Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Information Privacy Topics, A Discussion

Privacy is a sensitive issue that we all concerned about to some degree. Nobody wants to think that his or her every move is being watched...on the computer or not! This is also true for electronic messaging, files, and email in the workplace. When these issues are raised, inevitably there are questions that follow. Who owns these electronic files? Who can access and disclose their data? Such questions become especially important when company/client sensitive or confidential information is stored electronically. Anothe...

Copyright SANS Institute
Author Retains Full Rights

AD

Jennifer Celender
Information Privacy Topics, A Discussion
Version 1.0

Privacy is a sensitive issue that we all concerned about to some degree. Nobody wants to think that his or her every move is being watched…on the computer or not! This is also true for electronic messaging, files, and email in the workplace. When these issues are raised, inevitably there are questions that follow. Who owns these electronic files? Who can access and disclose their data?

Such questions become especially important when company/client sensitive or confidential information is stored electronically. Another issue is that of Internet privacy. Our preferences and personal information can be stored with Internet Service Providers and other companies operating online. Where does it end? Who can find out what about us? These topics are ones that are likely to be in the minds of people for years to come. This paper will discuss current laws over electronic data and emails in the workplace, and associated rights of both the employer and employee. Adopting a well-written security policy is a crucial aspect of the electronic world and an issue that needs to b taken seriously. Developing such a policy will be addressed, as well as ways to improve your current policy.

The employer can be held responsible for the employee's actions. From this standpoint, I understand the need to monitor employee usage. Companies can be responsible for employee activity on systems including e-mail, voicemail, and Internet use (and misuse). Employers need to make employees aware of the risks involved with using their systems. Firms are becoming increasingly concerned with what employees are saying and doing (on and off company time) with their systems, because of the fact that the lawsuit and fines would come to them. As a way to mitigate their risk, more and more firms are monitoring employee's usage of such systems. In fact, approximately 45% of U.S. firms monitor workers' electronic communications, to include e-mail, voicemail, and Internet use. 55% of firms use blocking software to prevent unauthorized use of their communications equipment, and 29% prevent access to what they considered inappropriate Internet sites (Yaukey, 1-2).

Email is one of the more sensitive topics, because of its traceable factor. Employee gossip in the traditional sense cannot be traced - there usually is no documentation of such conversations. Emails are typically backed up onto company servers and archived for a certain amount of time, which can be pulled if needed for proof or documentation of the event (Bacard, 2). Emails have actually been subpoenaed in lawsuits, so users beware! Companies can be subject to severe penalties if they cannot produce such records, so they are developing email policies stating that the purpose of the email system is for business purposes only (Nichols, 2). Once this waiver has been issued, the company basically has "free reign" over their employee's emails (Bacard, 2).

Courts have sided with the company and management on this issue, stating that they have the right to monitor employee's emails since it is the company that owns the computers (Yaukey,

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

2). One source stated, "An employee should have no expectation of privacy rights in the workplace. That's not what the workplace is all about. Employers own the system and the PC's or the laptops. They are liable for what the employee does on them, for harassing messages they might send. There's very little that protects employees from the eyes of employers," (The Perils of Privacy, 2). So employees (again) beware!

Employer concern is not only court action/lawsuits and liability; it is wasting employee time and using up precious bandwidth on the system. 90% of employees receive personal (not work related) emails, and the same number admit to surfing Internet sites unrelated to their jobs while on company time (Yaukey, 2). Highly graphical forwards, email jokes, and e-cards tend to use a lot of bandwidth, slowing the systems and networks down for users that need those resources for work related projects. Time is wasted as employees sift through numerous inboxes of advertisements and "junk mails." The tradeoff is the amount of money the company saves on conventional "snail mails" with associated stationery and postage costs, verse the reduced turnaround time associated with electronic communications.

From a purely legal standpoint, I tend to agree with the employer side of this argument. If a company is trying to track down abuse of resources that they own, they should have the right to monitor usage and have files available for documentation if needed. Several recent companies and court cases have also supported this view. The *New York Times* fired 23 employees in Norfolk, VA last year for emailing distasteful jokes from their company accounts (Yaukey, 1). Chevron paid a $2.2 million settlement to employees who claimed unmonitored, sexually harassing email created a "threatening environment," (Yaukey, 2).

In the Texas case McLaren, Jr. V. Microsoft Corporation (1999) an employee brought a common law case of invasion of privacy against Microsoft for breaking into some of the folders on his company-owned computer and releasing the contents to third parties. McLaren, Jr. had a personal password on these folders and thought that an expectation of privacy existed. The court sided with Microsoft, stating that the password did not create an expectation of privacy, and that the reasonable person would not find the interception of such messages highly offensive (Bruce/Wiley, 4).

Another, more shocking case in 1999 dealt with a Federal court in Pennsylvania adopting a similar view. Lets look at the details of Smyth v. Pillsbury Company (1997). The Pillsbury Company had repeatedly told its employees that their emails would remain confidential, privileged, and would not be intercepted and used against employees as grounds for termination or reprimand. Given this statement, an employee made unprofessional comments in an email to his supervisor. These comments were the basis for terminating the employee. As in the Microsoft case, the court found that the employee did not have a reasonable expectation of privacy. This after Pillsbury had assured employees that their emails would not be monitored or used against them (Bruce/Wiley, 4).

Both the Microsoft and the Pillsbury case deal with invasion of privacy and the common law of expectation of privacy. As we have seen, such claims will not hold up in a court of law. The courts general opinion is that the company owns the computer systems and has rights to all use and information on them (Perils of Privacy, 3). A way to mitigate such common law

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

invasion of privacy lawsuits is for the company to adopt an e-mail and resource use policy so that the intent of the company is known. Additionally, there are some state and federal laws regarding this issue.

According to the source entitled "Privacy Policy Toolkit," Connecticut enacted a measure requiring employers "who engage in any type of electronic monitoring" to give a prior, written notice to employees that may be affected by this monitoring, informing them of the type of monitoring that would occur. California vetoed a bill that would have required the same kind of disclosures; while Massachusetts is considering a very similar bill. In May 2000, California was considering a related bill that would prohibit an employer from secretly monitoring email or other personal computer records generated by an employee. The state of Washington ruled that the State privacy statute did not apply to email, since the statute did not explicitly refer to computers or email. This was ruled in a case where an individual was caught seeking sex with minors over the Internet. They obtained numerous emails as evidence against this individual but they were all inadmissible under this statute (Bruce/Wiley, 5).

There is no Federal statute that provides employees a federal right to privacy with respect to employer monitoring of their employees. The Electronic Communications Privacy Act of 1986 (ECPA) extends the wiretapping laws to cover electronic data. ECPA provisions prohibit the unauthorized access to or use of stored electronic communications. Providers of such communications are also prohibited from disclosing the contents of their stored communications. The Fourth Amendment of the Constitution protects citizens from unreasonable searches and seizures by the government. California's Constitutional provision extends and applies this right of privacy to email communications (Bruce/Wiley, 6).

From the standpoint of the employee, and being an employee myself, I can understand the desire to have your files and emails kept private. The thought of having someone watching your every keystroke is as unsettling as the thought of someone listening to your every phone conversation! The fact of the matter is, no matter what the company tells an employee to do; the company's resources are almost inevitably going to be used for personal reasons. I can't think of a way that your personal life would not affect your professional life, especially now that most people are working at least 8 hour days. The employees must be made aware of the company's intent to monitor and take action against misuse of resources. This is where the value of a comprehensive, well-written security and email policy is seen.

A security and email policy limits the company's liability. The typical policy statement is only about one to two pages in length and is written in clear, concise terms that the employee can easily understand (Peltier, 2, 4). There are two different types of security policies: Program-level and Issue specific. A program-level policy's main function is to establish the security program, assign program management responsibilities, state the organization-wide IT security goals and objectives, and provide a basis for enforcement. Issue-specific policies also can be developed. These identify and define specific areas of concern and to state the organization's position and expectations in relation to them (www.secinf.net, 1). Following are discussions on these two basic types of security policies.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Program-level policies are much broader in scope than Issue-specific policies. They generally are the first document to formally establish an IT security program. Program-level policies will define the goals and objectives of management and the policy, as well as the employee's roles, responsibilities, and accountability (www.secinf.net 2). Issue-specific policies supplement the program-level policy. They address a specific behavior or system. They are dynamic and tend to change as the environment changes. For example, with the increased threat of virus and hacker attacks on systems, companies are developing more strict policies on the use of floppy disks, downloading, and shareware (www.secinf.net, 2).

Important points to consider when formulating your email policy are to include the purposes for email in the company, the third-party access to email allowed, and consequences for breaching the policy (Peltier, 4-6). A "best practice" that companies are using to handle the policy issue is to make employee's read it and take and pass a test before starting employment. Passing the test makes the employee liable for any breach of the policy given the fact that they demonstrated they understood the policy and its consequences if breached.

Additional pieces of information that could be important in a security policy include Internet sites, use of the company telephone, and related resources. Email should not be the only concern. Employees that work from home, either during normal business hours or after hours, present another issue for corporate privacy policies (Feldman, 3). The work-at-home employee may use his own hardware, software, and Internet service provider, and then the general unspoken rule of the company owning the computer system/resources and being responsible for all information contained on it would not be applicable. In some cases, the company may provide the computer or subsidize the purchase. Agency law states that the employer may be responsible for that employee's actions if the actions are undertaken within the scope of employment and to benefit the employer (Bruce/Wiley 7-8).

Some employers are already addressing this growing concern. In 1998, the NASD, together with the SEC, issued a notice to all securities dealers in order to prevent unauthorized and fraudulent sales of securities claims to the public. The notice read, "NASD Regulation would expect members to prohibit correspondence with customers from employee's home computers unless the firm is capable of monitoring such communications," (Bruce/Wiley, 8). My company addresses this issue by providing our dial-in communications line and enforcing that only work-related activity be used on that line. The firewall monitors this external activity as well.

Courts have been able to subpoena home computers during lawsuits when work has been performed from home. Companies should take active steps to protect themselves from such subpoenas and surprises from home computers. The privacy policy should contain the employee's knowledge and consent to access that information in the same manner as that information housed on machines at the company.

As with any policy or management trend, the issue of privacy can cost companies a substantial amount of money. There are a lot of free resources regarding this issue on the web and in magazines, however, given the legal nature of this topic, one may want to consider investing a considerable amount of time and funds in the subject. For example, books are

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

available to help companies phrase policies in the right manner. This is important so that no issue is misstated. Also, there are resources available to help companies include all aspects of the topic and all departments in their plan. This may seem like a daunting task, but the lawsuits and liability could be even larger. I would recommend to companies large and small to develop a team to address the security policy and keep it current.

The team should consist of equal parts ownership, management, and staff. Attorneys and third party consultants should be used as necessary for verification and review of the policy (Peliter, 5). Once this issue is in the minds of management, it is sure to trickle down and be in the minds of the workers. And even if the company isn't of a tremendous size, this is important to minimize the risks. Additionally, as stated above, employees should be made well aware of the policy, even to the extent that they should take a test to demonstrate their understanding of it. Once all bases are covered, this will help to foster a level of trust and acceptance among the users.

Protecting privacy through the implementation of an organization-wide policy will enhance the work environment and promote a more positive morale among the user community. There is a fine line between "employee privacy and employer proprietary interests on their own" (Peltier, 8). Keep in mind these points from the Los Angeles Business Journal and you should be on the right track:

1) Adopt, implement, and enforce and email and Internet use policy.
2) To avoid employee right to privacy claims, include language in the policy to notify employees that their email messages and Internet activity may be monitored.
3) Include specific restrictions pertaining to the content of electronic messages, prohibiting messages that are defamatory, profane, obscene, tortuous, offensive, or otherwise unlawful and prohibiting employees from disturbing copyrighted material or company trade secrets and confidential information.
4) Establish and enforce a policy for email retention and system security, including the need for employees to protect their passwords and use security measures such as encryption to send sensitive documents.
5) Include procedures in the policy, which encourage early reporting by employees of offensive practices.
6) Implement internal procedures to effectuate a prompt, fair investigation of employee complaints involving the use of Internet and email transmissions, and inform employees that inappropriate conduct will lead to disciplinary action, up to and including termination.
7) Warn employees that email is for business purposes, and encourage employees to send and receive personal e-mail during non-business hours at home
8) Consider the use of filtering software to prevent employees from accessing certain web sites and monitoring software that identifies email containing specific terms
9) Examine contracts with communications and Internet access providers to determine whether certain services…could be considered an extension of the workplace in employment discrimination claims.
10) Communicate to supervisors and managers the importance of early reporting of policy abuses, and carefully monitor compliance.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

11) Periodically review Internet and email policies for legal compliance.

© SANS Institute 2002, Author retains full rights.

REFERENCES

Bacard, Andre. "E-mail Privacy FAQ." Date unknown. http://www.andrebacard.com/email.html.

Bruce, James T. "Privacy Policy Toolkit: A Guide to Formulating Your Company's Policy." June, 2000. http://www.ema.org/restricted/documents/.

Feldman, Carla. "Minimizing Employer Liability for Employee Internet Use." July 31, 2000. http://www.findarticles.com/cf_0/m5072/31_22/63986324/p1/article.jhtml.

Gaudin, Sharon. "The Perils of Privacy." 1999. http://www.nwfusion.com/power99/power99-privacy.html.

Nichols, Keith. "Are Prying Eyes on You?" September 22, 1998. http://www.zdnet.com/products/stories/reviews/0,4161,1600785,00.html.

Peltier, Thomas R. "Establishing Business Controls for Electronic Communications." 2001. http://www.gocsi.com/email.htm.

Yaukey, John. "Firms Crack Down on e-mail." June 28, 2000. http://www.usatoday.com/life/cyber/tech/cti164.htm.

© SANS Institute 2002, Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced