White Paper

Office Technology & Services

April 2013

Document Security and Compliance

Enterprise Challenges and Opportunities

Comments or Questions?

InfoTrends
A Questex Company

Table of Contents

List of Figures

Introduction

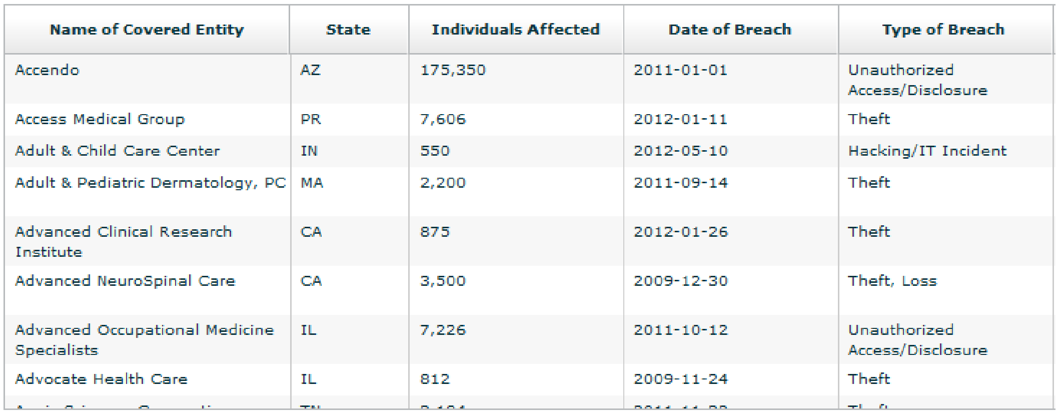
In today's age of interconnectivity, the potential for security breaches has multiplied. Not only has it become easier for outsiders to infiltrate company IT infrastructures, but it has also become easier for people within the organization to commit a privacy breach (either on purpose or accidentally). While many companies have responded to the first type of problem by installing network firewalls, anti-malware software, and intrusion detection/prevention systems, the area of internal security threats—particularly those related to document security— has largely been ignored.

Organizations' awareness of potential security problems that exist, or familiarity with the solutions that can prevent these types of breaches, varies from company to company. Within this white paper, InfoTrends will highlight the prevalence of document-related security and compliance breaches, provide examples of vulnerable elements of the document infrastructure (in the general office environment and in a variety of key vertical markets), and discuss proven solutions for addressing these risks.

Prevalence of Document-Related Security Breaches

According to a recent IT research study[1], 90% of U.S. organizations experienced leakage or loss of sensitive or confidential documents over the past 12-month period. The U.S. Department of Health and Human Services, meanwhile, lists over 500 health information security breaches that have affected 500 or more individuals over the last several years.

Figure 1: Partial List of More than 500 Health Information Security Breaches

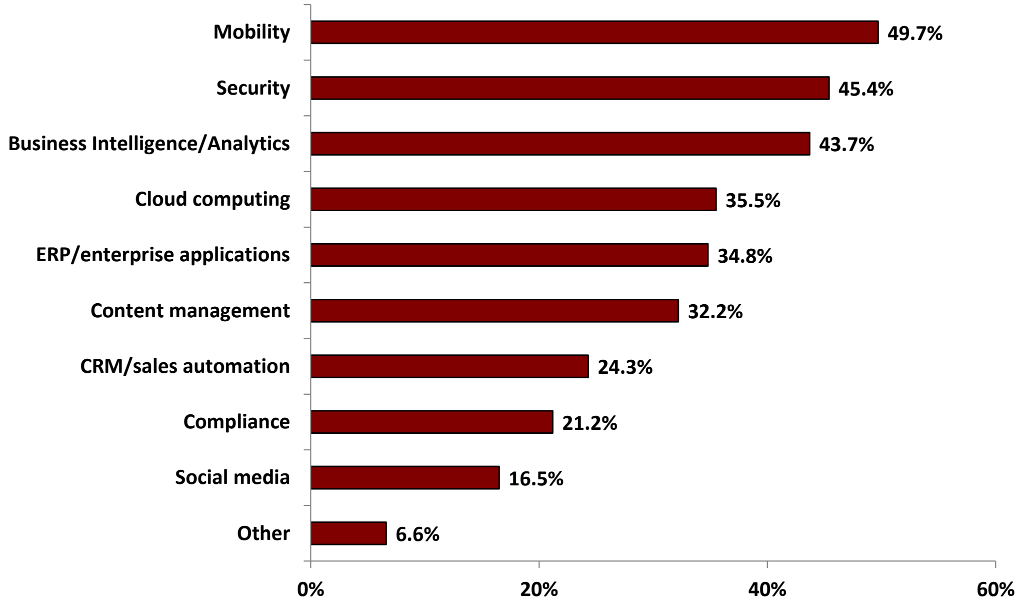


Name of Covered Entity	State	Individuals Affected	Date of Breach	Type of Breach
Accendo	AZ	175,350	2011-01-01	Unauthorized Access/Disclosure
Access Medical Group	PR	7,606	2012-01-11	Theft
Adult & Child Care Center	IN	550	2012-05-10	Hacking/IT Incident
Adult & Pediatric Dermatology, PC	MA	2,200	2011-09-14	Theft
Advanced Clinical Research Institute	CA	875	2012-01-26	Theft
Advanced NeuroSpinal Care	CA	3,500	2009-12-30	Theft, Loss
Advanced Occupational Medicine Specialists	IL	7,226	2011-10-12	Unauthorized Access/Disclosure
Advocate Health Care	IL	812	2009-11-24	Theft

[1] The study is titled *2012 Confidential Documents at Risk Study*; it was conducted by the Ponemon Institute.

Given the prevalence of document-related security breaches in the workplace, in addition to the potential costs associated with these breaches, it is not surprising that many companies consider security a top IT initiative. In fact, InfoTrends' research has identified security as one of two principal IT initiatives among U.S. businesses.

Figure 2: Top IT Initiatives



N = 487

Source: *Mobile Business Process Initiatives and Obstacles*, InfoTrends 2011

The fact that mobility was also a top response does not come as a surprise, as issues around security and mobility are very much intertwined. While only 21% of respondents identified compliance as a top IT initiative, it is clear this initiative is also very much tied to security.

In addition, vertical-specific government legislation has created an increased need for compliance. The Gramm-Leach-Bliley Act, for example, requires financial institutions to implement the appropriate technical, physical, and administrative safeguards to preserve the privacy of customer information.

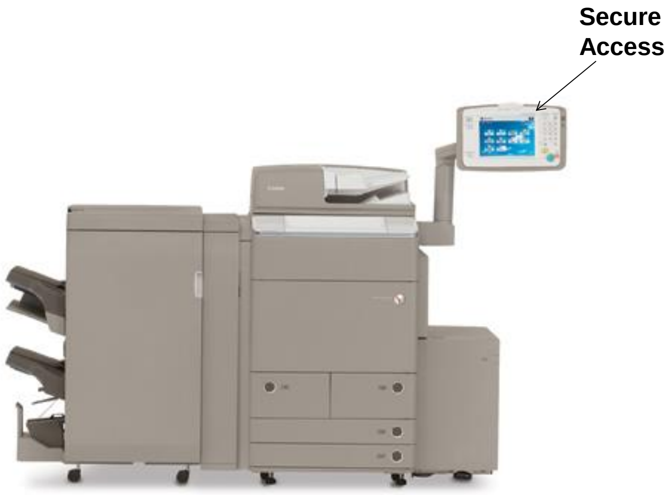
Document-related Security Threats and Opportunities

There are many ways that confidential documents and data can get into the wrong hands. While many people are aware of threats related to e-mail and computer hard drives, they may not be so aware of potential dangers tied to their printers and multifunctional peripherals (MFPs) (i.e., those that print, copy, scan, fax)—two key elements of the document infrastructure.

Exposed Hardcopy Documents

One risk (that has existed for some time) is that of employees forgetting to pick up their documents in the printer/MFP output tray, leaving them exposed to anyone who happens to walk by. This issue can be addressed through secure access solutions that only release documents after proper authentication (via password, security card, PIN code). Most of these solutions also provide an audit trail of who printed what and where, adding another layer of security.

Figure 3: MFP with Secure Access



Exposed Digital Documents

Digitized documents can also be exposed. In fact, many printers and MFPs have hard disk drives that log and store documents, user authentication data, and other sensitive information[2]. Sometimes the data is stored temporarily to help speed up a task, while other times it is stored indefinitely. Users can protect these documents and data through encrypting the hard disk drive.

There is also the option of disk image overwrite, which can automatically remove data once a job is complete—either on a scheduled basis or as needed. Additionally, network security protocols, such as Transport Layer Security, can protect data that is in transit.

Insufficient User Restrictions

As mentioned above, organizations can implement secure access solutions that require password, PIN, or card authentication. To further enhance security, they can restrict the access privilege of certain users to ensure they are only using the features that are required for their job. For example, certain users may not have access to faxed documents, while other users may not be able to access scanned files. In addition, companies can limit who can transmit stored documents and where these documents can be sent. All of these measures, as well as the associated audit trail, can help companies achieve their security and compliance goals.

[2] There are a number of ways the documents can be transmitted to the hard drive, including through a print, copy, fax, or scan job.

Uncontrolled Print Environment

While organizations can implement any of the security solutions mentioned above, the ideal solution is a comprehensive approach that enables companies to gain full control of the print environment. A number of vendors offer print management software, for example, that tracks all MFP activity across the company, enforces pre-set print and copy quotas to ensure proper usage and prevent waste, and improves security by releasing documents only when users are at the device. Other common features of a comprehensive print management solution consist of a PIN or swipe-card log-in system, the ability to re-direct print jobs to the most cost-efficient printer, and the option to allocate costs to particular departments or offices. While print management solutions are largely designed to increase document security, it is clear they also provide cost, environmental, and convenience benefits.

Unsecured Scan Infrastructure

With many organizations focused on digitizing and storing documents, there is a heightened need to ensure these documents are protected through every stage of the scanning process. The best security solution safeguards critical business data from the moment the MFP or scanner is accessed to the moment the document arrives at the appropriate destination—including *all* steps in between. Organizations looking for this level of protection are encouraged to pay special attention to solutions incorporating user authentication, document encryption, secure deletion of temporary files, scanned document access restrictions, and activity logging. Similar to print management solutions, document capture solutions can be integrated with cost recovery systems.

Threats and Opportunities by Industry

Every industry has unique challenges and requirements when it comes to safeguarding company documents and data. This section addresses industries with a relatively high level of confidential data/documents as well as compliance obligations. InfoTrends has used its recent *Business Process Automation Opportunities for Vertical Markets* study (2012), which covers the education, financial services, insurance, healthcare, and legal industries, to provide insight into these vertical markets.

Education

According to InfoTrends' *Business Process Automation Opportunities for Vertical Markets* study, around 55% of K-12 teachers identify improving student privacy as an important goal for their organization.

This concern for privacy is to be expected, given federal laws like the Family Educational Rights and Privacy Act (FERPA) that prevent federally funded schools from releasing information from students' education records without written permission from a parent or "eligible" student[3]. Penalties for noncompliance include loss of federal funds, as well as criminal and/or civil penalties for the person who disclosed the information.

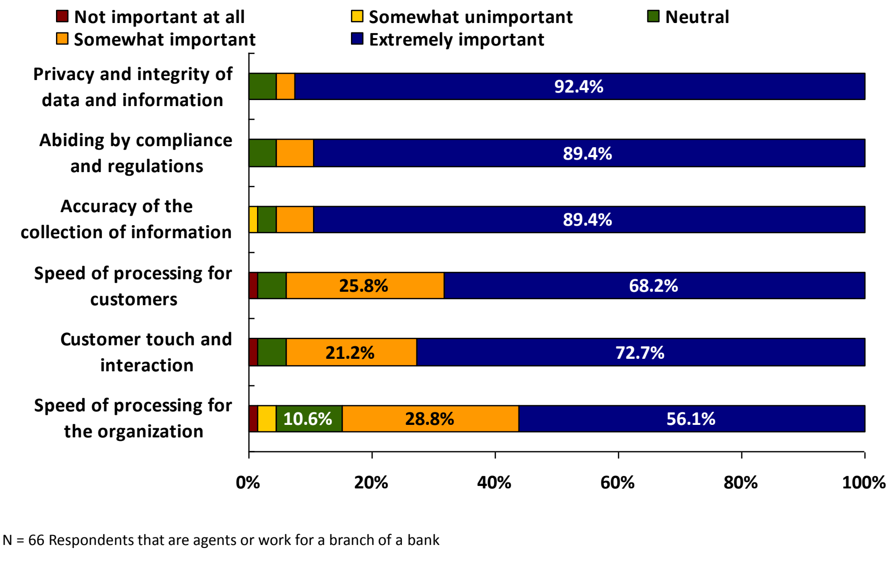
To ensure information such as grades, enrollment details, and bills are protected, grade schools, high schools, and universities may want to consider the solutions mentioned above. In addition, they can password-protect PDF documents to guarantee the information is not accessed or altered by third-parties.

Financial Services

The financial services industry is one of the most highly regulated industries due to the private nature of customer finances. As mentioned earlier, the Gramm-Leach-Bliley Act requires financial institutions, such as banks and insurance companies, to implement the appropriate technical, physical, and administrative safeguards to maintain the privacy of customer information; other similar regulations are in place, as well.

Financial services employees are well aware of the need to protect sensitive data. InfoTrends research shows that an overwhelming 92% of bank employees believe "privacy and integrity of data and information" is an extremely important goal for their organization. Similarly, 89% of these individuals consider "compliance and regulations" to be an extremely important goal.

Figure 4: For your organization, how would you rate the importance for each of the following goals and objectives?



Source: *Business Process Automation Opportunities for Vertical Markets*, InfoTrends 2012

[3] An "eligible" student is one who has reached the age of 18 or attends a school beyond the high school level.

Insurance agents surveyed by InfoTrends voiced similar concerns. One way for banks, insurance companies, and other financial institutions to protect customer data is through "print on demand." This term is used to describe the act of retrieving and printing documents via the printer or MFP touch screen. When the documents are accessed from a secure network folder, this method can be preferable to sending print jobs from a desktop computer. A number of risks are reduced, including the possibility of the document being seen on the desktop computer, the chance of it being intercepted during transmission, and the likelihood of it being left on the print/MFP output tray.

Healthcare

The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. law that requires healthcare organizations to protect private medical information. Under this law, medical institutions cannot release information related to health status, the administration of healthcare, or payment for healthcare that can be linked with a particular person. HIPAA violations can result in costly fines (the maximum annual penalty per violation is $1.5 million), imprisonment, and exclusion from participation in Medicare.

Healthcare institutions appear to be taking regulations like HIPAA very seriously. In fact, 95% of medical practitioners surveyed by InfoTrends said "compliance with regulations" is an extremely important goal for their organization. Furthermore, "confidentially of patient data" was an extremely important goal for 94% of respondents.

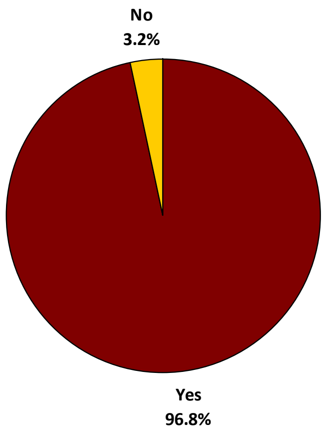
The October 2014 mandate for the adoption of an Electronic Medical Records (EMR) system has resulted in a significant increase in scanning activity. Given the privacy issues discussed above, it is crucial that healthcare organizations implement the appropriate MFP and network protections to guarantee that only authorized personnel are accessing the scanned files. There are also ways to restrict access to specific information, trace unauthorized accesses, and encrypt e-mail sent from the MFP.

Legal

A key concept in the U.S. legal industry is that of "attorney-client privilege," where certain communications between a client and their lawyer are considered confidential. While client-attorney privilege laws can differ from state to state, the underlying assumption as that information passed between the two parties is protected. With this in mind, it is not surprising that 90% of law firm employees surveyed by InfoTrends identified "privacy and integrity of information" as an extremely important goal for their organization, and 84% view "compliance with regulations" as extremely important, as well.

Given that many law firms continue to be highly dependent on paper-based processes, including printing and faxing, they may want to consider a secure print/fax release system, or a fax routing system that directs incoming fax messages to the intended recipient's e-mail inbox or network folder.

Figure 5: Do you still maintain a hardcopy file/files of relevant case paperwork?



N = 62 Respondents that work for law firms

Source: *Business Process Automation Opportunities for Vertical Markets*, InfoTrends 2012

InfoTrends' Opinion

As more and more documents become digitized, the possibility of these documents being transmitted to unauthorized individuals has increased—especially in industries where regulatory compliance is of paramount importance. While this document explores a number of highly-regulated verticals, including education, financial services, healthcare, and legal, the truth is that a wider spectrum of verticals (including government, retail, and manufacturing) could benefit from improved document and data security.

It is important for organizations to consider the entire document infrastructure when deciding on the appropriate security plan. This includes their hardcopy document storage systems, their printers and multifunctional devices, and their digital document storage systems (including network folders, cloud services, vertical-specific databases, and mobile devices). If all of these elements of the business are not protected, there is a very real possibility documents will end up in the wrong hands—potentially resulting in exorbitant fees, angry clients, or even criminal charges.

This material is prepared specifically for clients of InfoTrends, Inc. The opinions expressed represent our interpretation and analysis of information generally available to the public or released by responsible individuals in the subject companies. We believe that the sources of information on which our material is based are reliable and we have applied our best professional judgment to the data obtained.