Enhanced Cybersecurity Is Imperative For Arizona Lawyers

Cybercriminals often consider lawyers an attractive and vulnerable target.

Stories about massive computer hacking appear with increasing frequency. The perpetrators include state actors, sophisticated criminal operators around the world, political groups, and disgruntled employees.

Why Lawyers are Prime Targets

Victims of cybercrime include major corporations, political campaigns, and government agencies. Lawyers are not immune from this phenomenon.

To the contrary, cybercriminals often consider them an attractive and vulnerable "weak link," given (1) their relative lack of sophistication in using technology to protect confidential information and (2) the wealth of information they may possess, such as confidential information about cases, client information (including intellectual property), privileged communications and attorney work product, and "personally identifiable information" for employees, clients, and third parties (including health information and account-access information, like names, addresses, and payment card and PIN numbers).

Within the last year, very major – and technologically savvy – international law firms have suffered major breaches. A recent study in Great Britain reported that a quarter of all law firms there have suffered cyberattacks.

Ethics Guidelines and Legal Statutes

In Arizona, it is not just a matter of good business practices to use effective, up-to-date methods for protecting the confidentiality of your practice's electronic information.

Arizona's Ethics Rule 1.1 governs attorney competence. Its comments expressly state that lawyers must maintain requisite knowledge and skill, "including the benefits and risks associated with relevant technology." Ethics Rule 1.6(e), on maintaining confidentiality, requires that, "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." (See also, Comments 22 and 23.)

Federal law – for example HIPAA Privacy Regulations – and Arizona statutes mandating protection of "personally identifiable information" also make it a legal, as opposed to ethical, obligation to protect certain types of electronic information.

The consequences of not meeting these obligations are significant, including: suddenly losing access to one's own work product and documents; malpractice liability; ethics claims; loss of clients; and negative publicity.

Steps to Reduce Your Risk

It is challenging to keep pace with rapidly changing technology and sophisticated cybercriminals. There are, however, steps that will significantly reduce your risk of data breaches, including:

- **Require encryption of confidential information** on laptops and mobile devices, and when using email or other methods of transferring files – every time confidential information enters or leaves the firm.
- **Use cloud computing software** that offers secure online storage, redundant data backup, and built-in disaster recovery plans.
- **Use strong passwords in computers and other devices.** The more complex the password, the more effective it is. Consider using password manager programs that store passwords in encrypted form and allow safe access to them from multiple devices.
- **Use online, web-based client portals instead of email to share sensitive information.** These are often part of practice management software and allow easy, secure communication and document transmission.
- **Use strong intrusion detection and counter-espionage software** to detect malware and prevent loss of information, and have experienced IT forensic specialists available.
- **Have up-to-date written policies addressing cybersecurity,** including a breach response policy on how the firm will respond, as well as a policy on computer and device use.
- **Provide regular, effective user education** on firm policies and procedures, risks, and trends.

Steps such as these will significantly help you meet your ethical and legal obligations for protecting confidential information.

No portion of this article is intended to constitute legal advice. Be sure to perform independent research and analysis. Any views expressed are those of the author only.