



**James Clanton** is chief technologist for PropertyBoss Solutions, a provider of property management software solutions that empower your business. He has over twenty-five years experience developing large scale commercial applications with ten years focused on the property management industry. For more information about James or PropertyBoss Solutions, visit [propertyboss.com](http://propertyboss.com) or call James at 864-297-7661 x24.

## Taming the Paper Tiger P3

This is the last of the three part article series on document management. First, we addressed getting started with document management including how to choose a scanner, scanning software, and document/media management software. Then, we covered technical aspects of what types of media to keep and recommendations on the format for stored documents. Now, we will cover infrastructure issues with retaining documents including storage locations, backup, security issues, and web publishing.

### WHERE TO STORE DOCUMENTS

The primary goal of document management is that document organization and control is centralized. Documents should be stored on a network device accessible by all members of your organization.

For many smaller organizations with five or fewer employees, this network device could be one of the desktop computers used by one of your employees. Larger organizations should take advantage of a network server device to store the documents providing better performance and security.

No matter where the documents are located, you must take into account the physical security of the device holding the documents.

### SECURITY OF DOCUMENTS

Our discussion has focused on the needs of the smaller property management company. The goal is to provide an introduction to document management using a simple, understandable method to start with that is low in cost.

Unfortunately, even small companies must understand and provide for security of the documents they manage. You and your company could be held liable for information that is accidentally or purposefully released from your organization that compromises an individual's personal or financial situation.

Many of the documents you manage—including applications, lease agreements, driver's licenses, copies of birth certificates, etc.—contain personal and confidential information from your residents that could be used to steal their identities. This informa-

tion includes both obvious and not-so-obvious items like driver's license numbers, social security numbers, employment information, dates of birth, phone numbers, and so forth.

More companies are now scanning and electronically processing checks. These scanned images, along with credit card receipts and bank draft/credit card authorization forms, are a gold mine for criminals. The ultimate access a thief can have is to obtain both personal information and matching account number information.

The best systems consist of multiple layers of security, each of which must be breached using different information or methods. The more layers you set up, the more secure the information is. Unfortunately, additional layers of security make it more difficult to access the information. The key is to find a balance between robust security and easy access.

The first layer of your security system is the physical security of the hardware containing the documents. With thousands of installations, we too often hear of situations where break-ins occur and all the computers in a building are stolen. We recommend that the physical device containing the documents be in a secure location like a locked interior room. Another physical deterrent is the use of a computer locking device to chain the computer to the desk.

An often overlooked security loophole is the backup device, particularly those devices taken off-site. The backup devices should be both physically secured and password protected.

All computers should be secured with robust passwords to prevent an individual from walking up to a computer and leaving with the information.

You should implement access control over the documents in your document control system. At a minimum, the network directory containing the electronic documents should be limited to specific users and require a different, more secure password than the user's password on their workstation. Review what options you have available with your network administrator.

Specific documents may require more robust security. You should individually evaluate the risk and decide whether these documents should be individually secured when stored in the document management system. These types of documents could include:

- NACHA files containing bank account information
- check scans containing bank account numbers
- draft and credit card authorization forms
- application forms

The method and options to individually secure documents is more complex than can be addressed in this article since most of the document types do not support passwords. A relatively simple approach is to use a zip utility to zip the document and require a password. The difficulty here is whether each document has a separate, unique password or whether all documents use the same password. If you use separate passwords, each password must be stored somewhere securely.

#### **BACK-UP OF DOCUMENTS**

Few thieves have the wherewithal or desire to steal large file cabinets brimming with your company's documents. When stored electronically, a single thief can walk away with your entire company's information and history in a single hand.

We cannot overemphasize the importance of regular back-ups of your documents. You should make at least a weekly back-up of the data and keep one copy off-site.

Always, always keep a current back-up off-site. We have heard too many heart-breaking tales of clients losing both their systems and back-ups from fires and thieves because the back-ups were stored next to the computer.

External hard drives provide the best back-up alternatives because of their large volume and inexpensive price. USB-based external drives holding one terabyte will soon be below \$100. This is a low price for the security of knowing you have a copy of your critical data off-site.

#### **PUBLISHING DOCUMENTS OVER THE WEB**

Publishing your documents for residents and owners to view online can provide an immediate return on your investment. One of the most expensive and often overlooked expenses property managers face are mailing statements and copies of bills to owners.

Our experience working with customers validates the savings that can be achieved. By automating the transfer of documents to the web, including the


owner statement, our clients have eliminated the need for monthly mailings. One client who manages about 800 single-family homes with approximately 500 owners spent a full day with five employees sorting reports, copies of bills, and work orders to mail to clients. They have reported a direct savings of over \$4,000 a month in material, postage and labor costs since making the online switch. In addition, owners and residents are much happier because they can review and print only the documents they are interested in at any time. Phone calls to the property management company have been reduced because owners can see work orders as they are completed.

Two approaches you can use to publish the documents online are opening access to a web server in your office or transferring the documents to an external web server. Both approaches have their own advantages and disadvantages. You also need web-based software installed on the web server to authenticate users and to locate, restrict and list the documents in some logical format for your users.

The advantage of opening your own server to the web for access to the documents is that there is no transfer of large volumes of documents and the subsequent bandwidth requirements to move the documents. The disadvantage of this approach is that you need a very good network/IT support person to ensure your local network has appropriate security. You will also need sufficient Internet bandwidth to serve your residents and owners the documents without objectionable wait times.

The advantage of transferring the documents to an external website is that you do not expose your local network through the web server to the Internet (remember the layered security model discussed earlier). A disadvantage of this approach is that if your property management software provider does not have a built-in transfer capability, you will need additional software to transfer the documents. Sufficient bandwidth is required to transfer the documents, but your upload requirements are less because the transfers can take place over time and at night.

#### **CONCLUSION**

Implementing a sound document management strategy is one of the first steps toward establishing a digital office. If this discussion leads to more questions, feel free to contact me at 864-297-7661 ext. 24 to talk about your objectives. 

**The primary goal of document management is that document organization and control is centralized.**