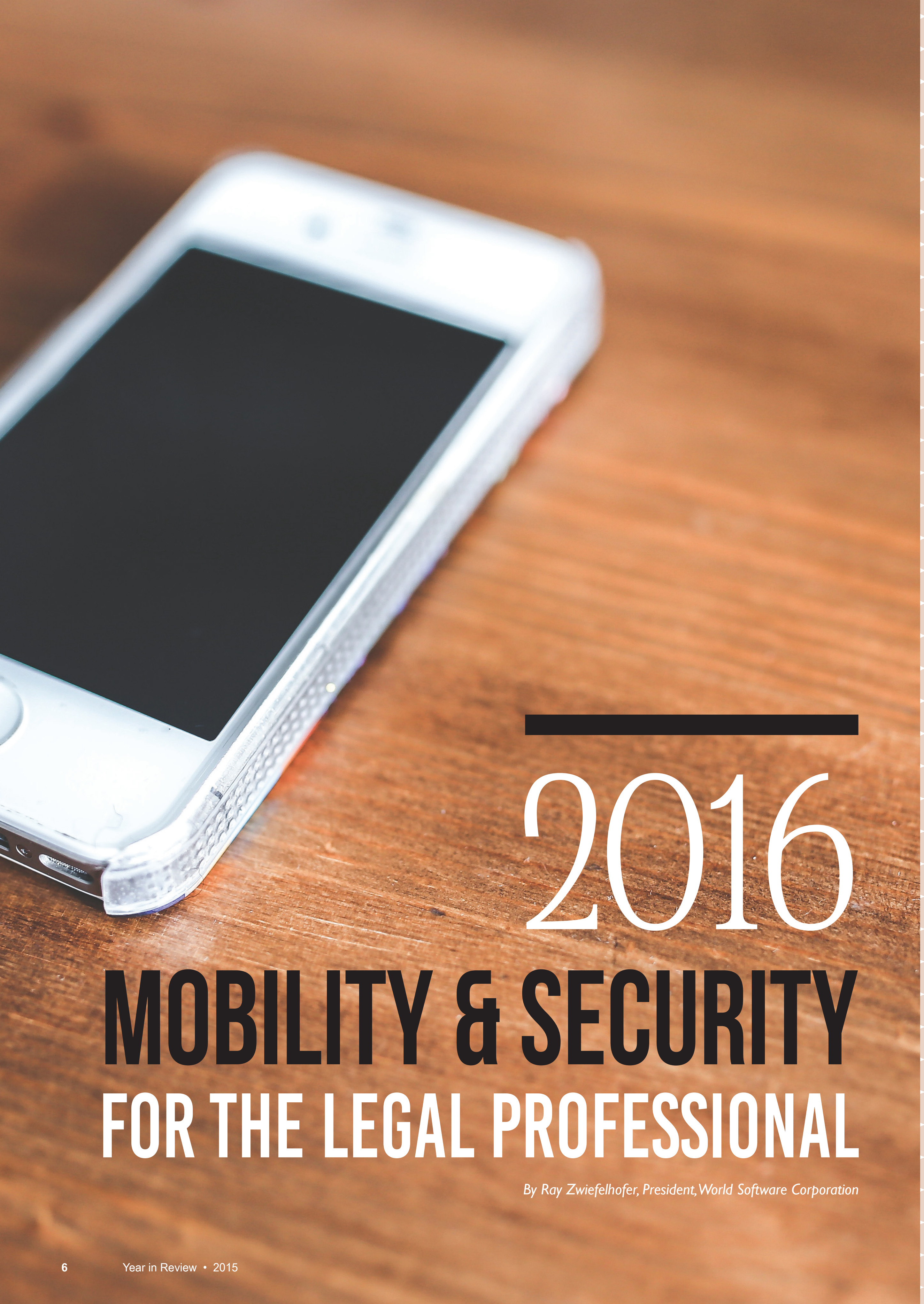

2016 MOBILITY & SECURITY FOR THE LEGAL PROFESSIONAL

By Ray Zwiefelhofer, President, World Software Corporation

As we all know, mobile devices have bombarded the market in the last few years. Mobility usage among legal professionals has skyrocketed. Today's attorneys expect to work from anywhere with any device and have an expectation of reasonable performance. In recent years "Bring Your Own Device" policies have become a norm that has added complexity to the jobs of IT Directors. They have had to engage in a juggling act between allowing attorneys to work with the devices and applications they want while ensuring firm data is secure.

Data security years ago was fairly simple. You bought an appropriate firewall, secured your server, created policies to add an additional layer of security and went about your day. Data protection in today's climate is much more complex and will only increase in intricacy in the coming years. Below are a few items to consider while working on your list to shore up your data protection plan: Data Repository. It is essential to have a good security wrapper around you valuable client data. For smaller firms that may not have in-house expertise, hire an expert IT security firm to assist with the deployment of a next-generation firewall, virus control, perhaps network access control software and other more high tech items.

It is also important to ensure that your DMS integrates tightly with Active Directory to increase security around document stored therein. If your DMS is Worldox, Active Directory integration combined with the built-in Ethical Wall feature provides a powerful tool to increase security on a very granular level. This will ensure there are no internal back doors to content that shouldn't be viewed by everyone. Perhaps the single largest hole in security is the lack of a good password policy. Make sure everyone understands how important it is to use strong and complex passwords, in my opinion this is the weakest link in the chain, a simple common password defeats even the highest level of firewalls and other technology you put into place.

Data Encryption. Data encryption has been around for some time but has really come to the forefront with all of the news of data hacks and leaks. While a complex subject, simply put, data encryption scrambles your content on your hard drive/servers so only valid team members can unscramble it. Cloud data center providers often inherently encrypt by default, however not everyone is ready or wants to go to the Cloud. There are hardware devices or applications that will encrypt your data at rest (while not in use), however they can be pricey for a smaller firm and at times complex. Worldox is finalizing a new product that will include encryption-at-rest technology built into the Worldox Document Management System. In this scenario all of the activity occurs in the background yet you can be confident when you leave the office that even if your server was stolen your content would be unreadable to the thief. Laptops and Portable Drives: More than ever, attorneys are working remotely with their laptops and copying data to external hard drives and thumb drives. Preventing this is probably not possible at most firms. Steps can be taken, however, to make sure the data stored on these devices is encrypted. There is third party software for laptops that will encrypt content on USB devices and Windows 10 even has this capability built in such that you can choose to encrypt a folder so that its contents can only be accessed with a password. Some of the newer portable devices have built in encryption so that a password is required to access the drive. USB portable drives are great tools but they are a big security risk unless precautions are taken.

Mobile Devices. Using a mobile phone or tablet for ad hoc work is also becoming a norm and most software providers have solutions for the mobile attorney. While these devices can be encrypted with a password, the IT team often has minimal control over enforcing passwords, wiping lost devices or controlling business apps on them using native functionality. The Mobile Device Management (MDM) industry has exploded in recent years to meet these ever-changing demands for ways to control content on these devices. Products like Good, Citrix XenMobile and MobileIron allow law firm IT Directors to have better control over their users' smart phones and tablets with tools that enable app deployment and a more granular remote wipe functionality.

Paying attention to the above security tips is not just a good practice. It is essential in securing future clients. We have heard many stories recently where a law firm's client demands certain security protocols relating to how this firm will protect their confidential information. In this new age of mobile computing we all need to increase our knowledge and sense of urgency on protecting the clients' data.

Mr. Zwiefelhofer has over twenty five years' product solution experience within the legal technology market with expertise in AMLAW 250 and Fortune 500. He was a President, CEO and CIO at several software solutions startups and the CTO at a Fortune 500 company. Those companies include Bowne, Imagineer, Equitrac and Diebold. Prior to joining World Software, Ray was the Founder and CEO for nQueue, a global cost recovery company.

Ray Zwiefelhofer, President,
World Software Corporation, Makers of Worldox
ray@worldox.com • 201-444-3228 • www.worldox.com