

The Importance of Archiving Security in a Transparent World

By Terry Wieczorek, President and CEO, DocuLynx, Inc.

In this digital age, the most complex of documents are being transmitted over the Internet and through wireless technologies. While digital technology has vastly improved communications and operating efficiencies in many industries, it also has necessitated the development of entirely new methods of ensuring the security of archived documents. And these security issues come at a time when businesses are under increasing pressure to meet internal governance standards as well as external regulatory requirements.

For example, in the financial industry, leading credit card companies have formed an organization called the PCI (Payment Card Industry) Security Standards Council, which in turn has established the PCI Data Security Standard (PCI DSS), a comprehensive set of requirements designed to ensure that all companies that process, store or transmit credit card information continually maintain a secure environment. There is also the SAS70, or Statement on Auditing Standards #70, which is a document prepared by an independent auditor that reports how well service companies—especially outsourcing companies like data centers and medical billers—handle their clients' information

Implementing an archive solution to meet these complex regulations requires more than just buying a box of software. It requires a team effort to develop procedures that meet the requirements of your enterprise as well as the ever-changing regulations of your industry. The members of this “security team” should consist of resources that can identify the people, technologies, and the processes needed to help businesses comply with and correctly meet the internal and external requirements for document management.

By addressing these requirements, it's important to recognize the three aspects that encompass archiving security: physical security, network security, and data security.

- **Physical Security**

Physical security means allowing only authorized and authenticated personnel to access the archive system, and then to access only those documents they need in order to perform their jobs. Authorized access should include an audit trail for all records transactions; protect physical records and media; support distributed management of records; provide for conversion and migration of records; allow users to access, retrieve, and use records; and facilitate retention and disposition of records throughout the entire

document life cycle. These rules need to be designed for all documents yet be flexible enough to suit different document types in order to meet all current and future compliance regulations. This includes the requirements of SAS70 and PCI DSS compliance.

- **Network Security**

Common solutions to address network security include firewalls and data management zones (DMZs). Firewalls can include both hardware and software, and provide a filtering mechanism that examines incoming and outgoing data, allowing only authorized data to pass through. DMZs are, basically, subnetworks that stand between an organization's most secure internal network and the outside world. A DMZ might include devices like web servers, mail servers, ftp servers, and VoIP servers that communicate directly—or through a firewall—with the public Internet. Any incoming data passed beyond the DMZ into the internal network should be scrutinized by a second, more restrictive firewall.

- **Data Security**

Archived data can also be stored on CD/DVDs, as well as on the Web supported by password-protected access. The data should then be encrypted and compressed for even further protection. In either case, the document must be readable, perhaps even years after the day it was created. Through archiving in a PDF format, this offers both space-saving file compression and platform-independence, allowing documents to be viewed on the desktop in its true fidelity. The ability to have secure remote administrative access, solutions for storage from 30 days to 10 years, and disaster recovery options provides you with even more functionality.

The new security challenges posed by digital technologies are being solved by the need for even more technology. Through a better understanding of what an effective, secure solution entails, you'll be ready to meet the varied and changing spectrum of both internal governance and external regulations.

Terry Wiczorek is president and CEO of DocuLynx, Inc., a leading provider of archive retrieval, electronic distribution, and web presentment solutions for print service providers. For more information about DocuLynx and its Mercury document archive/retrieval software for high volume transactional output, visit www.doculynxinc.com, or contact DocuLynx at info@doculynxinc.com.

###