File Retention, Data Security and Claims

Lawrence Rubin
Director of Insurance

LAWYERS' INSURANCE
ASSOCIATION OF NOVA SCOTIA

TOPICS

- Topic 1: File Retention
- Topic 2: Data Security and Cyber Insurance
- Topic 3: Claims

The views and opinions expressed in this presentation are the presenter's and as such do not necessarily represent official policy or position of the NSBS or LIANS. In the case of file retention, both NSBS and LIANS are discussing this issue with the goal of developing a formal position for the membership. In the case of data security, the presenter is expressing personal experience. This presentation does not replace independent professional judgment or legal advice.

File Retention

- Some refer to this as document retention, others destruction, but the idea and question is the same: How long should files be kept? Put another way, when can they be destroyed?

- NSBS Succession Planning Working Group report included comments on document retention

- That report aside, there is a question, and an ongoing discussion, as to whether the Society can regulate this activity within the current regulatory framework. Accordingly, though there is now a regulation about succession, there is no regulation on document retention / destruction

- Which leads to the question – Should this activity be regulated?

- On document retention, the working group stated:

Based on information received by the Working Group, their view is that an analysis of reasonable risk should allow lawyers to develop destruction policies that would permit files to be destroyed after fifteen years. The specific form of authorization may need further consideration for it may be a regulation or a professional standard specifically authorized by regulation. The Working Group has not come to a conclusion on this and awaits Council's consideration of the policy before doing so.

Though any such permission should be broad based, there are definitely exceptions that would need to be clearly articulated. For example, the limitation clock for certain matters may have a delayed start date such as the settlement involving an injury to a minor in which case the file should not be destroyed until that person reached the age of majority (and perhaps for some time after that). Or, a file for the preparation of a will or pow er of attorney should not be destroyed if the client/former client is still alive. There are other examples and a comprehensive list will need to be developed.

Any rules in this regard will have to deal specifically with electronically stored data.

- This issue will be placed on the agenda of the Law Office Standards Committee who, among other things, can establish considerations to be had when developing a file retention policy

- Until there is a rule or standard, to the extent you or your firm wish to develop a policy (which in my opinion it probably should), you will have to develop it on your own

- There are resources you can access, for example from the Law Society of British Columbia at https://www.lawsociety.bc.ca/Website/media/Shared/docs/practice/resources/ClosedFiles.pdf

- If you develop a policy, in my opinion, such a policy should consider and / or contain, as appropriate, the following (in no particular order):

- The law (limitations, common law v. statutory duties, litigation holds)

- If documents are the property of the client, whether originals should be returned when the matter is completed. On this theme, if documents are scanned, there should be advice on what to do with the originals

- A requirement that the policy be known within the law firm, apply to everyone and be implemented consistently throughout the firm

- There should be a clear statement of how long documents / files are to be kept and exceptions, if any

- If there are to be exceptions to the general rule for specific files or documents, they must be clearly set out

- There should be rules for paper and electronic documents
- There should be a description of the types of documents that are within the organization and provisions and rules for specific documents you want to, or must, keep must be clearly set out
- There should be provisions for enforcement and audit and the policy should clarify who is responsible
- You may require different retention times for different types of matters, you may not be able to destroy a file unless there is another step
- The policy should set out where and how documents and backups are filed and kept

- you want to avoid a sanction or adverse inference if the file is unavailable. If you have a policy, follow it and a claim arises in a destroyed file, you will have to refer to your policy to explain and support the unavailability
  - If you destroyed the file after you became aware of the claim or the potential for a claim or are not in compliance with your policy, or apply it arbitrarily and inconsistently, there will be a problem

- There is no guarantee if you follow a destruction policy that there will never be an adverse finding. But hopefully such a finding is not because the file is unavailable

- If you want to vary from the policy, there should be a reason for so doing. A valid reason is not I will destroy the files I have a risk in and keep the ones I do not.

Data Security

- You are a potential target for hackers, ransomware and cyber criminals. Lawyers are seen as low hanging fruit though technologically, some of your clients might be lower for a cyber attack

- At a minimum, you should have:
  - a firewall between the your firm's systems and the internet;
  - up-to-date antivirus and malware endpoint protection on all computers and laptops; and
  - weekly data back-ups.

- For the first half of 2018, for known breaches*:
  - 74% of data breaches involved confidential information
  - Canada had third largest number of incidents (48) after U.S. (1074) and U.K. (65) but ahead of India (45) and Australia (24)
  - Canada ranked 9th in total records exposed
  - hacking accounted for 69% of breaches
  - 75% of incidents originated outside the organization
  - of incidents originating inside the organization, 53% were accidental
  - 60% of incidents were discovered externally
  - Total exposed records from the ten largest breaches: 2,447,339,630 being 91% of total records exposed

* Data from Cyber Risk Analytics analysis of reported data breach incidents: *Data Breach QuickView Report – Mid-year 2018 Data Breach Trends.*

- Your LIANS cyber policy has four coverages:

  - Liability resulting from a Cybercrime
    - If a client's confidential information ends up on the internet or is disclosed inappropriately because of a cyberattack against you, the client might have a claim for damages.

  - Privacy Breach Notification and Mitigation Expense Coverage
    - If your systems are compromised by cyberattack, you may have a legal obligation to notify clients and third parties of a privacy breach

- System Failure and Digital Data Asset Rectification Expense Coverage
  - A cyberattack can result in your firm losing or being unable to locate data that you need to get your clients' work done

- Cyber Threat and Extortion Expense Coverage
  - In some cyberattacks, hackers hijack computer systems and deny access until you pay a ransom (usually in an online currency known as bitcoin)

- Referring back to the coverage conditions, I would add a couple other things to the list that you can do that may also help prevent a data breach and cyber attack

- Though these are not preconditions to coverage under your insurance policy, they are things you can do to protect yourself and your client's information and they may save you a lot of grief

- Be skeptical
  - Not to the point of paranoia. But skeptical.

- Be diligent.

- If your vacationing partner sends you an instruction by personal e-mail or through their firm e-mail to issue a trust cheque or transfer funds because they forgot to do it before they left, call the partner up. If they are not available call the client. Do not reply email because the email address may be compromised and if so, you will be communicating with the fraudster

- If you receive an email from your bank, the CRA or some other entity you do business with that directs you to open an attachment or click a link to confirm your password and it seems odd, it probably is. Look at the sender's e-mail address – not what it shows up as but what it actually is by placing your cursor over it

Claims

- Real Estate claims remain our number 1 area of claims, both by volume and cost.

- Early comments that the LRA will result in a reduction of these numbers have not been borne out, at least not yet. But we are trying.

QUESTIONS?

Thank you for your invitation and your time

For more information on the insurance program including excess insurance, please go to our website www.lians.ca

LIANS 2017 Annual Report contains a summary of our financials and a recap of year. It is posted on our website at: http://www.lians.ca/sites/default/files/documents/00113441.pdf