fucile & reising | LLP

March 2021 *Multnomah Lawyer Ethics Focus*

Getting Covered:
Cyber Risk Insurance

By Mark J. Fucile
Fucile & Reising LLP

The Oregon Department of Justice has a cyber breach database on its web site that lists breaches involving at least 250 Oregon residents that were reported to DOJ as required by state law. It makes for sobering reading. Both the number and type of institutions involved illustrate how common breaches have become. Professional service firms are not immune from this trend. A number are included in the DOJ database. Because professional service firms like law firms often have extremely sensitive client information in their electronic files, they make inviting targets for bad actors who are either looking to steal the information involved or hold it hostage. The former is often the functional equivalent of insider trading—with the thieves looking for valuable information, such as merger negotiations in advance of a public announcement. The latter is usually called "ransomware" and effectively locks a firm out of its own network by encrypting its files with malicious software.

Any cyber intrusion raises difficult technical questions of assessment and repair. Further, if a breach has occurred and personal information has been taken, data breach notification laws (in addition to "communication rule" for current clients—RPC 1.4) require very specific information to be communicated to the persons affected and, depending on the size of the breach and the type of

information, a variety of government agencies must also be notified. Although costs vary, responding to a serious cyber intrusion is never cheap and for most firms is an "unbudgeted expense." Cyber risk insurance coverage, therefore, should be a key element in any law firm's overall risk management plan.

In this column, we'll first briefly survey why responding to a cyber breach is inherently expensive. We'll then turn to available insurance coverage.

Cyber Breach Response

When a breach occurs, law firms typically incur expenses in two primary areas.

First, sophisticated technical help—often from outside vendors specializing in this field—is usually necessary to assess the nature of the breach, undertake repairs and attempt to restore or recover the files involved. A technical assessment, for example, may be needed to determine whether the firm's systems have actually been penetrated or whether the firm has simply been "locked out" of its files through ransomware encryption. The nature of the attack, in turn, may impact the nature of notification. If personal data was exposed, then statutory notification duties likely have been triggered. If not, then notification statutes may not be involved but the firm may still have a duty to

notify its clients if, for example, the firm's inability to access its files will materially impact continuing time-sensitive client work.

Second, equally sophisticated legal help—often from outside law firms specializing in this field—is also usually necessary to guide a firm through the notification process and possible related public media statements, interface with law enforcement and help assess the firm's own exposure. Depending on the firm's clientele, more than one state's notification laws may have been triggered. For example, a Portland firm serving clients both there and Vancouver would likely have to take account of both the Oregon and Washington notification statutes. Although similar, each state's law contains nuances on the content and timing of notice and whether state governmental agencies must also be notified. The notification statutes generally do not distinguish between clients and non-clients—focusing instead on defined categories of personal information that, if revealed through a breach, require notification. For example, a defense firm in a personal injury case may have sensitive medical and tax records obtained through discovery from a plaintiff. Depending on the content of the information, federal and even international notification regulations may also apply.

Insurance Coverage

From a management perspective, cyber risk coverage accomplishes two important tasks.

First, a carrier provides a contact point to access the critical, time-sensitive technical and legal help that a law firm needs. The shift to largely electronic files over the past decade combined with the sensitive nature of their contents means that a firm can't simply ignore a cyber intrusion and hope it will go away. Similarly, the middle of a cyber breach is not a good time to learn either new technical or legal skills by trying to solve the problem yourself.

Second, insurance can help defray what are often significant expenses for the technical and legal assistance needed. Importantly for Oregon lawyers, the PLF Basic Plan does not include cyber coverage. The PLF Excess Plan, however, does include coverage for both liability arising from a breach and the costs of response. More information about the scope and limits of PLF coverage is available on its web site at www.osbplf.org. Private carriers also offer a variety of cyber policies that can be integrated into a firm's overall blend of coverage. Like the threats, coverages also vary and should be evaluated in the context of a firm's particular practice. For one firm, for example, the largest risk may be its own exposure if commercially sensitive client information is stolen. For another,

it may be the interruption in time-sensitive client work while the firm network is restored. For those in firm management, the ABA has published an excellent resource—the Cyber Security Handbook (available through the ABA web site)—that includes an entire chapter on cyber risk policies and highlights their nuances and variations.

ABOUT THE AUTHOR

Mark J. Fucile of Fucile & Reising LLP handles professional responsibility, risk management 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 a member of the Oregon State Bar Legal Ethics Committee and the Idaho State Bar Section on Professionalism & Ethics. Mark writes the Ethics Focus column for the Multnomah (Portland) Bar's *Multnomah Lawyer*, the Ethics & the Law column for the WSBA *Bar News* 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.