Why Do Lawyers Resist Ethical Rules Requiring Competence with Technology?

By Sharon D. Nelson, Esq. and John W. Simek

Recently, the Virginia State Bar Council voted to adopt changes to the Model Rules of Professional Conduct. The changes were based on the American Bar Association's modifications to the Comments of Rule 1.1 respecting Competence ("…a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with technology…") and Rule 1.6 respecting Confidentiality ("(c) A lawyer shall make reasonable efforts to prevent the unintended disclosure of, or unauthorized access to, information relating to the representation of a client.")

What's reasonable? The Comments go on to list relevant factors:

1. the sensitivity of the information
2. the likelihood of disclosure if additional safeguards are not employed
3. the cost of employing additional safeguards
4. the difficulty of implementing the safeguards
5. adverse effect on the lawyer's ability to represent clients

The Comments also make it clear that the client can demand more security or, with informed consent, accept lesser measures. This was not adopted by the VSB Council, but many states have adopted it.

As to the remainder of the changes, which were adopted and will now be sent to the Supreme Court of Virginia for its blessing before becoming final, there was quite a firestorm prior to the final vote adopting the proposed rules.

Even before the Council met, there had been comments received on the proposals, saying things like "I believe it is unreasonable to expect a lawyer to become an IT professional in addition to all of our other responsibilities." This was echoed at the Council meeting.

This is a misunderstanding of the requirement. The change does not require a lawyer to become an IT professional – indeed, for most lawyers, dabbling in IT

would be dangerous. They need outside or inside IT help in most cases – the small firms generally contract IT work to an outside IT service company. But all lawyers should be aware of the benefits and risks of technology to be a competent lawyer in the digital era. Hence, the change to Rule 1.1 makes good sense.

Another comment made the point that technology is the only form of competence specifically referenced in the proposed rule.

We are all accustomed to taking CLE each year to maintain our competence as attorneys in the fields of law in which we practice. However, it is uncontroverted that the most disruptive force we have ever seen in the practice of law is technology. It is pervasive – and becomes more so with each successive generation of lawyers. We have reached the point in time where a lawyer cannot effectively practice law without technology – which makes it an imperative that lawyers know something about the technology they use.

We live in a "breach-a-day" world which suggests even more strongly that we need to pay attention to sensitive client data. According to a 2013 Mandiant Threat Report, law firms and consultants constitute 7% of the targets of advanced attackers. This has come to mean that we are the easy route to getting the data of our clients. Cybercriminals and state-sponsored hackers alike have attacked law firms, large and small – and they are all too often successful because employees are not trained in safe computing, security patches and updates are not installed, out-of-support software (receiving no security updates) continues to be used, and they do not employ encryption.

All of this can be addressed by a competent IT professional. Are there costs? Yes, certainly, but they are a matter of scale. The costs will be far greater for a large firm than for a solo or small firm practitioner. The measurement of "acting reasonably" is obviously different depending on the size of the firm.

In spite of all the rhetoric about "small firms can't afford this requirement" the truth is that many reasonable precautions cost nothing. Installing security patches is free – yet it is frequently not done. It costs nothing to encrypt a Word or PDF attachment with a password before sending it. Encryption is already a built-in feature of modern computers and smartphones – it may need to be enabled, but it is there.

You can encrypt e-mail easily these days with inexpensive products like ZixCorp, to name just one. A lawyer doesn't need to understand the mathematics of encryption – only how to use the products. And they are fast and easy to learn. You don't need to use encryption all the time, but when you are sending sensitive data, you probably should. You know what you have to learn? How to hit the "Encrypt and Send" button. That's it.

Using the cloud to hold data is fine, so long as you understand the security precautions. Chiefly, if you encrypt the data before sending it to the cloud, your data is safe because only you hold the decryption key. Holding the encryption key yourself means the cloud provider has "zero knowledge" of the decryption key – and that's the kind of cloud provider you want. There is no additional cost to this – you just have pick the right provider. As an example, SpiderOak is a "zero knowledge" file synching cloud whereas Dropbox holds a master decryption key and will, if given the proper paperwork, turn over your data to the authorities. We like SpiderOak and others that are moving in the "zero knowledge" direction, a far better solution for lawyers.

There is no cost to forbidding employees by policy from connecting to the law firm network with personal devices. Who knows what malware may exist on those devices? Large firms may choose to use sophisticated techniques to manage personal devices, but smaller firms are better off simply forbidding them to connect to the network.

There is a long list of free or reasonably priced safeguards for data, but that's why attorneys should go to CLEs – to learn them and see that they are implemented by their IT provider. How about making sure lawyers use strong passwords (and not same password everywhere) and change them (especially their network credentials) regularly?

The changes to the Model Rules require only reasonable safeguards and give a host of factors to be considered in determining what is reasonable. In some cases, where lawyers hold HIPAA data or data containing personally identifiable information, they may be governed by state or federal law beyond the scope of the proposed rules, which is noted in the new comments to Rule 1.6.

So why all the hoo-ha at the Council meeting? Largely, we believe that there are fundamental misunderstandings about the changes and what they mean. There is also a mentality – so common in the legal profession – that "we've always done it this way." One person actually said that lawyers shouldn't be required to do more to protect data in the digital world than they were in the paper world? Say what? It defies belief that this sentiment has such a strong hold on so many lawyers, but it does. Perhaps the speaker didn't realize that over 93% of documents are created electronically and that more than 50% of them are never printed.

One young lawyer took the microphone to point out that the digital world is a new one – and requires us to adapt. We might add "or face extinction."

Taken as a whole, what we cannot do is turn a blind eye to the impact of technology on our profession. There was a time when protecting client data involved locked file cabinets in a locked office. Today, we must still "lock" the data – digitally. The new modifications to Rule 1.1 and 1.6 are a measured and technology-agnostic step toward applying old rules to the 21st century.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com