ETHICS COMMITTEE OPINION

Lawyers' contact with expert witnesses

LAWYERS' CONTACTS WITH witnesses or potential witnesses are governed by section 5.3 of the *BC Code*, which provides:

> **5.3** Subject to the rules on communication with a represented party set out in rules 7.2-4 to 7.2-8, a lawyer may seek information from any potential witness, whether under subpoena or not, but the lawyer must disclose the lawyer's interest and take care not to subvert or suppress any evidence or procure the witness to stay out of the way.

In the opinion of the Ethics Committee, a lawyer must notify an opposing party's counsel when the lawyer is proposing to contact an opposing party's expert. Such notification promotes discussion between counsel about the permissible scope of such a contact at law, including the applicability of solicitor-client privilege. Failing agreement between counsel, either counsel may determine to take formal steps to resolve any issues.

Formal examination of an opposing party's expert witness is governed by the Supreme Court Civil Rules: see especially Rules 7-5(2) and 11-7.❖

NEWS FROM THE EQUITY OMBUDSPERSON

Respectful workplaces now expected

Anne B. Chopra

I HAVE OBSERVED a growing trend in the legal community: the expectation of a respectful workplace.

Treating each other with respect has become a prerequisite for building a successful and productive organization that will attract and retain lawyers and staff.

Firms can no longer afford to look the other way. There is a cost to doing nothing. When lawyers and staff are searching for new employment, one of their top concerns is, *how are people treated? What is the firm's reputation?* A poor reputation, lack of policies and structure, and lack of implementation of those policies will result in an inability to attract and retain top people. On the other hand, investing in healthy workplace behaviours will reduce staff turnover and training costs, foster staff commitment and innovation and contribute to staff well-being. This, in turn, results in greater job satisfaction and improved work performance.

We have heard it all before, so what has changed? Judging by the calls I have received over the last 14 years, there has been a definite shift in attitude. The lawyers I talk to seem to be more confident and are willing to take steps to secure a position in a firm that accepts the importance of work-life balance. They would rather risk losing the partnership track than stay at a firm that does not embrace their values. I believe lawyers today want, and expect, to feel respected and will not accept a work environment that is not supportive and does not respect the law.

If you are interested in learning more about respectful workplace behaviours and policies, the Equity Ombudsperson can assist you. A one-hour session is approved for one CPD credit towards the two-hour requirement (in professional responsibility and ethics, client care or practice management).

You can contact Equity Ombudsperson Anne Chopra by phone at 604.687.2344 or by email at achopra1@novuscom.net.❖

Services for lawyers

Practice and ethics advisors

Practice management advice – Contact **David J. (Dave) Bilinsky** to discuss practice management issues, with an emphasis on technology, strategic planning, finance, productivity and career satisfaction.
email: daveb@lsbc.org tel: 604.605.5331 or 1.800.903.5300.

Practice and ethics advice – Contact **Barbara Buchanan**, **Lenore Rowntree** or **Warren Wilson**, QC to discuss ethical issues, interpretation of the *Code of Professional Conduct for British Columbia* or matters for referral to the Ethics Committee.
Call Barbara about client identification and verification, scams, client relationships and lawyer/lawyer relationships.
Contact Barbara at: tel: 604.697.5816 or 1.800.903.5300 email: bbuchanan@lsbc.org.
Contact Lenore at: tel: 604.697.5811 or 1.800.903.5300 email: lrowntree@lsbc.org.
Contact Warren at: tel. 604.697.5857 or 1.800.903.5300 email: wwilson@lsbc.org.

All communications with Law Society practice and ethics advisors are strictly confidential, except in cases of trust fund shortages.

◆

PPC Canada EAP Services – Confidential counselling and referral services by professional counsellors on a wide range of personal, family and work-related concerns. Services are funded by, but completely independent of, the Law Society and provided at no cost to individual BC lawyers and articled students and their immediate families.
tel: 604.431.8200 or 1.800.663.9099.

◆

Lawyers Assistance Program (LAP) – Confidential peer support, counselling, referrals and interventions for lawyers, their families, support staff and articled students suffering from alcohol or chemical dependencies, stress, depression or other personal problems. Based on the concept of "lawyers helping lawyers," LAP's services are funded by, but completely independent of, the Law Society and provided at no additional cost to lawyers. tel: 604.685.2171 or 1.888.685.2171.

◆

Equity Ombudsperson – Confidential assistance with the resolution of harassment and discrimination concerns of lawyers, articled students, articling applicants and staff in law firms or other legal workplaces.
Contact Equity Ombudsperson, **Anne Bhanu Chopra**: tel: 604.687.2344 email: achopra1@novuscom.net.

PRACTICE TIPS, by Dave Bilinsky, Practice Management Advisor

Security practice tips

♫ Who can you trust these days
Cause people don't be about it like they say
Gotta be watching your back night and day
Who can you trust? ♫

Lyrics and music by Mint Condition

THE PARTICULAR VULNERABILITY of lawyers and law firms to hackers has been in the news as of late, so I decided to pull together some of the best tips I could find to improve the security of law firm IT systems:

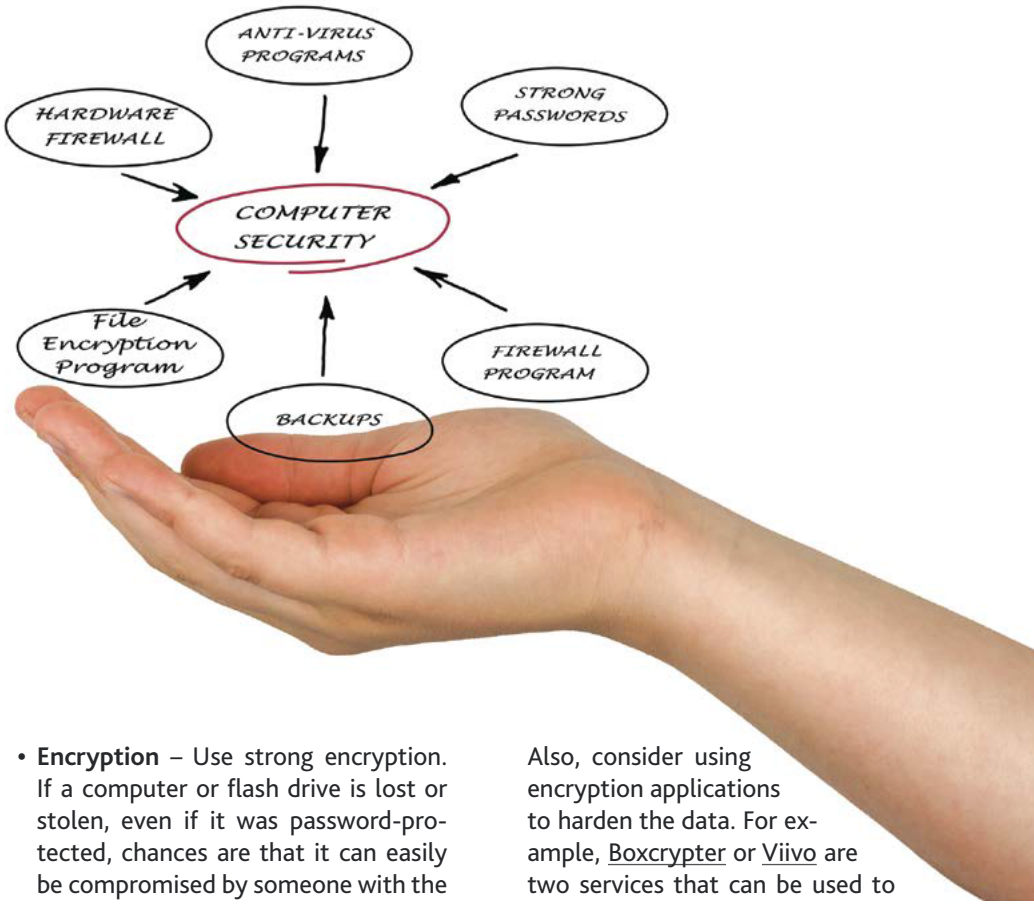
- **Acceptable use policy** – The first step is to put in place an acceptable use policy. There is a precedent on the Law Society website (see Practice Support and Resources > Model policy: Internet and Email Use Policy). The policy outlines the appropriate use of the firm's internet resources and establishes a clear expectation for staff use of these resources. Reducing a firm's vulnerability by implementing good practices and establishing appropriate standards for use of resources is a first step in increasing the security of the IT systems and data.

  The policy should be reviewed with staff annually and be consistently and strictly enforced. Needless to say, your acceptable use policy should state that you have the right to monitor all usage of the firm's IT resources to ensure that they are being used appropriately and that no vulnerabilities are being introduced into the system.

  Your policy should also state that the firm's resources may only be used for legitimate firm purposes. Sketchy websites are renowned for being infected with malware – and a business-only internet policy is a critical component of staying protected. If you do need to do research on the web that involves wide-ranging web searches, then you are advised to do so using a stand-alone computer that is not connected to the office network. You may wish to use a Mac, as they are, at least at this time, less vulnerable to some of the malware aimed to exploit Windows vulnerabilities.
- **Email attachments** – Do not click on email attachments without first determining that the email and sender are authentic. The cryptolocker malware (that locks up your system by encrypting files en masse and demanding a ransom be paid in order to de-encrypt them) is typically introduced by clicking on a ZIP file that is disguised as a PDF file. If you don't recognize the sender, it would be wise not to open any attachments. Even if you recognize the sender, if the email appears to be out of the ordinary, call the sender and verify that they in fact sent the email to you. They may have had their email address hacked or spoofed for the purposes of forwarding malware under the guise of being a legitimate email.

Reducing a firm's vulnerability by implementing good practices and establishing appropriate standards for use of resources is a first step in increasing the security of the IT systems and data.

- **System backups** – Maintain a backup of your data that is not connected to your network. This way, if your network is infected with cryptolocker or other malware, you should be able to retrieve a clean copy of your data.
- **Security software** – Periodically check that your security software is up-to-date and has not been compromised. For example, on the day of writing this column, TrueCrypt – hard drive encryption software – warned users that it was no longer secure and advised people to move to BitLocker (PC) or FileVault (Mac) instead.
- **Internet browsers** – Use a secure browser (in its Internet Browser Software Review, Purch ranked Mozilla Firefox, Google Chrome and Internet Explorer as the top three secure browsers in 2014). Take steps to increase the security of all browsers on your network as much as possible. For example, the computer security company Sophos advises that you:
  - Block third-party cookies (they can be exploited by cybercriminals).
  - Be wary of autocomplete (using autocomplete for log-ins poses a risk if your computer is stolen).
  - Restrict add-ons, as they can harbour malware and other security risks. At a minimum, configure your system so that you are prompted before these are installed.
  - Enable content filters. (All browsers maintain a database of phishing and malware sites. Turning on content filters ensures that this protection is in place.)
  - Turn on pop-up blockers (pop-ups can host malware or lure you into clicking on something that will install malware on your system).
- **Anti-virus software** – Install top-rated anti-virus software and ensure that it is kept up to date. For example, BitDefender Plus is consistently given a high rating, earning a 10/10 score for malware removal from Purch (see Best Antivirus Software Review).
- **Firewalls –** A strong firewall prevents unauthorized people from entering your system. A firewall can be implemented in hardware (wi-fi routers typically come with a firewall) or software. Next generation firewalls filter network and internet traffic and help detect unauthorized users. Gibson Research Corporation has a number of tests that you can run on your system to determine if your firewall and your system processor offer the best security possible (see Freeware and Security). They also offer other free tests to determine and shut down other vulnerabilities.
- **Passwords** – Use secure passwords.



Password insecurity is rife – everyone finds it difficult to remember several secure passwords, all containing a long string of random numbers, both uppercase and lowercase letters and symbols. To generate secure passwords, Gibson Research Corporation has created the Perfect Passwords feature that generates three 63-character, high-quality and cryptographic-strength passwords that are unique each time you visit the page.

Use a good password cache application. LastPass is consistently rated as an excellent password manager application, earning an outstanding rating by *PC Magazine* in 2014. LastPass stores all your secure passwords – all you need to remember is the one password to open LastPass.

- **Software updates** – Keep your operating system up-to-date and patched. Microsoft discontinued support for Windows XP on April 8, 2014, yet I still get calls from lawyers who are using XP machines! At the very least, upgrade to Windows 7 – if the computer can be upgraded – or, better yet, transfer your data off these old machines, perform a security wipe and then recycle them. For Mac users, Snow Leopard 10.6.8 has also discontinued support and users should upgrade to a newer version or, similarly, wipe the computer and recycle it. It is important to note that older machines may not be able to run newer versions of OSX. Using an unsupported operating system opens you up to attack as the vulnerabilities in the old system are no longer being patched.

  Install all application updates. Vulnerabilities are discovered all the time, so to be as secure as possible, you should configure your system to regularly check for updates on all applications.
- **Default settings** – Change key default settings that come with hardware and software programs. Hackers know these default settings, which may allow them to gain access. For example, there may be default administrator account names on servers and routers, and open ports on firewalls. Leaving these on the default settings increases your vulnerability.
- **Encryption** – Use strong encryption. If a computer or flash drive is lost or stolen, even if it was password-protected, chances are that it can easily be compromised by someone with the right software and skills. Encrypting your data is prudent. There are a number of encryption tools that you can use. Some experts advise using open source encryption, on the basis that proprietary encryption applications may have had "back doors" installed at the behest of the NSA.

Keep your operating system up-to-date and patched. Microsoft discontinued support for Windows XP on April 8, 2014, yet I still get calls from lawyers who are using XP machines!

- **The cloud** – If you store your data in the cloud, take extra measures to ensure that it is protected. Wikipedia lists a number of cloud services that use two-step verification, such as Dropbox, Evernote, LastPass, Google (including Gmail) and Yahoo mail. Turn on two-step verification and ensure that it is as difficult for someone to break into your data as possible.

  Also, consider using encryption applications to harden the data. For example, Boxcrypter or Viivo are two services that can be used to encrypt cloud storage providers, such as Dropbox.
- **Public wi-fi** – Use public wi-fi with care. There are tools available that allow people to sit in public wi-fi areas and capture log-in credentials and much, much more.
- **Mobile devices** – Ensure that your mobile devices can be remotely "wiped" if they are lost or stolen. All the major smart phone and tablets have some kind of remote erase capability. Ensure that it is enabled and you know how to initiate it.
- **Bring Your Own Device (BYOD)** – Be cautious about BYOD situations in which an outsider connects to your network. Each device increases your vulnerability. For more information, read Six Tips for BYOD Security from IBM, published by NetworkWorld.
- **The inside job** – Just one final thought … the most dangerous people may be those inside the moat, as they already have the credentials to get inside.

When it comes to IT security, you gotta be watching your back night and day!❖

Discipline Digest

BELOW ARE SUMMARIES with respect to:

- Rudi Gellert
- Thomas Paul Harding
- Roger Dwight Batchelor
- Alan Gordon Shursen Hultman
- David Donald Hart
- Douglas Warren Welder
- Stanley Chang Woon Foo

For the full text of discipline decisions, visit the Hearings reports section of the Law Society website.

RUDI GELLERT

Surrey, BC
Called to the bar: May 19, 1995
Ceased membership: December 16, 2003 (reinstated May 11, 2006) and January 1, 2011
Discipline hearings: July 18 and November 27, 2013
Panel: David Renwick, QC, Chair, Dennis Day and David Layton
Decisions issued: August 26, 2013 (2013 LSBC 22) and February 13, 2014 (2014 LSBC 05)
Counsel: Carolyn Gulabsingh for the Law Society; no one appearing on behalf of Rudi Gellert

FACTS

Between March 2008 and September 2010, Rudi Gellert misappropriated $14,486.69 of client funds by means of 31 transactions involving 31 different clients. Most of the transactions involved cancelling a stale-dated trust cheque made out to the client, after which the same amount was paid either to Gellert's law firm or a company run by his wife. The bulk of the money went to his wife's company.

Gellert's misappropriations were discovered during a routine compliance audit at his law office in October 2010. After the two Law Society auditors arrived, Gellert expressed displeasure and told one auditor that if he had a gun he would shoot someone. He also said that he would not allow the first auditor to look at any files and would not have her in his office.

Later on during the audit, Gellert refused to answer an auditor's question about a number of trust cheques he had caused to be made out payable to cash. He subsequently failed to respond to Law Society letters asking for information regarding these cheques as well as numerous other matters.

Gellert failed to appear at the hearing on facts and determination as well as the hearing on disciplinary action. The panel exercised its discretion to proceed with each hearing in his absence.

DETERMINATION

The panel concluded that Gellert had committed professional misconduct by misappropriating over $14,000 in client trust funds, making discourteous and threatening comments to a Law Society auditor and failing to respond to communications from the Law Society. It was also determined that he had breached three rules by issuing trust cheques payable to "cash" and failing to maintain proper trust accounting records.

The panel considered a number of factors, including that Gellert had deliberately misappropriated a substantial amount of client money. Further, the misappropriations occurred over a period of almost three years and involved 31 different clients. This was not a one-time misadventure on Gellert's part.

There was no evidence that any of the 31 clients complained. Since the money was taken from clients whose matters had concluded, it was likely that they did not realize that any funds were left owing to them. However, the failure of a client to know or complain about deliberate misappropriation does not mitigate the seriousness of the infraction.

Gellert received an indirect benefit from the misappropriations insofar as most of the funds were transferred to a company in which his wife was the sole director and officer.

A particularly aggravating factor was that there are 12 prior findings of professional misconduct against Gellert, arising from four different citations covering conduct occurring from 1999 to 2003, including a prior finding of misappropriation of client funds.

The penalty decision in Gellert's prior instances of misconduct shows that he came close to being disbarred. It was only the presence of significant mitigating circumstances that resulted in an 18-month suspension and the imposition of conditions on any return to practice.

Gellert returned to practice after his suspension and was prohibited from having signing authority over any trust accounts. This restriction would have underlined for him the paramount importance of properly managing trust accounts and avoiding any conduct that might put a client's trust money at risk.

However, six days after the Law Society removed the restriction regarding his handling of trust money, Gellert commenced misappropriating client funds. His actions demonstrated that even a lengthy suspension combined with practice restrictions and supervision were insufficient means of protecting the public from his continued misconduct.

DISCIPLINARY ACTION

The panel ordered that Gellert:

1. be disbarred; and
2. pay $8,630 in costs.