-created or client-provided information. If the LSP determines it should keep its work product longer than its retention time, it should hold onto the work product for only a reasonable period.

In instances where a client does not consent to retention of its confidential information after the close of a matter, the client file retained by the LSP may still contain work product that the LSP wishes to keep as precedent, form, or history (such as legal memoranda, pleading drafts, or case notes). Under these circumstances, the LSP should "sanitize" those documents, removing PCI before storing the documents in the LSP's precedent bank or file repository.

Deletion of a client's PCI should be comprehensive and involve all locations where the information resides.[96] Deletion will likely require efforts by the LSP's IT personnel and by the employees who accessed client information. To the extent feasible, the LSP should confirm deletion from all potential locations, including document management systems, shared and private network storage, employee email, employee computers, electronic devices, external storage, backup files, and cloud servers. The LSP should also direct that the same steps be taken by any parties to whom they delivered client information, including opposing parties and TPSPs, as well as other LSPs. LSPs should deliver written confirmation to clients of having exercised reasonable diligence in the deletion of PCI.

E. Step 5: Implement Training Program

People have unfortunate tendencies to lose things, speak at inopportune times, open strange emails, visit inappropriate websites, and so forth. Accordingly, LSPs need to train their owners and employees. Begin with teaching people about written information security and privacy policies that document and standardize the provider's practices for maintaining information security and confidentiality. Training should cover client information generally and identify categories of information that may require additional protection, identify applicable federal and provincial or territorial laws, and explain the nature of the client information held and any contractual obligations applicable to it.

---

[96] "Deletion" methods and underlying hardware can differ in degrees of information recoverability. Physical shredding of the storage media is the most secure deletion of information but may be impractical. Therefore, more commonly acceptable standards of deletion include secure overwrite methods. Most drive electronics have built-in secure erase commands that can be activated with software and thoroughly erase the drive. LSPs may also consider using crypto-deletion where overwrite methods are insufficient or impractical, e.g., cloud services. Crypto-deletion involves encrypting information and destroying the encryption key rather than the information, rendering the information unusable. Deletion policies need to account not only for the LSP's technology infrastructure, but also regulations and requirements for specific types of information. For example, crypto-deletion may not be a valid solution if there is a strict requirement that the information must be scrubbed.

Information security and privacy policies clearly apply to all personnel who might handle PCI. This includes the LSP's most senior people, its owners, managers, employees, contract staff, and other parties engaged by the LSP who can access private or confidential information.

Annual training that meets the above criteria is no less important for solo practitioners and their staff than for large law firms. However, it may be impractical for a solo practitioner or small law office to create an internal training program. Instead, such LSPs should consider using an accredited third-party organization; for example, by attending a conference, arranging for an in-house presentation, or employing a web-based solution.

Illustration #14: The training paid off

Considering the impersonation attack that the firm's email banner just warded off, Alex is relieved that the training the firm's administrator took was worthwhile. Alex knows that LBS LLP holds $35,000 in trust for Real Estate Agent LLC and is glad that the firm's annual cybersecurity training—new hires are required to complete cybersecurity training, which the firm outsources to an online provider, and all staff have to renew it with a two-hour review once every two years—has prevented such a sizable potential loss.

The following elements are features that an LSP should consider including in its training program:

1. Make Training Mandatory for All Personnel

An LSP should consider making security training mandatory for all lawyers, paralegals, assistants, law clerks, contract staff, records staff, IT staff, and other personnel, regardless of whether such staff members will have access to sensitive information. Universal mandatory training is beneficial because the nature of IT systems and legal practice makes it highly likely that all employees will encounter private or confidential information at some point during their employment, and even those who do not could still be the source of a security breach that spreads beyond their own computers or office. It takes only one employee holding a door open for someone he or she does not recognize, or clicking on a link in an email message, to compromise an LSP's entire network.

2. Provide for Annual or Biannual Frequency

The nature of security threats and tactics used by hackers and social engineers is constantly changing, as is the underlying technology. Accordingly, LSPs should consider sponsoring training on an annual basis. In addition to formal training on at least an annual basis, periodic reminders or updates might also be sent to all personnel reminding them of best practices and updating them on emerging threats. Besides keeping personnel informed, such regular reminders show that the LSP takes information privacy and security seriously and expects its employees to do the same. Privacy and security training should also be mandatory for all new hires.

3. Provide for Accountability

There should be clear and meaningful consequences for personnel who fail to successfully complete training or abide by the LSP's privacy and security policies. For example, LSPs that pay bonuses might want to consider reducing bonus compensation for employees who fail to complete training in a specified time frame. Alternatively, they may wish to consider denying such employees access to the LSP's network until training is completed.

4. Include Core Content

An ideal training program may include the following content:

a. General Background and a Clear Statement of Importance

Training programs should include a general overview or primer that provides a context for addressing information security and privacy issues. This primer should give examples that demonstrate the significance of these issues and the serious consequences that may result when information is inappropriately handled. These examples should reinforce the direct connection between the LSP's adherence to information security and privacy principles and the LSP's reputation and success. This primer will therefore reinforce the serious damages the LSP may likely suffer if it—or its employees—violate laws surrounding information privacy/security or cause data breaches. These are both group and personal efforts, and training should convey that each employee is personally responsible for maintaining the LSP's standards for privacy and security.

b. LSP Policies

Training should include all aspects of the LSP's information privacy and security policies, including policies regarding the use of social media and mobile devices.

c. General Practices

In addition to explaining the LSP's own information privacy and security policies, training programs can include reasonable practices to maintain information security and privacy, such as those set forth in this *Commentary*.

d. Applicable Ethical, Legal, and Regulatory Rules

Training programs should cover ethical, legal, and regulatory rules applicable to the information held by the LSP.

e. Applicable Contractual Restrictions

If the LSP has access to information that is covered by contractual obligations, such as where a client has imposed additional information privacy or security restrictions on its information through a business associate agreement, training should cover and highlight those additional requirements.

f. Role-Specific Requirements

In larger organizations where some employees, such as human resources staff, may be exposed to a large amount of highly sensitive information covered by detailed regulatory requirements, additional role-specific training may be warranted for such employees.

g. Interactivity and Real-World Scenarios

LSPs may wish to consider implementing training programs that present "real-world" scenarios and prompt participants to indicate how they would respond under similar conditions. For example, such training programs might provide examples of methods successfully employed in the past by hackers and social engineers to bypass security controls and obtain access to private or confidential information. In this way, the trainee can learn from past mistakes made by others and hopefully avoid repeating them.

5. Conduct Testing

In order to facilitate accountability and ensure mastery of the training material, the LSP's training might also include a test that would be scored.[97] Failure to achieve a minimum score would require the individual to continue or repeat the training until a satisfactory score was achieved.

6. Consider Additional Messaging and Reminders

Larger organizations should consider supplementing formal training with posters, screen-saver messages, desk toys, and other aids to remind people on a regular basis of the importance of maintaining privacy and security over the LSP's information.

F. Step 6: Prepare for the Worst

An information security program is not complete unless it includes provisions for the worst possible scenario. Technical problems and human mistakes are inevitable: a device will almost inevitably be lost or stolen, a critical server will irreparably crash, a social engineer will send a phishing email that someone will click on, or an intruder will breach the firewall and either damage the IT system or steal something, or both. An LSP should prepare and test a data-breach response plan that anticipates common incidents.

---

[97] This approach is similar to that already used in many training programs about sexual harassment and other human resources issues.

This plan might consist of the following:

- Training all personnel to follow procedures for reporting and responding to potential information security breaches, including loss of devices or media, inadvertent transmission of information, or the interception or theft of information.

- Identifying a person or a team to direct the LSP's response to a breach incident.

- Creating a process for conducting a prompt investigation of a suspected breach, including assessing how and when the breach occurred, as well as what information sources have been compromised and what information is contained in those sources. (If an investigation would likely require third-party forensic or IT experts, they should be identified beforehand and listed in the LSP's policy.)

- Depending on the risk profile of the LSP, running periodic "fire drills" or "tabletop" exercises to test the plan under various scenarios.; (This will allow for the potential absence of employees who would ordinarily be critical to the successful implementation of the plan.)

- Developing procedures to mitigate damage when a breach is ongoing, bearing in mind that unplugging the affected computer may not necessarily be the best approach to defeat a sophisticated attack or to preserve important evidence. (Indeed, in some instances the "obvious" source of the intrusion may be a decoy meant to distract the security team from the real assault on the LSP's systems.)

- Establishing contingency plans for providing notice to the owners of compromised information, including clients and other interested parties after a breach or loss is confirmed.

- Developing procedures to revise and adjust policies after an unauthorized disclosure, loss, theft, or other data breach to avoid future occurrences.

- Implementing a system to receive news and updates of reported breaches outside of the LSP, which may affect the LSP's information security.

- Notifying appropriate law enforcement authorities and insurers.

- Abiding by applicable breach notification regulations.

Illustration #15: Back to the cottage	
Alex was under attack. But the firm's simple defences were enough to ward off the attacks and prevent loss of funds and sensitive client information. The firm's processes for dealing with an attack, in this case resetting passwords, wiping devices, and calling in suitable experts, was enough to ensure that no sensitive data was lost. Contented, Alex calls Bryce, who is still relaxing in the privacy of his secluded cottage, and continues to counsel a dear friend through a difficult time.	Finally tired of this string of failures, Haxor3k decides to move on to easier prey and abandons the attack on LBS LLP, but it saves the research, email accounts, and passwords for potential later use.

V. CONCLUSION

LSPs have the responsibility to take reasonable steps to protect PCI, a responsibility that is grounded in the ethics rules applicable to LSPs as well as in federal, provincial, and common law rules. In some situations, a duty may also arise under the laws of foreign nations. The nature of the risk, and significance of the potential consequences, must not be underestimated. This *Commentary* is intended to help LSPs assess security risks and provides guidelines for implementing privacy and information security policies. Where appropriate, reliance on third parties for risk identification, assessment, and mitigation measures will be necessary.