The Law Society of British Columbia

Practice Resource

What to do if your laptop or briefcase is stolen

If your laptop or briefcase has been stolen or if you have otherwise lost control of your client's records, consult your security breach response plan. A "record" includes accounting records and supporting documents (trust account, general account. cash transaction and billing records); client identification and verification information and documents; and metadata associated with electronic records, and client file documents, whether in paper or electronic form).

If you do not have a plan, below is a short list of procedures to consider (not a substitute for a detailed plan). Determine the applicability of the procedures and their order in context.

1. Establish your response team, its responsibilities and priorities, including a communication plan to staff and others.

2. Contact your IT professionals to identify the problems, contain damage (they may have immediate tips) and advise you as to whether any client and banking records are compromised.

3. Report to your insurers immediately. If you bought cyber liability or other insurance to respond to a security breach, coverage may include assistance from data breach consultants and others regarding required steps, including procedures in this list. Contact the Lawyers Insurance Fund to see if you should also be making a written report to them.

4. If bank accounts and credit cards are at risk, contact those organizations. Consider recommendations and take steps to contain damage.

5. Contact a Law Society Practice Advisor if you have questions regarding your professional responsibilities (604.669.2533).

6. Report to the Law Society's Executive Director c/o Manager, Intake and Early Resolution in writing at professionalconduct@lsbc.org under Rule 10-4 (Security of Records). (Do not use your work email to report unless your IT professional says that it is safe.)

7. Figure out your legal obligations, including any obligations to third parties (e.g. other counsel, parties, the court). You may need to consult outside counsel.

8. Inform your clients if their information has been compromised or lost. It may be appropriate to recommend that the clients get independent legal advice. If the information obtained from the breach includes SIN numbers, credit cards, driver's licence information, bank information, or health cards, the clients may be exposed to identity fraud and loss

9. You may need to set up a telephone hotline to answer questions if the breach involves many clients.

10. Recreate client files as best as possible if information is missing.

11. Report to the police (optional but may be a requirement by some insurers).

12. Redesign or design your response plan from what you have learned.