

PRACTICE TIPS

CYBER SECURITY POSES INCREASING CHALLENGES FOR LAW FIRMS

by W. Brian Ahern, RPLU

Cyber security is increasingly on the minds and agendas of business leaders across a wide spectrum of industries. A recent [CFO Magazine article](#) on risk management reviewed a report by the Corporate Executive Board (CEB) ranking information security as the top priority risk for 2012; tellingly, data security wasn't even among the top three concerns in CEB's 2008 survey.

It's no wonder that concerns over cyber security have risen – and continue to rise – so dramatically. The [Privacy Rights Clearinghouse](#), a San Diego-based nonprofit organization tracking data security issues, estimates that since 2005 data breaches have affected over 540,000,000 records. A PwC study published in November, the [2011 Global Economic Crime Survey](#), notes a striking increase in cyber crime since 2009 and reports that 42% of respondents expected to encounter some sort of cyber crime in the next 12 months. The issue was of such importance that PwC's US supplement to the global survey is titled "[Cyber crime in the spotlight.](#)"

As dramatic and headline-grabbing as cyber crime is, cyber security involves more than protecting against hackers and cyber thieves. Data breaches can occur due to lost or misplaced laptops and portable devices. The phenomenal increase in social media use has also added a number of new and unanticipated challenges to protecting sensitive information.

Along with every other business, law firms must also put cyber liability on their list of critical management issues. Client relationships center on trust, and protecting that trust includes protecting the sensitive information divulged in the course of representing individuals and businesses. Law firms must also be vigilant in protecting the private information of clients, the firm and employees.

Along with the grave professional repercussions of a breach of cyber security, law firm leaders should consider

the financial implications of cyber exposure. Breaches can be extremely costly, with an estimated cost to rebuild records at over \$200 per record – and that's just the tip of the iceberg. While law firms have been slow in exploring cyber insurance, firms should take a hard look at their existing policies as soon as possible and ensure that their coverage is adequate.

Coverage options to consider include privacy (the unauthorized acquisition, access, use, physical taking, identify theft, mysterious disappearance, release, distribution or disclosures of personal and corporate information, including breaches by rogue employees and unauthorized third parties); technology security; web-media services, including Internet and intranet websites; privacy breach containment; technology extortion; and data restoration.

Your insurance broker can help you review the various types of policies and help decide which coverage you need. With the risks high and the cost of coverage relatively low, no law firm should go without cyber liability coverage.

While cyber security is an evolving area, firms can turn to a number of resources as they build their defenses, in addition to those listed above. Among them: the [FTC's Bureau of Consumer Protection](#), the [California Office of Privacy Protection](#) and the [Ponemon Institute](#).



W. Brian Ahern, RPLU, is President / CEO of Ahern Insurance Brokerage, one of the largest independently owned insurance brokerage firms specializing in the insurance needs of law firms. Ahern Insurance Brokerage is the Designated Professional Liability Broker for the OCBA.

AHERN | INSURANCE
BROKERAGE