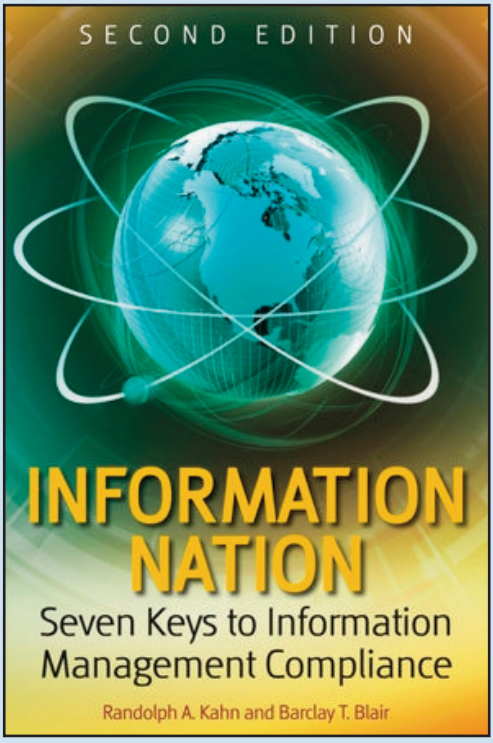
INFORMATION NATION

Chapter 9: Information Management Policies



By Randolph A. Kahn and Barclay T. Blair

9 Information Management Policy Issues

A compliant Information Management program must address myriad policy issues. The intention of this chapter is not, however, to provide a catalogue of those issues. Rather, this chapter focuses on a selection of issues that are worthy of specific focus because they commonly seem to cause problems for organizations, either because of their complexity or their relative newness.

Issue #1: Electronic Discovery

> *In this…era of widely publicized evidence destruction by document shredding, it is well to remind litigants that such conduct will not be tolerated in judicial proceedings. Destruction of evidence cannot be countenanced in a justice system whose goal is to find the truth through honest and orderly production of evidence under established discovery rules.*
>
> *Cabnetware, Inc. v. Sullivan*, 1991 U.S. Dist. LEXIS 20329

Increased reliance on information technology has inevitably led to greater use of electronic evidence in litigation, investigations, audits, and other formal proceedings. In fact, according to the courts, "[c]omputers have become so commonplace that most court battles now involve discovery of some type of computer-stored information."[1] Litigators often take advantage of this lack of preparation by making digital information, especially e-mail, a target of discovery.

Every organization involved in litigation, audits, investigations, and other formal proceedings needs to turn over all relevant information in their "care, custody, or control" to the opposing side (unless subject to a privilege, such as attorney-client), regardless of how embarrassing or damaging it is. Additionally, regulators and auditors may ask for information regarding transactions that occurred years earlier.

What Is Discoverable?

> *All parties in litigation must disclose "a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things the disclosing party has in its possession, custody or control and may use to support its claims or defenses…"*
>
> Federal Rules of Civil Procedure[2]

The *Federal Rules of Civil Procedure*, which provide discovery rules (among other things) for federal courts, define a discoverable "document" as including, "any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form."[3] As this definition of discoverable information is very broad, it could be applied to nearly any type of electronic information imaginable.

Because of the scope of allowable electronic discovery, organizations need to think beyond traditional definitions of an "electronic record" or "document," and consider the entire range of digital information that may be subject to a discovery order. While the need to produce word processing and spreadsheet documents may be obvious to most organizations, e-mail, instant messages, presentations, server log files, HTML code, and other "casual" or "hidden" types of evidence may not be.

An organization's electronic discovery plan should consider the full range of electronic information that the courts may require it to find and produce.

WHAT SECRETS ARE LURKING ON YOUR COMPUTER?

When investigators examine a computer during a trial or other formal proceedings, they can learn a great deal about the owner of the computer from many obscure sources that even the most sophisticated computer user may not think of. From an information security perspective, this also presents challenges when computers are hacked or stolen.

For example, words that a user has added to the custom dictionary in his or her word processing and e-mail programs can reveal a lot about that person's business. A consultant may have added the names of clients, places, and products relating to their work, to avoid the annoyance of a spell-checker consistently tripping over them in word processing documents and e-mail messages. These proper names and confidential data (along with industry jargon) are likely to be extremely important indeed, as they were used frequently enough to cause a spell-checking annoyance.

Electronic Discovery Planning Checklist

To prepare for the possibility of a discovery order covering electronic records, consider the following questions:

1. **Access.** Can electronic records and information be quickly and efficiently found and produced from the storage media and devices upon which they are stored? If not, consider revisiting retention plans, data center capabilities, indexing and searching methods, and characteristics of storage technology in use.
2. **Separation.** If "responsive" e-records (i.e., those relevant to the litigation) will be viewed in electronic form, can they be easily separated from "non-responsive" records and information? This is required to protect against the inadvertent disclosure of irrelevant information that may be proprietary or confidential, and to protect information subject to the attorney-client privilege and/or the attorney work product doctrine. If not, consider how system configuration or new technology investments may provide this functionality, by allowing several different "views" of information according to metadata, access privileges, and other search mechanisms and criteria.
3. **Long-term access.** Can records be preserved in such a way that they can be found, accessed separately, utilized, produced, and/or printed several

years from now if required? Have you accounted for media, software, and hardware obsolescence? These should be standard components of any Information Management program.

4. **Disposition.** Does your organization have outdated, unneeded information and records "lying around" that no longer need to be retained? Ensure that records disposition procedures account for the disposition of *all copies* of digital information.

AN E-DISCOVERY SCENARIO

Your corporate attorney asks you about the company's ability to search for and produce e-mail messages. She needs some help responding to a request from a regulator regarding complaints about aggressive sales tactics targeted at the elderly, and wants to know what e-mail records can be searched and found in the next two weeks.

Are you prepared to respond to her needs? In particular:

- Who would you contact to search and find the required e-mail (called *responsive* e-mail in legal terminology)?
- Do you know for certain what records exist and where to find them?
- Do you have a listing of computer systems, applications, and their administrators and locations within the company?
- Where would you start to look and whom could you assign to help?
- If you have to look in all company facilities in which servers or computers are located, which staffers at each location will do the looking?
- If employees are asked to look through their stored e-mail and for responsive material, how much time will that take, and what will the cost be in terms of lost work, opportunity costs, and real hard costs?
- Which employees could be pulled from their current duties to help search for needed e-mail?
- What contents are stored on backup tapes, and how long are they retained?
- With your company's current technology, can you search every place an e-mail may be stored, and if not, what will you do or whom will you rely upon for assistance?

If you can't readily answer those questions, you should develop a more comprehensive and responsive electronic discovery plan.

The vast majority (89%) of the companies responding to a recent Kahn Consulting survey were actively addressing e-discovery issues. Overall, 93% of organizations were addressing e-discovery, GRC, and/or RIM issues.[4]

Issue #2: Privacy

You've likely received privacy policy statements from your bank, your stockbroker, and your creditors in the past year. And you have probably noticed that e-commerce websites publicize their privacy policies. Whether you've bothered to read any of them or not, you certainly know that privacy has become a prominent consumer issue. The personal information that banks, brokerage firms, creditors, e-merchants, and others collect about their customers is so valuable that other marketers are willing to pay tidy sums for such data. But consumers have become very protective of their private information.

Private Information Is an Asset

Government has recognized the value of private personal information. In *Collier v. Dickenson*,[5] the court ruled that the sale by the Florida Department of Motor Vehicles of the plaintiffs' personal information to mass marketers without the plaintiffs' consent could violate the Driver Privacy Protection Act (DPPA), 18 U.S.C. § 2721-2725, which prohibits disclosure of personal information obtained by the DMV in connection with a person's motor vehicle record without the consent of the person. Plaintiffs could also bring a general civil action for deprivation of rights under 42 U.S.C. § 1983.

Privacy Policy Revisions

Internet retailer Amazon.com faced a similar outcry in 2001 when it allegedly made a change to its privacy policy that would allow it to sell its customer information to a third-party in the event that it was acquired or went out of business. The FTC launched an investigation into the way Amazon.com's change in its privacy policy affected consumers. Around the same time, Amazon paid up to $1.9 million to settle a class action lawsuit launched by users of the company's "Alexa" service, who complained that personally identifiable information was being collected and retained in violation of the

company's privacy policy. The FTC said that, "certain of Amazon.com's and Alexa Internet's practices likely were deceptive," and Amazon.com agreed to pay $40 to each affected user.

Organizations must ensure that their privacy policies are comprehensive enough to address all reasonably foreseeable events, like mergers, acquisitions, new business partners, and changes in business direction. Also, organizations must be prepared to live by the promises made in these policies. If drastic changes are required, it may be necessary to "grandfather" existing customers under the old policy, while applying the new policy only to new customers. In any case, a proactive communication plan for all customers should be a prerequisite of any privacy policy change.

Writing a Privacy Policy Is Not Enough

Even the most well drafted policy won't protect the organization if the policy is not implemented. In Illinois, a consumer brought suit against a retailer for intentionally failing to follow policies designed to keep customer's personal information secure after her debit and credit card information kept by the retailer was stolen by a hacker. Under the Illinois Consumer Fraud and Deceptive Practices Act, the practice must inure to the defendant's benefit. The plaintiff solved this problem by alleging that failure to follow the security procedures enabled the defendant to save money.[6]

Ownership of Information

Your organization has a responsibility to properly manage and protect information assets as it would any other asset that it owns. The data stored on the information systems across your organization, from the largest customer relationship management databases to the smallest handheld e-mail devices, are your organization's lifeblood, and must be protected as such.

The information that employees generate in their day-to-day working activities is also part of your organization's information asset collection. It is your responsibility to inform employees, through policies and training, that all such *business information* is the property of the organization. This will help to establish the importance of the information and set expectations for how this information will be treated when an employee leaves your organization.

The following is a sample policy statement that informs employees about this issue.

Ownership of Company Information: Sample Policy Statement

All information that you create, receive, and/or use while conducting company business is owned by the Company, regardless of whether that information is in paper, electronic, or any other tangible form. In addition, all employees must provide all business information in their possession or control to the Company upon request, at any time, for any reason.

Individuals who cease to be employees of the Company must provide original and all copies of any business information to his or her supervisor prior to leaving the company. All business information located in any Company facility or facilities managed by another entity on behalf of the Company are presumed to be company property. All business information created or stored on or in a Company computer, imaging system, communications system, telecommunications system, storage device, storage medium, or any other Company system, medium, or device are presumed to be company property.

All business information, regardless of its location, that in any way pertains to the Company or Company business is presumed to be Company property. Only upon a showing that the business information in question does not in any way relate to Company business will such information be deemed to be other than company property. Theft or appropriation of any business information is strictly prohibited. Giving access to another person who is not authorized to have access to, review, or otherwise see company business information is also strictly prohibited.

Undertaking these prohibited acts may result in termination and/or civil or criminal penalties.

Privacy of Employee Information at Work

You need to be clear with employees about whether or not they should expect that the information they create and receive on the job is private. Generally speaking, organizations in the United States have taken the approach that such information is not private, and the organization thus reserves the right to access and review it at will.

U.S. courts have generally supported this approach. For example, in *Garrity v. John Hancock Mut. Life Ins. Co.*,[7] two female employees were fired for sending sexually explicit e-mail over the company e-mail system, in contravention of the company e-mail policy. The employees viewed the e-mail containing the offensive content as personal, and argued that the company invaded their privacy when it accessed and examined it. The court weighed the issues in order to determine if "the expectation of privacy was reasonable."

In this case, the court did not find that expectation reasonable, for several reasons:

- The company's e-mail policy stated, "Company management reserves the right to access all Email files," and "there may be business or legal situations that necessitate company review of Email messages and other documents."
- The company "periodically reminded employees that it was their responsibility to know and understand the e-mail policy," and employees had been warned about "several incidents in which employees were disciplined for violations."
- The two employees testified that they sent the e-mail messages (some of which were jokes) to other employees with the expectation that they would subsequently be forwarded to others.
- The employees admitted that they knew the company had the ability to examine company e-mail messages.

Legal opinions on this approach to employee privacy at work are not consistent in every jurisdiction, and companies should investigate the laws of each jurisdiction in which they do business. For example, the Social Chamber of the Supreme Court of France ruled in 2001 that an employee's personal e-mail sent or received on company systems could not be accessed and viewed by an employer, even if the company advised employees that they would do so.

Privacy of Employee Information: Sample Policy Statement

Company resources used by employees to create, transmit, receive, and store business information, such as computers, the email system, and facsimile machines, should only be used for business purposes. In addition, the information in these systems should only be related to Company business. These resources, and the information contained within them, are the property of the Company. Furthermore, the company reserves the right to access and review any business information, whether it is located in company facilities or not.

Employees do not have and should not expect any right to privacy with respect to any Company business information, including email transmission, electronic communication, or Internet or intranet communication. The Company reserves the right to monitor the use of any company property, equipment, phone line, computer, software, or any storage device.

Issue #3: Protecting Company Information—the Programmer's Toolkit

Computer programmers often make copies of programs they create for their employers for their personal use. They may use the programs as part of their "portfolio," examples of their work they can show other potential employers. They may reuse the code in other projects so that they don't have to reinvent the wheel. For whatever reason, this practice can run up against the employer's desire to maintain the confidentiality of their own proprietary information. By reusing code developed for company A in a project for company B, company B may enjoy the fruits of the programmer's labor for company A from reduced costs in terms of reduced programming time, up to what may be the incorporation of innovative and proprietary functionality developed for company A into company B's products.

In *United States v. Shiah*,[8] the U.S. government attempted to prosecute a former programmer, Shiah, under the Economic Espionage Act (EEA) after the programmer created a toolkit of files developed while employed by one company, Broadcom, and used them for a subsequent employer. The government was able to establish that Shiah had copied the files without authorization, that the files constituted trade secrets as defined in the EEA, and that Shiah knew the information constituted trade secrets. The court found, however, that the measures taken by the company to keep the information secret were "barely sufficient to qualify as reasonable" at the time the misappropriation occurred, in 2003. The court observed that "the reasonableness standard will become more and more stringent as time passes. Over time, there will be and have been improvements in technology, information, and knowledge pertaining to data secrecy, as well as more awareness of the EEA and its implications."

The measures taken by Broadcom appear to be impressive:

> *Broadcom's measures included a Confidentiality Agreement signed by every employee. The Confidentiality Agreement explained the value placed on confidentiality at Broadcom and attempted to indicate which documents were considered confidential. This document also prohibited employees from taking confidential information with them upon their departure. Furthermore, Broadcom protected its electronic data through its information technology team, which managed firewalls, file transfer protocols, intrusion detection software, passwords to access the Intranet, a layer of protection between the Intranet and Internet, and selective storage of files. When sharing information with outside entities, Broadcom required non-disclosure agreements, tracked the sharing through DocSafe, and marked documents as confidential. Finally, Broadcom maintained a high security physical facility.*

However, the court found a number of deficiencies in Broadcom's efforts. Broadcom failed to thoroughly explain the Confidentiality Agreement to Shiah before he signed it, and failed to give Shiah a copy so that he could refer to it over the course of his employment. Broadcom also did not give Shiah training about what information is confidential and how to handle confidential information. The Agreement was overbroad in that it designated almost all

information as confidential, so that it would be difficult for Shiah to determine what information actually was confidential. Ongoing training should have been provided to Shiah and other employees, which should have included methods for ensuring that information stayed protected. Broadcom also lacked a comprehensive system for designating which documents were or were not confidential.

The court also criticized Broadcom's performance during Shiah's exit interview; which the court found was intended more to scare Shiah than inform him as to what his obligations were regarding Broadcom's confidential information. Finally, Broadcom never checked Shiah's computer before he left, which would have revealed that he had recently copied thousands of files from the computer. The government's prosecution of Shiah ultimately failed, however, because it could not prove that Shiah intended, beyond a reasonable doubt, to misappropriate the trade secrets for the economic benefit of anyone other than Broadcom, with the intent or knowledge that Broadcom would be injured.

Lessons Learned

- Make sure that policies regarding confidential information are thoroughly explained to employees when they first begin working for the company, ensure they have a copy of the policies by having them sign an acknowledgment that they have received them (and that the policies have been explained to them, and the employees have had the opportunity to ask questions about them).
- The policies should clearly identify confidential information and contain a process by which employees can easily identify information as confidential.
- Develop policies and procedures for departing employees—policies that establish that the company owns all information stored on company systems, and procedures that minimize the chance that employees will steal information when they leave. The obligations of departing employees regarding confidential information should be clearly explained to them in an unintimidating manner.
- Immediately disable all network and e-mail access when the employee is terminated, or at a predetermined time on the employee's last day. Instruct security personnel to develop procedures for quickly disabling network access for any employee at any time, as instructed by senior

management. Inspect any computers used by employees for work purposes to determine whether any files have been recently copied.
- Use Information Management policies to inform employees that you reserve the right to monitor their use of corporate systems, including the e-mail system.
- Your most valuable information may not be in paper form. Thousands of contacts and volumes of information can fit on a single CD, USB memory stick, mobile e-mail device, and numerous other media that can easily be slipped out of your facilities.

Issue #4: Disaster Recovery and Business Continuance

Although organizations have long prepared contingency plans designed to enable them to survive a disaster, after the events of 9/11, the concept of disaster recovery and business continuance has widened and become more complex. Today, it is clear that disaster recovery and business continuity concepts need to be a part of every Information Management program.

Moreover, contingency plans need to be constantly updated and adapted to account for new realities and risks. For example, when the SEC summarized the "Lessons Learned" by the financial industry after 9/11, they found that, although most Wall Street firms had backup systems and data centers, many had not counted on the "wide-area" disaster of 9/11. As a result, some firms that had "arranged for their backup facilities to be in nearby buildings… lost access to both their primary and backup facilities in the aftermath."[9] Clearly, the events of 9/11 required all firms to revisit many aspects of their disaster recover plans to provide for greater geographic dispersion of backup facilities, and many other elements that respond to newly understood disaster scenarios.

Hurricane Katrina required many firms to put their disaster recovery plans into operation. The importance of following those plans was demonstrated in *Bank of Louisiana v. SunGard Recovery Services, Inc.*[10] The bank had previously tested its disaster recovery plans with SunGard several times, sending backup tapes to SunGard's facility in Georgia and successfully getting their systems running on SunGard's equipment.

When Hurricane Katrina struck Louisiana, the bank's CFO was unable to contact appropriate personnel. Although the CFO contacted SunGard and declared a disaster, she ultimately was not able to find the backup tapes. At SunGard's suggestion, she attempted to start up the system and make a backup using generator power but was not successful. Ultimately, she decided to send the system's hard drives to the vendor to which the bank had previously decided to outsource its IT functions.

The court ultimately found that SunGard had not breached its contract, noting the bank's failure to find the backup tapes, and that the CFO "did not request a deviation in the rehearsed plan. She did not ask SunGard to send personnel or a mobile data center to New Orleans or to deliver the recovery system to a Bank of Louisiana facility."

> *There is no evidence that Schaefer [the CFO] consulted with SunGard to notify them she had removed the hard drive or to inquire whether she should send them to Georgia, instead of Michigan, or send the tapes to Georgia after the data was retrieved. Schaefer instead ceased all contact with SunGard until she canceled the disaster declaration on September 14, 2005. Meanwhile, after retrieving the hard drives, she forwarded them to Michigan.*

Although the Court lauded the CFO's actions in getting the bank back into operation, nevertheless, it found that SunGard had not breached the contract, and that the bank was liable for the unpaid balance of its 60-month contract.

IMC relies on disaster recovery and business continuance plans that protect business information and records. The best developed and maintained Information Management program is of little utility if the information assets that it is designed to manage are put at risk by an organization's failure to identify and respond to disasters and other risk factors that could cause large-scale loss of data, system outages, and other events that hamper an organization's ability to properly retain and manage business information.

Issue #5: Information Security

Protecting your information assets can be a difficult task, requiring a complex mix of technology, policies, and people to combat expanding threats from viruses to hackers and everything in between. IMC depends on good information security practices, and there are several unique Information Management issues to consider, as explored below.

What Are We Trying to Protect?

There are several reasons why organizations need to implement security strategies for e-mail. Failing to address security around our business information, including e-mail, unnecessarily exposes organizations in all sorts of ways. Information security has a broad purpose that includes:

- Protect information from corruption
- Protect information from misappropriation and misuse
- Protect business operations
- Protect systems from interruptions, failures, and outages, and resulting loss of productivity
- Promote secure business
- Protect company reputation from bad publicity
- Promote confidence in leadership and company management
- Protect the integrity of company data
- Guard against loss or theft of property
- Prevent repudiation and unwinding of business transactions
- Protect the identities of business partners
- Protect different classes of company records, including proprietary, trade secrets, and privileged and confidential communications

Managing Information Security Records

Information security systems create unique types of data that should be given special attention in your Information Management policies and procedures. Some data may require special handling procedures due to their complex or technical nature (e.g., encryption keys), and your Information Management program must account for this type of information. While special procedures may be required, you must ensure that such information is managed according

to your established IMC principles, regardless of how unique the content or form of the information may be. You should:

- Conduct an inventory of information security-related software and hardware used throughout your organization, such as encryption systems, firewalls, and user authentication modules.
- Work with IT/IS to determine what kind of information these technologies are generating or storing.
- Determine if any of this information meets your definition of a record. If so, establish a plan for the capture and retention of such information, which may include the creation of new categories for such information in organizational records retention rules.
- Remember that some information (firewall logs in the case of break-in, for example) may be required for litigation and other formal proceedings, and should be included in any Records Hold order related to such proceedings.

A good example of unique information security data is the records created by Public Key Infrastructure (PKI). PKI is a system of policies, people, and technology used to secure information systems. PKI uses advanced cryptography, and can be used for a variety of security-related purposes such as authenticating online identity, and protecting the confidentiality and integrity of information using encryption and digital signatures.

The records produced in the operation of a PKI include a variety of important policies, representations, contracts, and statements that have legal importance to the people and organizations that use and rely on transactions involving PKI. These include documents such as Certification Policies and Certification Practices Statements.

In providing guidance to organizations faced with the task of properly managing PKI records, NARA stated:

> *A key premise for this guidance is that PKI-unique administrative records do not constitute a new category of records that require a total "reinvention" of lifecycle Records Management policies and guidance. While the records a PKI produces may be unique in their content and application, the Records Management practices, as already embodied in certain federal statutes, regulations, guidance and standards, still apply.*[11]

Road Warriors

Recent surveys indicate that the number of employees who work remotely more than 8 hours per week was about 12 million in 2007, up from 6 million in 2000. The number is expected to hit 14 million by 2009.[12]

Although the benefits of telecommuting includes lower office overhead, improved morale, and boosted productivity,[14] companies must also be careful to consider the Information Management implications of this movement.

Mobile and remote workers present several unique IMC challenges that you must address in policy and procedures, including:

- **Data protection.** Valuable data stored on mobile devices is more vulnerable to theft and loss than those stored inside the walls of the organization. Train employees to be aware that their laptop and PDA are targets for thieves. Airport security screening procedures post-9/11 that require the removal of these devices from carrying bags increase the risk of theft.
- **Retention.** You need a plan to ensure that information on mobile devices is routinely backed up or "synced" to your data center. There are a number of ways to securely perform remote backups to the corporate data center, which you should investigate with your IT/IS department. Data should not be retained or backed up on employees' home computers.
- **Unique records.** Mobile devices may create and retain data in proprietary or obscure formats that may not easily be handled by your Records Management systems. Ensure that data from such devices can be captured and retained in an accurate and reliable fashion before allowing employees to use such devices.

DO YOU HAVE A LAPTOP PROBLEM?

A clothing retailer retained a third-party business to help with hiring employees. A laptop containing the personal information of 800,000 applicants was stolen. According to the September 28, 2007 *Computerworld* story covering the disaster, the company was notifying all that may have been impacted by the data theft and also offering them a year of free credit monitoring and fraud resolution assistance.[15]

DO YOU HAVE A LAPTOP PROBLEM? ***(Continued)***

Sales of laptop and notebook computers are outpacing sales of desktop computers.[16] Now is the time to look around your organization and see if you have a laptop problem.

Laptop computers can go anywhere, hold vast amounts of data, and can be connected wirelessly in an increasing number of public places. These advantages can be an Information Management nightmare. Are you addressing these issues?

- Ownership of data on laptop computers, especially if the computers are purchased by employees
- Loss resulting from theft of laptop computer containing proprietary company information
- Remote regular backing up of data for road warriors
- Information security policies for employees connected to public Internet and wireless terminals
- Finding and producing laptop content for litigation, audits, or investigations
- Personal use of laptop computers
- Installing and using only approved software on laptops
- Protection of confidential and trade secret information

Employee Use of Public Terminals

Maybe now you think that equipping employees with the latest and greatest laptops and portable devices isn't the best idea, and you should make road warriors use public Internet terminals like everyone else!

Not quite.

In 2003, a 24-year-old Queens, New York, man pled guilty to federal charges of computer damage, access-device fraud, and software piracy.[17] According to reports, the man had surreptitiously installed keylogging software on a number of Kinko's public Internet access terminals throughout Manhattan. The software enabled him to record each key pressed by customers accessing the Internet, including their passwords and a wealth of confidential and personal

information. He then used that information to invade those customer's bank accounts, open new accounts in their names, and transfer funds to unauthorized accounts.

In this case, the hacker's plans seemed limited to using the stolen information to rob personal bank accounts. What if the motives were corporate espionage? What kind of information could he get from a Wall Street administrative assistant checking work e-mail from an Internet café on a lunch break? Financial information? Company passwords? If he or she opened an e-mail attachment containing a confidential presentation, for example, a copy of that file may be created on the public computer, even if the administrative assistant does not save it. And, a sophisticated criminal, such as our man in Queens, would know where to find it.

What can you do to protect against these security risks? One approach is to prohibit employees from using public computers for work purposes. If this is not practical, at a minimum, employees should receive training on the risks of using public terminals.

Patch Management

In the summer of 2003, organizations around the globe were hit with a double whammy. The W32.Blaster computer worm took advantage of operating system security vulnerabilities, and a virulent new form of the Sobig virus generated thousands of infectious e-mail messages. Computers were disabled, airline flights were delayed, and some trains stopped running.[18]

For organizations in the northeastern United States, which were also victims of power outages around the same time, it was an information security "perfect storm." In fact, there is evidence that the worm significantly hampered efforts to address the blackout.[19]

Patch Management (PM) is the art and science of keeping software up to date with the latest *patches*—pieces of computer code that fix a vulnerability, correct mistakes, improve functionality, and so on. While it may sound simple and neat, PM today is messy work. Allowing your antivirus software to automatically update itself on your personal computer is one thing—applying an operating system patch to 20,000 computers across the globe is another.

Organizations employ a variety of tools and techniques to help. For example, many vendors provide software that will automatically inform an IT department when updates are available for a specific piece of software, and then help them test and install that update across an enterprise.

In the case of the W32.Blaster worm, many people questioned why the worm was able to spread at all, given that the vulnerability, and the patch fixing the problem, had been released weeks before. This event served to highlight the many difficulties of PM.

Organizations with massive computer networks that support many different operating systems and complex customized software cannot simply install the latest patch without adequate testing—a process that may take weeks and months to complete. However, new vulnerabilities are discovered every day. According to the CERT Coordination Center (a noncommercial institution that tracks and advises on information security incidents globally), the number of software security vulnerabilities has doubled every year since 1999. In 2002, there were nearly 4,200 reported vulnerabilities.[20]

To address the gap, organizations apply risk management principles, weighing the damage potentially caused by the security vulnerability against the cost of testing and applying the patch. And to ease the pain of applying the patch, many organizations also employ change management techniques to ensure that their systems will not malfunction due to software changes caused by new patches.

Aside from the inherent difficulties of PM, many organizations continue to be vulnerable simply because they have inadequate policies and procedures. Through lack of awareness, commitment, resources, or other reasons, increasingly, organizations without a PM plan are putting themselves, and other organizations, at risk.

Patch Management must be a part of your organization's Information Management Program.

Notes

[1] *Bills v. Kennecott Corp.*, 108 F.R.D. 459, 462 (D. Utah 1985).

[2] Fed. R. Civ. Proc. 26(a)(1)(A)(ii).

[3] Fed. R. Civ. Proc. 34(a)(1)(A).

[4] "*GRC, E-Discovery, and RIM: State of the Industry*—A Kahn Consulting, Inc. Survey in association with ARMA International, BNA Digital Discovery and E-Evidence, Business Trends Quarterly, and the Society of Corporate Compliance & Ethics," (Fall 2008), p. 5, found at `http://www.kahnconsultinginc.com/library/surveys.html`

[5] 477 F.2d 1306 (11th Cir. 2007), *cert. den.* 128 S.Ct. 869 (2008).

[6] *Richardson v. DSW, Inc.*, 2006 U.S. Dist. LEXIS 1840 (N.D. Ill. Jan. 18, 2006).

[7] *Garrity v. John Hancock Mut. Life Ins. Co.*, 146 Lab. Cas. (CCH).

[8] *United States v. Shiah*, 2008 U.S. Dist. LEXIS 11973 (C.D. Cal. Feb. 19, 2008).

[9] "Summary of 'Lessons Learned' from Events of September 11 and Implications for Business Continuity," Securities and Exchange Commission, February 13, 2002.

[10] *Bank of Louisiana v. SunGard Recovery Services, Inc.*, 2008 U.S. Dist. LEXIS 20788 (E.D. La. Mar. 17, 2008).

[11] "Records Management Guidance For PKI-Unique Administrative Records," National Archives and Records Administration, March 14, 2003.

[12] Eve Tahmincioglu, "The quiet revolution: telecommuting," msnbc.com, October 5, 2007; available at `http://www.msnbc.msn.com/id/20281475`

[13] "Hotspots: Hot Wireless Initiative," Yankee Group and Gartner Dataquest reports, eMarketer, July 8, 2003.

[14] "Business Benefits of Telecommuting," Economist Intelligence Unit report, eMarketer, July 17, 2003.

[15] Brian Fonseca, "Personal data on 800,000 Gap job applicants exposed in laptop theft," *Computerworld,* September 28, 2007.

[16] "Notebooks Claim Over 50% of Retail PC Sales," NPD Group report, eMarketer, July 9, 2003.

[17] "Queens Man Pleads Guilty to Federal Charges of Computer Damage, Access Device Fraud and Software Piracy," U.S. Department of Justice press release, July 11, 2003.

[18] Guth, Robert A., and Daniel Machalaba, "Computer Viruses Disrupt Railroad and Air Traffic," *The Wall Street Journal*, August 21, 2003.

[19] Verton, Dan, "Blaster Worm Linked to Severity of Blackout," *Computerworld*, September 1, 2003.

[20] CERT website—`http://www.cert.org/stats/`

Resources from StoredIQ:

StoredIQ

- **Legal Aid: How IT Can Be the Difference Between Litigating or Settling**
- **Product Profile: StoredIQ for Intelligent eDiscovery and Information Management**
- **The Top 10 Questions: You Should Ask Vendors When Evaluating an In-House eDiscovery Solution.**