Today's GENERAL COUNSEL

Cybersecurity Protocols and ADR

By Diana Didia

Three years ago, a whistleblower hacked into the computer network at the Mossack Foneseca law firm, leaking 11.5 million documents known as the Panama Papers and placing a target squarely on the back of the legal profession. That event proved that law firms, similar to banking/credit card and health-care companies, have what cyberthieves desperately want — a treasure trove of valuable, confidential information.

How has the legal profession adapted to cyber threats in a post-Panama Papers world? Unfortunately, not well enough.

According to the ABA'S 2018 Legal Technology Survey Report, 23 percent of attorney respondents reported that their law firm had experienced a data breach at some time. Although financial services firms and healthcare companies have been swift to adopt new cybersecurity measures, law firms have been much slower to respond to 21st century security challenges.

As reported in Forbes, Mossack Fonseca left itself extremely vulnerable to attacks by maintaining weak, outdated web technology; failing to encrypt emails; using a shared email/server; and going without firewall protections.

If the legal profession, in general, needs to modernize its approach, alternative dispute resolution (ADR) has even more work, given its unique composition. ADR participants — arbitrators, mediators, representatives — come from vastly different organizations, each with its own systems, technologies and procedures. This heightens the risk that something will get into the wrong person's hands. What's more, it's not uncommon for ADR professionals to use a mix of consumer and enterprise software, inviting additional risks. To safeguard sensitive documents, clients should look for ADR firms that have secure document exchange, extensive use of encryption, web-browsing control and advanced intrusion detection, among other systems and controls.

Ultimately, the ADR industry will need to come to terms with several major questions: How will participants with varying degrees of technology and training collaborate without risking sensitive data? What's the ideal process for managing large volumes of material? How should parties handle document retention and deletion? Who has the authority to enforce these measures? The good news is that the legal profession at large is slowly moving in the right direction.

In May 2017, the ABA Standing Committee on Ethics and Professional Responsibility issued guidance to help attorneys address their obligations to safeguard their clients' sensitive information, stating: "A lawyer should understand how their firm's electronic communications are created, where client data resides, and what avenues exist to access that information. Understanding these processes will assist a lawyer in managing the risk of inadvertent or unauthorized disclosure of client-related information."

> To safeguard sensitive documents, clients should look for ADR firms that have effective systems and controls.

A growing number of state bar associations are also clarifying best practices in cybersecurity.

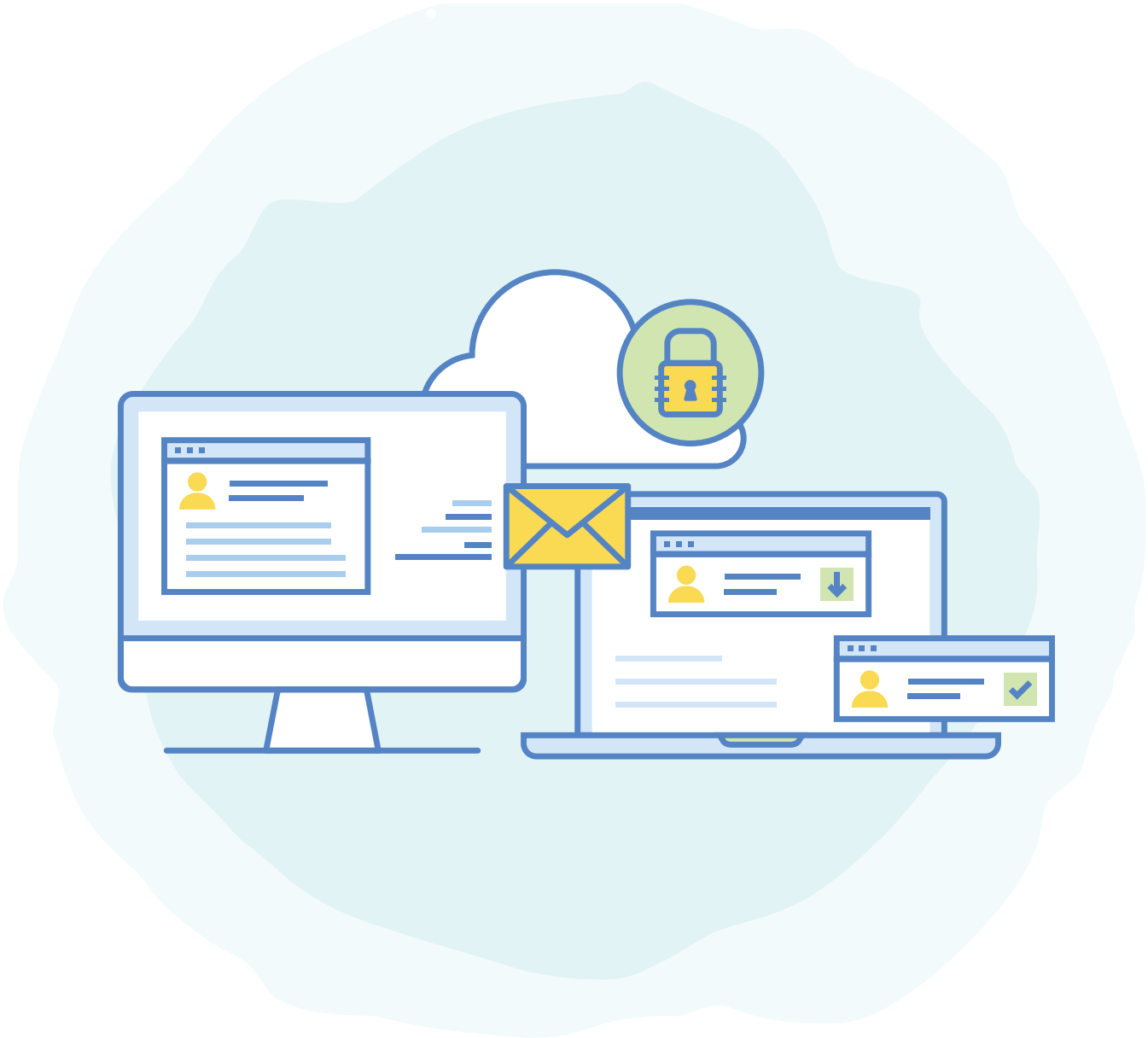
On a global scale, the EU is leading the way. Last year, the General Data Protection Regulation (GDPR) went into effect throughout the EU. The most sweeping set of regulations of its kind, the GDPR provides far-reaching steps businesses need to take to properly safeguard people's personal data and serves as a kind of roadmap for multi-national companies operating in jurisdictions outside of the EU.

In a legal setting, cybersecurity threats can originate from any number of places — from cyber criminals looking to steal intellectual property and other valuable information, to hacktivists like the Panama Papers whistleblower, and disgruntled employees or partners who gain access to data through various means, including malware, ransomware, social engineering and phishing.

There are steps ADR professionals can take to guard against hacks and data breaches, and not all involve installing expensive new systems. Legal professionals can better safeguard sensitive information by using complex passwords and passphrases; tools such as password manager and two-factor authentication; and freeware avoidance. Additionally, they should use full disk encryption on all computers, encrypt files on portable storage devices and never send passwords by the same media as password-protected files. Of course, it's important to remember the basics. Exercise caution before clicking on links or attachments, and if you see something, say something — alert your IT team and colleagues if an email looks out of the ordinary.

In the modern mobile workforce, professionals can conduct business from an airport, a café or, indeed, anywhere. But legal professionals should always remain aware of their surroundings when using public Wi-Fi and mobile hotspots. And they must also take old-fashioned precautions such as using a privacy screen to prevent visual hacking and shredding documents before disposal.

For ADR professionals, a major cybersecurity challenge involves the sharing of large volumes of documents. Although there is no quick fix to this issue, everyone should take a more thoughtful approach to document sharing. Instead of



blindly forwarding emails, professionals should think carefully about what kind of information they must send and receive, pushing back when colleagues offer to share non-essential material or instead use a cloud-storage system.

Although these measures will help lessen the likelihood of a cyberattack or breach, nothing removes the risk altogether. That's why businesses need to have a plan to respond and notify their clients. All 50 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have enacted laws requiring private or government entities to notify individuals of security breaches involving their personal information.

Ultimately, the legal community, ADR in particular, should approach cybersecurity as they do any other important aspect of their work, taking part in training programs; keeping abreast of research, new guidelines and technologies; and empowering themselves to be part of the solution, not the problem. ■

Diana Didia is Senior Vice President and Chief Information Officer at the American Arbitration Association, International Centre for Dispute Resolution.
www.adr.org