OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXVII NUMBER II
FEBRUARY 2020
www.mnbar.org

Bench&Bar MINNESOTA

eDiscovery without the endless battles

Minnesota needs more foreign-trained lawyers

THIRD CHILD. FIRST REAL PARENTAL LEAVE.

Why Minnesota should join the ranks of states making it easier for lawyers to take parental leave

Taking responsibility for your cybersecurity

Cyberthreats continue to be a huge source of risk for public and private organizations alike. On December 4, the Senate's bipartisan cybersecurity caucus learned about the threat that ransomware poses and discussed learning, mitigation, widespread education, and the importance of information sharing in constructing realistic protection measures.[1] While the hearing emphasized the need for public and private interplay to best face the difficult-to-manage nature of evolving cyberthreats, U.S. Sen. Angus King (I-Maine) pointed out, "The federal government can't provide support for every institution in America that's subject to ransomware." And while that may sound bleak, I think it is simply an acknowledgement of our current reality. When it comes to our digital age and its expansive impact on the way we conduct our lives, it is ultimately the responsibility of each entity (really, each individual) to protect themselves and take a proactive approach to their security.

MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 matters. He is a member of the MN Lawyers Professional Responsibility Board.

The risk of falling victim to a ransomware attack is one of many possible cyberthreats that organizations face. Law firms are at particular risk given the sorts of sensitive client data they collect and store. In previous articles, I have expounded upon the dangers of social engineering attacks, and more particularly, the risks associated with phishing attacks. Social engineering takes advantage of human vulnerabilities rather than technological weaknesses. Cybercriminals often do their best to make a phishing email appear legitimate, attempting to make an employee carry out some action and to do so quickly. They often capitalize on urgency to cloud an employee's sense of something seeming out of place.

Ransomware attacks are often introduced via social engineering methods, particularly by email, and will block access to or threaten dissemination of an organization's data until a ransom is paid. Public and private organizations, including law firms, have been made victims of ransomware. Breaches of this kind are costly in more than one way, and as discussed recently by the cybersecurity caucus, could have devastating future effects on government entities.

Given the methods by which cyberattacks are introduced and the fact that cybercrime is constantly evolving to match new technologies and security measures, it only makes sense that the ultimate responsibility for cybersecurity postures rests within organizations. No framework, guidance, or amount of federal support could account for the multitude of ways in which a cyber event can transpire. While such support systems may be helpful in providing some sort of guidance, as I discussed in my last article, pursuing compliance with a standard set of best practices does not automatically ensure that an entity is secure. Federal support may aid in compliance, but the day-to-day requirements and cultures of security needed to combat cyberthreats can only be developed and maintained in-house. Resisting internal security protocols and failing to provide adequate budgeting for these measures will undercut any degree of compliance that an organization may believe that it has achieved with respect to federal guidelines. For the legal community, prioritizing cybersecurity means prioritizing clients, their sensitive information and privacy, and the reputation and future of the firm.

So with respect to Sen. King's comment, it's probably true that the federal government cannot reasonably assist each and every organization that is subject to the sort of cyberthreats we face today, especially when each and every organization is at risk. When it comes to security, compliance is no guarantee. But it is nonetheless within these organizations that security cultures can flourish and thrive. Information sharing, proactive strategies, education, and the sorts of countermeasures that the cybersecurity caucus proposed all rely on individuals for their widespread implementation and support.

As we start the year 2020, a good resolution for all of us may be to take heed of our personal responsibility in bringing about the sort of security awareness for which our organizations and firms aim. ▲

[1] *https://www.fifthdomain.com/congress/capitol-hill/2019/12/04/heres-what-senators-learned-about-the-ransomware-threat/*