fucile & reising | LLP

July-August 2016 *Multnomah Lawyer Ethics Focus*

Law Firm Cyber Risk

By Mark J. Fucile
Fucile & Reising LLP

Law firms today depend on technology to deliver almost all facets of legal services. As practice has become more "electronic," law firms have also become more vulnerable to a variety of cyber risks. In this column, we'll look at three: data loss; theft of client funds; and unauthorized release of client confidential information. Because there is no one source of cyber threats, there is no single solution either. As lawyers use technology, however, they need to understand the risks that unfortunately accompany the important benefits that technology brings to our practices.

Data Loss

Data loss is not new. Law firm paper files and other records have long been vulnerable to catastrophic loss from hazards ranging from fires to floods. With the increasing shift to "paperless" offices, however, data loss has taken on a new and potentially more ominous meaning. A data loss in today's electronic context may mean that the lawyer or firm has effectively had their entire office "burned down."

OSB Formal Opinion 2011-188, which addresses cloud computing generally, notes that a part of our duty of competent representation under RPC 1.1 in a "paperless" practice environment is to make sure that electronically stored information is backed-up. The particular means used will vary depending

on the size of the firm involved and will also evolve as technology changes over time. The imperative of preserving firm data and ensuring continued access, however, remains the same. The Oregon State Bar Professional Liability Fund has a number of very practical guides and checklists available on its web site (www.osbplf.org) to assist Oregon lawyers in preventing catastrophic loss of both conventional and electronic records.

Theft of Client Funds

There are few "bad things" that can happen to a lawyer or firm on the risk management front that are worse than a theft of client funds. We have significant fiduciary and regulatory (RPCs 1.15-1 and 1.15-2) duties to safeguard funds clients have entrusted to us. Moreover, the PLF basic plan considers trust accounting an administrative rather than a legal services component of law practice and, therefore, does not cover it. In fact, the comments accompanying the coverage section of the current plan (Section III at 8 of the 2016 Plan) give an example of a common Internet scam that is not covered by the PLF plan: a lawyer is duped into accepting a fraudulent check from a supposed new client and then wire-transfers funds out of the firm trust account to a recipient who, unknown to the lawyer, is a participant in the scam. The check then bounces

and the lawyer's wire-transfer, in effect, sent other clients' money to the person masterminding the fraud.

Again, the PLF has a number of guides and alerts on its web site addressing common scams aimed at lawyers. These are not only helpful in proactively warning lawyers but also offer sound advice on vetting prospective clients and allowing sufficient time for trust account deposits to clear before writing new checks on those funds.

Unauthorized Release of Confidential Information

In December 2013, the Oregon Supreme Court adopted an amendment to the confidentiality rule—RPC 1.6(c)—that made specific a lawyer's duty to protect client confidential information from unauthorized disclosure: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." The 2013 amendment mirrored a similar change to the ABA's influential Model Rules of Professional Conduct and reflected earlier guidance offered by the Oregon State Bar in Formal Ethics Opinion 2011-188 on cloud computing.

The amendment to RPC 1.6 dovetails in many respects with the statutory duties law firms have under ORS 646A.622 for protecting particular categories of

sensitive personal information—such as Social Security or credit card numbers—that fall within the Oregon Consumer Identity Theft Protection Act (ORS 646A.600-.628). If a data breach occurs, ORS 646A.604 specifies the notice to the clients affected that must occur. The PLF has developed a template notification letter that is available on its web site. Notification and related remedial expenses can be significant depending on the extent of the breach involved. Although the PLF basic plan does not cover data breaches, its excess plan includes a cyber liability and breach response endorsement that provides (among other features) legal and forensic assistance to determine compliance with applicable law and to implement appropriate mitigation measures. Private carriers also sell cyber risk plans.

Although a data breach can occur as a part of a sophisticated hacking scheme, it can also come through the more mundane loss of an unprotected firm laptop computer or other mobile device. To guard against the former, firms need to obtain competent technical systems and advice commensurate with their size and practice. For the latter, firms need to follow simple steps such as password protection. Formal Ethics Opinion 2011-188 also makes the point that what is "state of the art" for security when selecting a storage system may not remain

that way and that lawyers need to stay abreast of changes in the technology they are using in their practices.

ABOUT THE AUTHOR

Mark J. Fucile of Fucile & Reising LLP handles professional responsibility, regulatory and attorney-client privilege issues for lawyers, law firms and corporate and governmental legal departments throughout the Northwest. Mark has chaired both the WSBA Committee on Professional Ethics and its predecessor, the WSBA Rules of Professional Conduct Committee. Mark is also a former member of the Oregon State Bar Legal Ethics Committee and is a current member of the Idaho State Bar Section on Professionalism & Ethics. Mark writes the monthly Ethics Focus column for the Multnomah (Portland) Bar's *Multnomah Lawyer*, the quarterly Ethics & the Law column for the WSBA *NWLawyer* and is a regular contributor on legal ethics to the WSBA *NWSidebar* blog. Mark is a contributing author/editor for the current editions of the OSB Ethical Oregon Lawyer, the WSBA *Legal Ethics Deskbook* and the WSBA *Law of Lawyering in Washington*. Before co-founding Fucile & Reising LLP in 2005, Mark was a partner and in-house ethics counsel for a large Northwest regional firm. He also teaches legal ethics as an adjunct for the University of Oregon School of Law at its Portland campus. Mark is admitted in Oregon, Washington, Idaho, Alaska and the District of Columbia. He is a graduate of the UCLA School of Law. Mark's telephone and email are 503.224.4895 and Mark@frllp.com.