The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2015
PHILADELPHIA, THURSDAY, DECEMBER 17, 2015 VOL 252 • NO. 118 An ALM Publication

PARALEGALS PAGE

The Paralegal's Role in the New World of Cybersecurity

BY VICTOR F. PANIECZKO
Special to the Legal

Cyberattacks have affected virtually every industry. These include, but are not limited to, health care, education, finance, energy, retail, hospitality and government. Most of us have seen or heard about the security breaches of Home Depot Inc., eBay Inc., Target Corp., Sony Pictures Entertainment, JPMorgan Chase, and the U.S. Office of Personnel Management. What is cybersecurity? The National Initiative for Cybersecurity Career and Studies (NICCS) defines cybersecurity as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation." Oxforddictionaries.com states that cybersecurity is "the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this." Finally, Webopedia.com characterizes cybersecurity as "the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks."

Cybersecurity is by all accounts a growing challenge. Today, hackers are more advanced and better equipped. Their success mostly depends on finding a hole, or vulnerability, that goes unpatched or unnoticed by defenders. The more difficult a system is to infiltrate, the more time, energy and skill hackers must invest into cracking that system. More attacks are coming from highly skilled and sophisticated hacker groups, with their motivations varying from monetary gain to disruption and injury to their targets for any number of non-monetary reasons.

VICTOR F. PANIECZKO *is a paralegal with Flaster Greenberg. He is currently serving as a board member of The Philadelphia Association of Paralegals and chair of its technology committee. He can be contacted at 215-587-5674 or victor.panieczko@flastergreenberg.com.*

Virtually every cybersecurity expert and commentator agrees that the threats to cybersecurity are evolving and growing more worrisome. Risks associated with cybersecurity have escalated for many law firms, managing partners and corporate boards of directors. They are working and prioritizing cybersecurity to establish security awareness throughout the organizations and demonstrating cybersecurity as an enterprise priority. Lawyers and law firms handle highly sensitive and confidential client data and play a critical role in assisting general counsel on how to handle a cyberbreach when information is compromised. Edward J. McAndrew, assistant U.S. attorney and cybercrime coordinator, explains what have been the most significant developments in the area of law firm cybersecurity:

"Because of the information entrusted to them, the sensitive matters they handle, and the prominent positions in society they often occupy, lawyers are primary targets for all types of cyberattacks. ... Cybersecurity has become both an ethical obligation and business imperative for law firms of all sizes. The Model Rules of Professional Conduct and the ethical rules of a growing number of state bars expressly encompass obligations to secure, and to maintain the confidentiality of, client data. Clients are under increasing pressure to secure their own and their customers' data. They are applying that pressure on law firms."

Many law firms have offices around the globe, and their clients' operations are constantly expanding. Clients conducting business in industries such as health care, banking and financial services, retail and telecommunications are at a high risk for cybersecurity breaches. Clients are raising their cybersecurity concerns with their lawyers and looking for advice from law firms on how to protect against a breach and design a security plan in case a breach does occur. When asked if paralegals will be involved in their law firms' processes of creating and developing cyberrisk management protocols, Joseph Raczynski, technology manager from Thomson Reuters, explained that "it makes natural sense that paralegals who have an interest in process and cybersecurity take a significant role in managing these protocols. Paralegals touch so many aspects of the firm. They use various applications, websites, manage

large volumes of data and email. All of these facets can be an entryway for viruses, malware and hackers. Paralegals who have a natural inclination toward process and an interest in cybersecurity would be a great fit in this realm to help fill the void at the firm."

On a large scale, law firms handle and store a large volume of their clients' confidential information in their networks. Law firms are vulnerable targets for hackers because they represent clients in high-risk industries. The more high-volume and sophisticated clients they have, the better information they possess, and the more value it holds for hackers. Lawyers are holders of clients' personal and legal information and have an ethical duty to protect client data. The American Bar Association Model Rules of Professional Conduct, in Rule 1.6(c), state, "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." Corporate and individual clients entrust their lawyer and the law firms with their sensitive and confidential data. A client's data might relate to intellectual property, employment or labor disputes, real estate, political matters, victim statements, and witness and expert identities and testimonies. Benjamin M. Lawsky, New York State Department of Financial Services superintendent, stated in a letter to CEOs, GCs and CIOs:

"Recent cybersecurity breaches should serve as a stern wake-up call for insurers and other financial institutions to strengthen their cyberdefenses. Those companies are entrusted with a virtual treasure trove of sensitive customer information that is an inviting target for hackers. Regulators and private-sector companies must both redouble their efforts and move aggressively to help safeguard this consumer data."

Further, DFS "encourages all institutions to view cybersecurity as an integral aspect of their overall risk management strategy, rather than solely as a subset of information technology."

Because law firms these days have highly mobile workforces, they should be aware of the emergence of cyberrisks in their respective firms. If the firms do not have proper protection in place to stop hackers from obtaining critical and confidential information related to client matters, the breaches will result in substantial loss of time, resources, productivity, revenue, and perhaps most importantly, credibility. To help law firms and businesses deal with cyberattacks and breaches, U.S. Congress has passed legislation regarding cybersecurity enforcement, the Cybersecurity Enhancement Act of 2014 (S 1353). Additional pending federal legislation includes the Protecting Cyber Networks Act (HR 1560); the National Cybersecurity Protection Advancement Act of 2015 (HR 1731) and the Cybersecurity Information Sharing Act of 2015 (S 754).

Lawyers are holders of clients' personal and legal information and have an ethical duty to protect client data.

Legal technology is constantly undergoing development and change. We went from microfilm and microfiche to CD-ROM, to Lexis and Westlaw, to email and the Internet, to technology-assisted review (TAR) and electronically stored information (ESI), to social medial and now to cybersecurity. These technological advances transformed the law firm workplace. Many litigation paralegals obtained skills in TAR and ESI. Should paralegals learn new skills related to cybersecurity? Raczynski explains what effect he foresees cybersecurity and other technological developments will have on paralegals:

"Paralegals are squarely in the mix with regard to cybersecurity activity for both the protection of client data, but also as targets for hackers. They carry a significant responsibility in assuring that the firm is not compromised. Through their everyday projects paralegals are on the frontlines of major security threats. They must be vigilant in awareness about the software they download and use, sites visited, and links clicked. As law firms become larger targets for hackers because of IP and proprietary information for mergers and acquisitions, there are a host of ways that they are being targeted."

Further, McAndrew answers if he thinks paralegals will spend more time assisting and/or working on cybersecurity projects:

"Yes—in at least two respects. First, the need for cybersecurity-related legal services has exploded seemingly overnight. Many firms are building practices focused on the legal issues created by cybersecurity needs across industry sectors. Working on these issues requires a very high level of legal and technological expertise. More paralegals are likely to begin specializing in cyberlaw, just as more lawyers and firms are beginning to do so. Second, cybersecurity is becoming an important business issue for the law firms themselves. Inadequate cybersecurity is becoming a business disqualifier; good cybersecurity is a business differentiator. Those firms and professionals who can distinguish themselves as knowledgeable and appropriately focused on these issues add additional value to the service they can offer clients. As integral parts of the legal services team, paralegals are likely to spend additional time learning about and working on cybersecurity-related, business development projects."

What is next for the technological-savvy paralegal? Internet of Things? •