Communications of the IIMA

2007

The Influence of Government Regulations on Content Management Systems: An Exploratory Study

Douglas A. Goings
Georgia College & State University

Judy J. Johnson
Georgia College & State University

Bryan Marshall
Georgia College & State University

Tanya Goette
Georgia College & State University

The Influence of Government Regulations on Content Management Systems: An Exploratory Study

Douglas A. Goings
Judy J. Johnson
Bryan Marshall
Tanya Goette
Georgia College & State University
Milledgeville, GA
douglas.goings@gcsu.edu

ABSTRACT

The primary focus of this study was to determine why and how small businesses implement content management and to clarify the relationship of content management to regulatory compliance issues presented by the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley Act (SOX). A combination exploratory/narrative case study was used to investigate three organizations that use content management to improve their businesses and guard their businesses against litigation for non-compliance with HIPAA and SOX. Each person interviewed expressed satisfaction with his content management system and each suggested his organization operates more efficiently because of the content management system.

INTRODUCTION

Our information rich world offers tremendous advantages to decision makers, but there are disadvantages too. Information, like any resource, must be managed in order for users to receive maximum benefit. Content management is becoming widely popular, as businesses are beginning to understand the necessity of efficiently handling information, managing compliance, and protecting against litigation. Content management is a broad term for software applications, strategies, processes, and overall management of information. An organization's information includes paper documents, data stored in databases, Web pages, and other information assets, like photographs, blue prints, and sound files. Enterprise content management is used to refer to an organization's entire collection of content management applications and processes.

Purpose for the Study

The primary focus of this study was to determine why and how small businesses implement content management and to clarify the relationship of content management to regulatory compliance issues presented by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Sarbanes-Oxley Act of 2002 (SOX). This study is unique in that it attempts to identify key issues in planning, implementing, and managing content management applications. This paper presents a review of content management, including factors affecting content management growth, features, and benefits. Compliance issues are then summarized to complete the review of content management literature. Following the literature review, an introduction to the case study approach is presented, as well as a description of this study. A narrative of research findings follows the methodology section, and issues and conclusions complete the paper.

CONTENT MANAGEMENT

Bruce Tuemmler (2006), a document management consultant, suggests that systems for managing organizational content be based on a critical review of business processes. End users should identify processes and information needs—not hardware and software consultants and vendors. From such information, an information lifecycle can be

established to manage paper documents, desktop files, and data files, as well as video and audio files. In addition to the type of information required, a lifecycle study should also identify type of capture technology, dissemination requirements, and information storage and retrieval needs. Finally, any information lifecycle study must address disposition and destruction of records that are no longer essential. Mancini (2006b) reports that only four in ten respondents understand the importance of the information lifecycle. In addition to end user requirements of the information lifecycle, Sarbanes-Oxley defines procedures and policies for managing information.

Information Lifecycle

Like crops, animals, and humans, information has a lifecycle. Typically, the lifecycle of information has five phases: creation or receipt, distribution, use, storage, and disposition. A well-designed content management system overlays the information lifecycle transparently. An example of the lifecycle of an e-mail message is as follows:

Phase One. When a writer drafts an e-mail message he or she creates a record, and when a person opens an e-mail message he or she creates a record. With either of these actions, the first phase of the lifecycle is realized. Even a bounced back e-mail could be considered an important message.

Phase Two. Once the e-mail message is prepared and the writer proofreads the message and clicks **Send**, the second phase is realized—the message is now in circulation for the purpose of sharing or disseminating information. It becomes a record, whether it was sent to another organization or remains within the writer's organization.

Phase Three. The value of an e-mail message is realized, and the third phase of the lifecycle begins, when it is used by the intended receiver. Use may generate a decision, an action, or the creation of another document. The record is far from used up, however. Use of an e-mail message may extend to unintended users, called secondary readers.

Phase Four. Once an e-mail message has been used to satisfy its intended purpose, it may be stored by the creator's organization and/or the receiver's organization if it is considered to be useful or essential. Generally, this phase is characterized by activities known as indexing, filing, retrieving, and transferring.

Phase Five. The final phase is known as disposition, where infrequently used records are relocated to inactive storage or off-site storage. Records in phase five must be protected to ensure privacy and confidentiality. When a particular e-mail message is assumed to have permanent value, it can be archived or microfilmed. Once an e-mail is classified as non-essential, it is destroyed.

Content management includes technologies and management principles used in the information lifecycle and involves tracking and managing documents from creation to copyediting and revision to Web posting to storage, disposition, and destruction (Kaplan, 2002). Content management supports businesses by allowing executives and administrative support personnel to share information throughout the entire information lifecycle.

Need for Content Management

Businesses must track information about personnel—some required by governmental agencies. Additionally, businesses track information about products (both in research and development phases and in production), environmental and safety measures and regulatory data, legal information (corporate entity information, partnership information, contracts with suppliers, distributors, and dealers), and information about customers. In addition to computer-based storage, microfilm, optical disc, and even paper technologies are used in preserving or storing information. Archiving content is as important as creating and using information. Management must have such information for making decisions. Businesses need the ability to access information, in its correct version, in order to achieve business goals. Central to this strategy are the tools and technologies used in content management. Information must be managed throughout its lifecycle—from creation to disposition.

Information includes both structured and unstructured content. Structured content typically reside in databases and commonly conform to row/column formats. Such database depositories are highly efficient. Unstructured content, however, which Vignette (2006) estimates as 80 percent of all content, can be anything of value to an organization (e-mail messages, voice mail, images, videos, graphics, Web pages, and software applications).

Content management technologies used with both structured and unstructured content include information capture capabilities or document imaging technologies like scanners, OCR readers, and handprint character recognition equipment (HCR). These older technologies now share content management venues with Web services technologies like XML, where documents are "created" from standard data items held in structured databases. Capture technologies are just the beginning, however. A typical content management venue will also employ tools to "manage" content. Collaboration tools include video conferencing technologies and smart boards so that dispersed users can view and edit the same content.

Content management tools also manage the storage of information. Businesses need to protect the integrity of their information, as it may be needed for decision making and needed to address compliance requirements. Audit trail technologies assist at this point, while repositories help trace check-out/check-in activities and version control. CD-ROM, DVD, optical disc, and RAID (redundant array of independent disks) are included in the technologies used by content management personnel.

It is too simplistic to believe that businesses are driven by costs, especially when it comes to yesterday's information. Businesses are driven by need—efficiency needs and compliance needs. Content management initiatives are also driven by costs—the costs associated with information retrieval and the risk of noncompliance. Howard (2002) suggests an organization could spend up to 25% of its content-related budgets on content management. Businesses go beyond the capital costs of hardware acquisitions, software licenses, and administrative support. Compliance costs, as a part of doing business, are spread over the life of hardware and software. Many businesses have adopted content management technologies without having to justify cost—their thinking, apparently, is that such technologies are a logical investment that must be made and the cost is simply a cost of doing business.

When businesses are small or when managers decide to focus personnel on mission critical activities, they have the option of outsourcing content management activities. Hosted content management specialists may cost less than appropriately scaled in-house content management bureaus. Perhaps proprietary software and platforms are not the answer. When managers decide to implement a content management system, however, they should expect content management to integrate well with other business systems. Information technology (IT) specialists can employ content management services and application modules, which are integrated easily into existing information systems. IT specialists will be able to choose content management tools and service providers that best meet the requirements of unique business processes. Enterprise content management vendors typically offer service interfaces and content formats for most business models. Google provides a list of content management vendors at: http://directory.google.com/ Top/Computers/Software/Internet/Site_Management/Content_Management.

Forces Affecting the Growth of Content Management

Several factors currently affect the growth of content management. Kaplan (2002) speculated that the growth in content management implementations would double between 2001 and 2006. Such growth is associated with management's understanding of the importance of their data and their possible strategic use of data within the organization. Mancini (2006a) offers additional reasons for the growth of content management implementations: continuity of business operations, dissemination of information across the organization, and reduction of litigation risks and costs.

The Web is another force affecting the growth of content management (Arnold, 2003). There is a greater push than ever before to get content written, approved, and published to the Web for dissemination. Arnold reports survey findings that one-fifth of Web site managers (19 percent) indicate they will be involved in content management consolidation projects as they work to manage Web properties.

Regulatory requirements also have affected the growth of content management; one of the leading compliance issues in recent years is passage of the Health Insurance Portability and Accountability Act of 1996 and Sarbanes-Oxley Act of 2002. Ignoring compliance demands could lead to lost business, financial penalties, and criminal charges for chief executives. Organizations can use content management to achieve compliance and manage organizational governance. The following content management technologies are suggested by Jenkins, Köhler, and Shackleton

(2006): document lifecycle management, archiving and records management, enterprise application extensions, e-mail management, rich media and digital asset management, Web content management, and search. Information lifecycle studies, understanding at the broadest level of the capabilities of content management applications, and mastery of compliance issues can help managers understand their roles and responsibilities in the fast growing field of content management.

Features of Content Management Systems

Early in its evolution, content management was viewed separately from document management. Today, with the growth of intranet and private virtual networks, many documents are now available on the Web that were primarily paper based in the past. According to Wilkoff (as cited in Kaplan, 2002), "It's no longer strictly about Web content—it's just as much about managing users who are involved in the content process as it is about managing the content." In order to meet user expectations, content management systems should offer the following capabilities: repository management and version control, with check-out/check-in features; delegated administrative capabilities; search; workflow process control; authoring, template creation, and file transfer processes (Arnold, 2003; Jenkins, Köhler, & Shackleton, 2006; & Kaplan, 2002). In addition to a system's capabilities, enterprise content management vendors frequently provide customer service, training, and continued product development.

To illustrate a feature of an enterprise content management system, consider, once again a typical e-mail message. Essentially an e-mail message is a memorandum that might demonstrate a specific business transaction or provide support facts of a business-related event. As soon as an executive writes and sends an e-mail message (the first phase of the information lifecycle), he or she creates a record. Content management can capture that e-mail message and archive it. This process can be transparent and not affect the executive's productivity. The content management system would then automatically classify the message and store it, while automatically linking it back to the executive's desktop or to an appropriate folder.

Benefits of Content Management

There are obvious benefits to managing information. Having the right information, at the right time, at the lowest possible cost, is a major benefit of having a content management system. Other major benefits include: providing organizational memory, aiding in decision making, preventing litigation, achieving organizational efficiency, and ensuring compliance with state and federal regulatory agency requirements. Smith and McKeen (2003) offer other benefits for content management: simplified forms and work processes, improved navigation through organizational records, reduced materials costs, increased access to information, and improved accuracy and currency of information. Arnold (2003) promotes greater customer satisfaction and reduced employee turnover as benefits of Web site content management.

Business people can realize their own benefits for a fully functional content management system, which could be implemented for their entire organization (enterprise content management). As proposed by Chen (as cited in Newing, 2002), individuals within organizations are empowered to own, create, and maintain content so that information users have an accurate, up-to-date snapshot of the state of the organization, which should improve efficiency and productivity. Better interaction between executives, employees, business partners, and customers is also a benefit of a well-designed content management system, according to Chen. Content management systems also offer collaborative work capabilities, which are managed with check-out/check-in procedures.

Converting existing forms to Web-based versions can make the process of accessing, completing, and submitting "paper work" more efficient. The United States Air Force has implemented such a transfer of paper-based forms to Web-based versions (Bednarz, 2003). The conversion has empowered Air Force personnel, as Chen suggested. As the system matures, says Bednarz, electronic forms will be prefilled from appropriate Air Force databases. As the new system was being planned and implemented, Air Force staff members were able to cut the number of forms used by 10 percent, with another 25 to 30 percent reduction in forms anticipated.

Compliance Issues

With the increased use of computers came restrictions from the government. One portion of HIPAA, for example, was established to increase the privacy and accuracy of electronic medical information. Sarbanes-Oxley mandates compliance with Securities and Exchange Commission (SEC) policies, which require businesses to maintain records for retrieval when required by SEC and officials of the Internal Revenue Service (IRS). Information technology plays an important role in offering content management capabilities for classifying, storing, and disposing of nonessential content. Integration methods, like Web services and XML, have made integration of content easier; but the down side of integrating systems is the explosion of documents being maintained on company computers. Keeping track of this explosion is as daunting as is keeping track of regulatory requirements. For example, there are over 10,000 regulations worldwide that govern management and disposition of electronic content (Open Text, 2006). Businesses headquartered in other countries are nonetheless subject to the provisions of Sarbanes-Oxley if they operate in the United States. Content management can serve to lower litigation risks for foreign-headquartered businesses, because appropriate policies and procedures would be in place for the proper classification, management, and destruction of non-essential records (those, for example, that do **not** document a business-related event or activity).

HIPPA

The Health Insurance Portability and Accountability Act of 1996 (HIPPA) is a set of federally-mandated regulations that were developed to regulate the privacy of patient records in the medical industry. The security rule, which is a subsection of HIPAA, contains policies on keeping electronic health information secure. Most practices use information technology to ensure the security of electronic patient records. The consequences of not complying with the security rule include: (a) a lack of patient record security, (b) potential criminal and civil litigation, and (c) fines for not meeting federally mandated regulations.

The security standard was based on three basic concepts derived from the administrative simplification provisions of HIPAA. First, the standard must be comprehensive and coordinated to address all aspects of security. Second, it must be scalable, so that it can be effectively implemented by covered entities of all types and sizes. Third, it must not be linked to specific technologies, allowing the use of future technology advancements (Department of Health and Human Services, 2003). The medical industry alone is not being subjected to federally mandated regulations; the corporate world, as a whole, is regulated.

Sarbanes-Oxley Act

In the wake of the exploits of Enron and WorldCom accounting scandals, the federal government developed and established a law requiring accountants to provide annual reports on the status of the internal audit controls of organizations to the Public Company Accounting Oversight Board (PCAOB). This law is known as the Sarbanes-Oxley Act of 2002 (SOX). These reports must include, among other things, a detailed audit of the information systems, policies, and procedures taken to secure and authenticate information stored on the systems (U. S. Securities and Exchange Commission [USSEC], 2003). Because of its inability to produce e-mail records for the SEC and New York Stock Exchange, a leading financial services company was fined $7.5 million in 2004 (Open Text, 2006).

Companies have spent millions on acquiring the technology required by the regulation (Flint, 2005). Swartz (2004) believes Sarbanes-Oxley will cost nearly $5.5 billion to implement; and of that amount, $1 billion will be spent on information technology. The Sarbanes-Oxley Act has as its purpose, "To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws and for other purposes." Of particular impact on accounting firms, as well as corporations, are sections 302 and 404 of the Act.

Section 302—Corporate Responsibility for Financial Reports. This section sets up review and certification responsibilities on principal executive officers and principal financial officers in corporations. These high-level officers are required to file periodic reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. § 78m, 78o(d)). This certification must be attached to each quarterly or annual report filed with the

Commission. In essence, corporate officers are being held accountable for any and all untrue statements of material fact, requiring internal controls to be put into place. This is where content management is essential.

Section 404—Management Assessment of Internal Controls. This section mandates the internal controls set up under Section 302, above, be assessed and evaluated. Section 404(b) directly involves auditors. It states, "…each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer." Both Sections 302 and 404 of the Sarbanes-Oxley Act will require cooperation and interface between the corporation and auditors. Records must be maintained by corporations for retrieval when requested by the SEC or IRS. Independent accounting firms will have a like need to retrieve records of and for audits of those firms, mandated by the Act.

In a search of the case law, no court action related to Section 302 (15 U.S.C. 7241) or Section 404 (15 U.S.C.7262) of the Sarbanes-Oxley Act has been found. One of the reasons for this is, it is speculated, is that Section 404, as amended, has an effective date of the first fiscal year after July 15, 2005, for accelerated filers (Sarbanes-Oxley, n.d.). It is early, therefore, for a case to have made its way through the court system based on the foregoing implementation date. Case law flowing from other provisions in the Act seems to center around Section 806 "Protection for employees of publicly traded companies who provide evidence of fraud" (See 18 U.S.C. 73, Sec. 1514A). Under these provisions, a claimant must first file a grievance with the Occupational Safety and Health Administration (OSHA). Few claimants have prevailed at the agency level, and none that have progressed to the final state of the appeal process (review by a federal circuit court of appeals) provided for in OSHA rules and regulations. If after 180 days no action has been taken by the agency, the claimant can file a complaint in federal district court. Of the first 169 complaints filed with OSHA only seven were filed in federal district court (Riordan & Taylor, n.d.).

CASE STUDY APPROACH AND METHODOLOGY

The primary focus of this study was to determine why and how small businesses implement content management and to clarify the relationship of content management to regulatory compliance issues presented by HIPPA and SOX. To that end, researchers used the case study approach for an in-depth study of content management implementations in three businesses. Case studies have been employed in sociological studies in business before, offering understanding of phenomena in a real-life context; and Yin (1994) and Stake (1995) offer interesting insight to the case study approach. Case studies are used to collect data in order to gain a sharper understanding of a subject and what might be important for further, more extensive research later. Researchers who use the case study approach are interested in the actions taken by subjects. Rogers (1978) suggests that case studies describe events within a framework, where problems or issues emerge as the case is analyzed. According to Stake (1995), information generated from case studies often resonates experientially with a broad cross section of readers. Finally, Tellis (1997) proposed the case study as a reliable method for study of information technology issues.

This study is a combination of an exploratory case study and a narrative case study. Exploratory case studies are used to study processes, where researchers wish to explore unfamiliar phenomena before designing and implementing a larger study. Researchers are able to identify questions, develop measurable constructs, and develop measures. Narrative case studies present findings in a narrative, focusing on perceptions, actions, and reactions of subjects. From the analysis of findings, researchers should be able to identify issues for in-depth study.

Sample Selection

This paper presents a case study of content management applications from three perspectives or lenses: a software developer's perspective, a HIPAA compliance officer's perspective, and an executive end-user's perspective. Researchers used professional networks to identify professional who were interested in participating in the study. Interviews were designed to solicit input from these different actors in three different organizations: a Medicare service organization, an oral surgery practice, and a public accounting practice. A key executive in each organization agreed to participate in the study. The selection of such a broad audience was made because researchers wanted to capture data relating to content management and compliance issues from a broad perspective. Participating organizations were located in Virginia, Louisiana, and California, so the broad perspective also encompassed a broad geographic representation of the United States.

Procedures

A principal person in each participating organization was asked a targeted list of questions, which were based on a review of literature on content management, content management implementations, and compliance issues. Researchers were interested in identifying issues that would be important for advanced study of content management.

Targeted Areas

Questions were designed within the areas of security, regulations, management, and content management software. Some issues explored in the area of security were Internet usage policies, levels of access, user roles, monitoring, database security, and backup strategies. In the area of regulatory concerns, individuals were encouraged to discuss the privacy of patient data, conformance to standards, changes in regulations, ensuring compliance, Medicaid, and the matching of software to the regulations.

Management issues addressed included user acceptance and training, information bottlenecks, workflow studies, employee processes and productivity enhancements, cost reduction, and return on investment. Issues within the area of content management software included managing digital images, document retention and retrieval, version control, hardcopy locations, and auditing.

By targeting these areas in the discussions with the interviewees, researchers felt they could get a grasp of key issues prevalent in the implementation and use of content management software. The key issues are presented below in the findings.

FINDINGS

The following narrative of research findings is divided into three parts or perspectives: software developer, HIPAA compliance officer, and executive end-user.

Software Developer's Perspective

The first business (Company A) to participate in the study was a publicly traded software development company. Currently serving ten states, its main function is to regulate and manage patient billing between Medicaid and hospitals. The person interviewed is a private consultant who is responsible for the development of the company's in-house, organization-wide content management system. The purpose of the content management system is to maintain vital documents throughout the organization and across the ten client states. Both HIPAA and SOX regulations apply, and the company and its software are constantly being monitored.

How are government regulations monitored? Company A has a regulatory department, staffed with lawyers and information technology personnel, that is responsible for monitoring regulatory agencies, disseminating changes in regulations, and testing the content management system to ensure the company is in compliance. This department is the "internal audit" entity that has the main responsibility to monitor compliance with government regulations. The biggest challenge personnel faced in developing their system was deciding on an appropriate level of access.

To whom does the company report? There are no reports that Company A is required to send to any government agency. Their content management system reports user access to certain data. This report, or audit trail, can be made available at any time to internal or external auditors.

How important were government regulations when the application was developed? The content management system at Company A was developed from the ground up, with security and audit subsystems specifically designed for their implementation. Currently, people spend about 10 percent of their time addressing security and auditing issues based on government standards. The entire system was designed and coded by outside programmers. As

modifications have been needed, due to changes in regulations at the federal level, modifications were coded in-house.

What is the usage of the content management application? Six financial applications are currently in use at Company A. These systems interface with the content management system. The content management system is used daily to audit billings and payments. It provides needed checks and balances, rather than being a payment application.

How was the content management application developed? Company A's content management system was created in three phases: development, quality assurance, and production. The development phase is where the system is maintained and information technology personnel troubleshoot to reduce chances for failure. This phase is also where the content management system is enhanced and modified to meet changing regulations.

The quality assurance phase is where the system is tested and is where user acceptance is measured. In the production phase, users access the system. There is no access to source code and no direct access to the data tables. Both vertical and horizontal queries can be performed on data due to strict HIPAA requirements. HIPAA strictly limits access to sensitive medical information to those who need it for patient care. For example, data for a patient who is HIV positive cannot be shared with those outside the patient-care relationship.

What are the security issues for the company? There is a great deal of security for the relational database. Although the company's relational database is less secure than older systems, due to the nature of mainframe computing, its functionality is necessary. In order to maintain a neutral non-proprietary environment, Company A did not purchase a specific content management application. All security, therefore, must be done at the application level instead of the database level. Without database security, SQL commands could be used to access the entire database.

The content management system limits access to the database only as long as users access the database through the content management system. The database does not maintain any level of security on its own. Company A operates on the assumption that outsiders will assume they cannot access the database from outside the content management system. Company A does not report itself as a HIPAA violator because there is no government agency that polices databases and no clear way for Company A to be forced to maintain a higher level of security.

HIPAA Compliance Officer's Perspective

The second business (Company B) to participate in the study was a small oral surgery practice located in southern California. The person interviewed is the HIPAA compliance officer, who was hired specifically to deal with the HIPAA regulations. Company B's full-time staff is made up of six nurses, four front office employees, and one doctor.

In order to conform to HIPPA regulations, Company B began its search for an up-to-date content management system in 1996. Due to strict HIPPA requirements, the system had to provide added security to ensure the privacy of patient data. To that end, the system had to establish clear boundaries between front office employees and the doctor and nurses. For example, the nurses did not need to see billing information, and the front office employees did not need to see a patient's blood pressure records.

What were the problems in selecting a content management system? A few bottlenecks were discovered; the biggest was a lack of product information. At the time Company B started planning its content management system, it was difficult to know about different applications. The HIPPA compliance officer relied heavily on information obtained at medical conferences and from content management software vendors.

The content management software purchased for Company B was specifically written for oral surgeons and incorporates functionality to address HIPAA standards. Because the shift from the paper-based system to the electronic-based system was so drastic, a workflow study was not undertaken. The software included a robust relational database housed on a local server. Each workstation is connected to the server via a front end application. The front end application has built-in security to ensure the privacy of patient records. Along with being HIPAA compliant, the software also has the ability to manage digital images, like photographs and x-rays; e-mail; Word

documents; and employee time sheets. It also has a built-in patient management system, which handles billing, insurance, and patient records.

What services did the vendor provide? As part of the content management software purchase, the vendor went to California to install the system. The vendor also provided several days of training for the front office personnel and nurses. No follow-up training was provided, however. This has been problematic since approximately one half of the current staff of office personnel and nurses were not employed when the training was provided. Additional modules were purchased, including a touch screen module, which is used in the operating rooms.

What problems were experienced in the implementation phase? Another bottleneck appeared during the implementation phase. After the software purchase, a significant computer hardware upgrade became necessary before the application could be installed. New server hardware was purchased, and several workstations had to be replaced.

What was the driving force behind the new system? HIPAA was the driving force for implementing the content management system. Because of HIPAA regulations, other policies were also incorporated into the way the business functions, which also increases efficiency. These policies include a restrictive Internet usage policy. Only two front office employees are allowed to access the Internet to complete insurance inquiries, which are only available online.

What about computer security? Because of the server-workstation relationship, Company B has a high need for security. If the server is compromised due to a lack of security on a workstation, the business could be in violation of the HIPAA security rule, not to mention the down time of getting the server back up. Soon Company B will be moving to a third party firewall, which does deep packet inspection, a form of computer network-packet filtering. This will allow for a more lenient Internet access policy in the future.

Did the new system meet the requirements of HIPAA regulations? The major "pain" point faced in planning and implementing Company B's content management implementation was whether the software would satisfy federal standards. Anxiety also surfaced concerning the implementation of newer versions after holes were fixed and patched. One benefit of going with a software vendor is that the regulatory responsibility ultimately shifts to the vendor. HIPAA requires companies to perform reasonable due diligence, and purchasing content management systems has been deemed diligent enough.

Were costs reduced with the content management system? Overall, patients seem to be impressed with the system. They seem to trust the doctor more because he uses cutting edge technology in his practice. Cost reduction, however, was not a major outcome of the content management implementation. Since the business is small, no strong need was in place for implementation to ensure a particular return on investment (RIO). In the future, cost-justification for upgrades to the system is likely to be based on intangibles, like "just the cost of doing business or the cost of being government compliant."

Executive End-User's Perspective

The third business (Company C) to participate in study was an accounting firm in southwestern Louisiana. One of the largest accounting firms in the city, Company C is staffed with certified public accountants, other degreed professionals, and degreed clerical and administrative support personnel. The person interviewed is a managing director. People in Company C specialize in various functions, such as improving clients' profitability through strategic planning; developing and implementing financial plans; serving as expert witnesses in litigation; preparing information for audits and compiled financial statements; and preparing plans for taxes affecting individuals, businesses, trusts, and estates.

How are changes in legislative or regulatory action tracked in the organization? Changes in legislation and compliance regulations are received by e-mail from Taxnews, a tax service provider. Auditing updates are obtained through e-mail from an organization that acts as a clearinghouse, and members of the staff attend seminars and conferences in order to keep current.

Did regulatory requirements prompt implement of the content management system? Regulatory requirements did not drive the implementation of the paperless office application (purchased from CCH, an enterprise digital solution vendor). Audit files must be maintained regardless of the system, as well as regulatory requirement reports and peer review documents. Reporting is simply the result of standards. The paperless office application, part the practice-wide content management system, has facilitated the storage of required reports, however. Document version control has also been enhanced. Individual directors, accountants, and staff members store their own e-mails in the paperless system; they are not, however, required to do so.

How has the content management system impacted reporting requirements? Implementation of the content management components was not prompted by reporting requirements. Submitting paperwork to outside agencies is easier with the system, however. Copies of documents sent to banks, for example, are now e-mailed in PDF format. Also, remote access is now possible, as all documents created since the implementation of the system are available through the Internet worldwide. Security is maintained through sophisticated firewalls and content management administrative role controls, where access to different documents is restricted to individuals at different levels within the organization.

How has the content management system impacted document generation? There was some impact on document generation procedures. Executive (directors, accountants, and other degreed professionals) are more likely to draft their own documents since they have direct access to files through their desktops. This empowering of top-level personnel enhances productivity. Work flow did slow temporarily, however, as personnel took time for training and for becoming familiar with the new system. Enhancements will occur as current paperwork is rolled forward next year, with key information like names, addresses, and other identification information being maintained while financial data from last year is dropped out.

How has the content management system impacted document retention and retrieval? There was signification impact on document retention and retrieval with the new system. For example, now the person responsible for purging non-essential files and out-of-date files can do so with the click of a button. Electronic documents are typically classified as essential, temporary, and non-essential and are stored in binders (folders); and a single click, for example, can purge all audit files from 2006 for all clients automatically, assuming they are no longer needed.

Were anticipated reporting, tracking, and availability expectations realized? Transmission time has decreased because all records are now electronic; this has been a signification benefit of the new system. The entire office functions better with the new system once the training kicked in. The vendor provided a week of training and the learning curve was considerable. Now the practice can do more for clients and everyone is more productive. Directors and other professionals no longer need to have administrative personnel access documents—everyone has instant access to all records on his or her desktop. There is a real since of empowerment. Instead of, "Hold on, let me get that file," clients now hear, "Give me a minute to access the file."

How are modifications to the content management system handled? The vendor makes changes to the software, and updates are accessed as they are available, assuming the practice wishes to purchase them. Two people, who were quick to learn the system, help others when problems arise. No one in the practice is permitted to modify system code. The vendor provides telephone support when users need expert help.

What compliance issues impact the organization and the content management system? Audit documents must be maintained in hardcopy form, as must letters from attorneys. Letters of engagement must also be kept in hardcopy form. This has always been the case and has not changed with the implementation of the paperless office system. The practice's directors are responsible for oversight of the system and for compliance.

Do financial and other operating systems interface with the content management system? The new system interfaces with Excel and trial balance software. This is an important productivity feature, and version control allows sufficient check-out/check-in procedures to allow collaborative work.

ISSUES OF CONCERN

Analysis of the data from case study interviews revealed significant issues to guide future content management research. Issues were grouped into categories: management concerns, procedural concerns, regulatory concerns, and security concerns. Content management is being used in the companies who took part in the case study to reduce costs and to empower executives.

Concerns for management include the impact of content management on organizations and desired return on investment, user acceptance, and training. How do organizations defend organizational-wide implementation of content management systems? What ROI do organizations require, if any? What role does employee training play in the decision to implement a particular content management system from one vendor or another? Additionally, organizations need to understand the likelihood that technological and workflow bottlenecks could hinder or slow implementation of an appropriate content management system. Workflow studies are an important part of a well-designed content management system and should not be overlooked, as was the case of Company B in this study.

Procedural issues that surfaced included document retention and retrieval concerns, which could have been discovered during a workflow study. Version control was also mentioned as an important part of content management, as was the case with Company C. Check-out and check-in capabilities, along with administrative access are critical to personnel in the case study businesses. Other capabilities of a well-designed content management system must address the range of documents, files, and images used in contemporary business. Content management is more than handling digital images. What do businesses do with exiting paper files and office-site file depositories? Finally, this study identified audit and paper-trail requirements that must be addressed with any content management system.

Following the interviews, top regulatory issues, including the HIPAA security rule (privacy of patient data) and conformity to HIPAA standards, were recognized—this was clear from Company A. Organizations are aware that monitoring of regulatory changes is important, while concerns about digital content must include conformity to government regulations for audit purposes. The strongest areas uncovered for monitoring government auditing purposes involve Medicaid and IRS regulations.

The study revealed important security issues, which include the role of Internet usage policies and appropriate level of access to online information. Monitoring and user roles are administrative duties that must also be considered with database security and backup strategies.

CONCLUSIONS

This study presents an overview of issues of concern in content management, especially when dealing with governmental regulations. Future research may include a more comprehensive study of each type of firm to see if these issues are widespread.

Content management systems are important to business. Companies must be sure that the content management systems they purchase are capable of handling whatever regulations are imposed. Companies must also be sure that proper backup and maintenance is performed to keep content management systems functioning properly. In each case, the persons interviewed expressed satisfaction with his content management implementation; and each person believes the business will continue to experience benefits associated with well-managed information.

REFERENCES

Arnold, S. E. (2003). Content management's new realities. *Online, 27* (1), 36-40.

Bednarz, A. (2003). Air Force streamlines electronic paperwork. *Network World*. Retrieved April 26, 2007, from http://www.networkworld.com/news/2003/0113airforce.html.

Department of Health and Human Services. (2003). Security standards final rule: 45 CFR Parts 160, 162, and 164. *Federal Register, 68* (34).

Flint, A. J. (2005). Solutions to corruption in the auditing profession. *Review of Human Factor Studies: Special Edition, 11(*1), 113-129.

Howard, J. (2002). Finding the ROI in content management. Retrieved April 26, 2007, from http://www.cmswatch.com/Feature/67.

Jenkins, T., Köhler, W., & Shackleton, J. (2006). Enterprise content management methods: What you need to know. Waterloo, ON: Open Text Corporation.

Kaplan, S. (2002). Cool tool. *CIO Magazine*. Retrieved April 26, 2007, from http://www.cio.com.au/index.php/id;696052489;fp;;fpid;;pf;1.

Mancini, J. (2006a). ECM technologies are moving to the mainstream. Retrieved August 30, 2006, from http://outputlinks.com/html/General/ECM_051606.shtml

Mancini, J. (2006b). The role of ECM in storage decisions: The why, what, and how of storing business critical information. Silver Spring, MD: AIIM.

Newing, R. (2002). A key facility for making better business decisions: The bigger picture, *Financial Times* (London). Retrieved April 26, 2007, from http://www.infuture.pro/Documents/London%20Times%20Article.pdf

Open Text Corporation. (2006, February). Litigation readiness: The best offense is a great defense. Waterloo, ON: Author.

Riordan, R. P., & Taylor, L. D. (n.d.). Sarbanes-Oxley whistleblower claims: Fast start or fizzle? Retrieved September 15, 2006, from http://www.lawmemo.com/articles/sox.htm

Rogers, L. A. (1978). Business analysis for marketing managers. London: William Heinemann, Ltd.

Sarbanes-Oxley Act: Section 404 effective dates. (n.d.). Retrieved September 15, 2006, from http://www.sox-online.com/basics_404_dates.html

Sarbanes-Oxley Act of 2002, 15 U.S.C. § 7201.

Securities Exchange Act of 1939, 15 U.S.C. § 77a et seq.

Smith, H. A., & McKeen, J. D. (2003). Developments in practice VIII: Enterprise content management, *Communications of the Association for Information Systems, 11*, 647-659.

Stake, R. (1995). The art of case research. Newbury Park, CA: Sage.

Swartz, N. (2004). Compliance costs rising. *The Information Management Journal, 38* (6), 6.

Tellis, W. (1997, September). Application of a case study methodology. *The Qualitative Report, 3* (3). Retrieved August 23, 2006, from http://www.nova.edu/ssss/QR/QR3-2/ tellis2.html

Tuemmler, B. (2006). Basics of successful document management: New to document management? Top 10 things to do to get your DM system started right. Retrieved August 30, 2006, from http://www.aiim.org/article-docrep.asp?ID=31181

U.S. Securities and Exchange Commission. (2003, April 14). Final rule: Management's reports on internal control over financial reporting and certification of disclosure in exchange act periodic reports. Retrieved December 21, 2006, from http://www.sec.gov/rules/final/33-8238.htm

Vignette. (2006). Transforming your content from a liability to an asset. Austin, TX.

Yin, R. (1994). Case study research: Design and method (2nd ed.). Thousand Oaks, CA: Sage.