Global Information Assurance Certification Paper

Consideration of Privacy Issues in Risk Assessments and Policies

Kelly Glines
GSEC Version 1.4b, Option 1
March 18, 2003

Abstract

The proliferating use of computers, networks, Internet, and e-mail, has introduced to the world new benefits and drawbacks in this Information Age. The technology affects each individual in their workplace, community, travels and home. Cognizant or not, individuals are using computers and providing information…personal and confidential information. Entities receiving this personal information are using it for good cause; and they are manipulating, storing, and disseminating the information, sometimes to the chagrin of the individual.

For entities receiving personal and confidential information, a careful awareness and action must be made in order to retain reputation, loyalty, and consideration of an on-going concern. This information is a valuable resource and must be treated as such. Information technology has potential for vulnerabilities and abuse, and management is urged to observe the risks involved. Knowledge of the vulnerabilities and risks provide guidance to the best possible solution for securing the information. An introduction is provided here to describe some privacy issues the field of information technology faces. The risk assessment methodology will be used as the framework for acknowledgement of potential risks and problems, and privacy policies will be introduced as the platform for securing the sensitive information at an acceptable risk level.

A Brief Legal History of Privacy

In 1789 the U.S. Constitution came into effect. Shortly thereafter, a more specific, personal demand for individual rights promulgated the adoption of ten amendments. In 1791, dubbed the "Bill of Rights," the Fourth Amendment states that:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath of affirmation, and particularly describing the place to be searched, and the person or things to be seized.*[1]

Later, the 20th Century saw an increasing number of court cases concerning an individual's right to privacy as set forth in the Fourth Amendment. Some landmark privacy cases include[1]:

- Griswald v. Connecticut (1965) – relating to a married couple's decision to employ birth control;
- Roe v. Wade (1973) – regarding the woman's decision to have an abortion; and
- Cruzan v. Director, Missouri Dept. of Health (1990) – relating to the decision whether to continue one's life or not.

These types of cases focused on what Harry Henderson considered "a "zone"- a house or a person – that was protected from intrusion by the Government except under specified circumstances."[1] These 'zones,' however, were more focused on the individual rights regarding a decision about one's body or material belongings.

In the new Information Age, immense strides in technology forces the focus of privacy issues more on the flow of information about a person, the person's ability to decide who will get the personal information, and how the information will be used. Court rulings in the 1970's and 1980's, however, held that individuals did not have a 'reasonable expectation of privacy' as the following cases indicate[1]:

- U.S. v. Miller (1976) - Checks and bank records are not private because they flow between banks as part of ordinary commerce;
- California v. Greenwood (1988) and Oliver v. U.S. (1984) - Garbage at the curb or materials stored in an open field are not private; and
- Florida v. Riley (1989) - It is permissible for a police helicopter to peer through a hole in a roof to look for marijuana plants.

Privacy of this personal information does not pertain to the person's body itself, nor does it preclude any security measures on the part of the person. Privacy advocates, however, have structured their effort on important legislation, such as the Freedom of Information Act of 1964, the Privacy Act of 1974, and the Electronic Communications Privacy Act of 1986.

The New Millennium

During the early 21st Century, prior to the tragedies of September 11, 2001, privacy over personal information emerged as a hot subject for the advocates, victims of identity theft, lawmakers, business decision-makers, and a struggling IT staff. Periodicals clamored to keep pace with the daily news of workplace surveillance, medical privacy regulations, FBI e-mail wiretapping, consumer tracking, and the arrival of the new position of CPO (Chief Privacy Officer).

A feature from the journal, Information Systems Control, listed the top 10 stories concerning privacy issues in the year 2000, according to privacy advocate analysis:[2]

1. "Workplace Surveillance Heats Up" (66 percent of American workplaces report performing in-house surveillance and 27 percent monitored email)
2. "Patient Privacy Rules" (regarding HIPAA (Health Insurance Portability and Accountability Act, 1996) – the new medical privacy regulations)
3. "Carnivore Attacked" (FBI e-mail surveillance)
4. "Double-Click Unplugged" (marketing of consumer data)
5. "Rise of the New CPO" (dozens of Fortune 500 companies have created the new position)
6. "Amazon.com Surveys the Data Mine" (changing privacy policies to capitalize on customer data)
7. "The Urge to Merge Financial Information" (regarding G-L-B (Gramm-Leach Bliley Act), the new financial regulations November 2000)
8. "Wireless Privacy Battles Loom" (deployment of location-sensing E911 service for cell phones)
9. "Microsoft Crumbles on Cookie-Blocking" (backing off on patches to 3rd party cookies due to Internet advertiser's push)
10. "A New Kind of Public Record" (emails and server logs of government and schools sought after and obtained by media and individuals as public record).

Clearly these issues were important considering their potential ramifications. However, post-September 11, privacy interest waned in a trade-off for overall security. As an effort to secure the homeland, the public and businesses acquiesced to increased scrutiny and surveillance. New governmental programs were created for the sake of a secure nation. Most notably, in addition to the newly formed Federal Homeland Security Department, the Total Information Awareness (TIA) program was implemented by DARPA (Defense Advanced Research Projects Agency). The TIA objective is to "play offense with personally identifiable information to find patterns otherwise noticed…and using that insight to preempt threats"…The program…"adds identity and a wide swath of transactional records – financial, educational, travel, medical, immigration, transportation, accommodation and communications."[3]

The trade-off of privacy for security was further reflected in a Harris Interactive Study conducted March/April 2002.[4] In this study, employees in private, governmental, and non-profit organizations were surveyed. The published report indicated that 76 percent of the respondents felt that their employer's privacy rules and practices could be "tightened up." They felt that employers, specifically, could perform more in-depth background checks on current and potential employees.

While the post-September 11 trade-offs and acceptances were real and commonplace, the latter part of year 2002 saw resurgence in privacy concerns. With the aftermath shock dissipating, as well as fears of terrorism and war, the intensity of this resurgence was perhaps even stronger. A brief perusal of news headlines in January 2003 on any given day brings the threats of personal privacy and information technology back in focus:

> "**Latest ID Theft Scam: Fake Job Listings"** [5]
>
> **"Crucial Data Rescued After Hacker Raid: Key Server Stripped: 'It was Akin to Hacking the Pentagon' "**[6]
>
> **"ATM Encryption Weaknesses Leaves Accounts Vulnerable"**[7]
>
> **"British Intelligence PC Stolen"**[8]
>
> **"Millions of Credit Card Numbers May Have Been Compromised"**[9]
>
> **"Personal Storage Sites are the Latest 'Security Risk' "**[10]

These examples represent just a miniscule portion of actual occurrences threatening the privacy of individuals and entities over the course of just a couple of weeks. Many other similar breaches of privacy could also have been included. The point here is to recognize that negative things can happen if information is obtained. Maintaining confidential and sensitive information is a serious undertaking.

Framework for IT Security: Assessing the Risk

Realizing the potential consequences of sensitive information leakage must be understood in developing the steps that should be taken by an organization to ensure the security of the private and sensitive data in their possession and charged to their care. The negative ramifications of privacy breaches regulated or not include litigation, bad publicity, loss of revenues, diminished customer confidence, and a decrease in employee moral. Without a doubt, this type of information must be protected along with the rest of the resources of an organization. The risks related to privacy issues are numerous and grave; they dictate a need for assessment and effective security policies.

Prior to implementing policies and procedures for protecting sensitive information, it is important to define the risks involved. This process is most effectively achieved through a formal information technology (IT) security risk assessment.

The objectives of the risk assessment, notably the IT security risk assessment, are to:[11]

1) Identify the information technology risks,
2) Determine the level of risk,
3) Identify the risk factors, and
4) Develop risk mitigation strategies.

Numerous resources are available that offer guidance and templates in performing a risk assessment with respect to IT, including consultants that specialize in IT, security, and risk assessments.

One such network security consulting firm, Veridyn, has produced a white paper outlining the steps they follow when performing security IT risk assessments. In "The Ten Essential Steps to Effective Security Risk Assessments,"[12] Veridyn divides the risk assessment project into three phases consisting of ten steps. Using the Veridyn phases and steps as a working template, an illustration is created here to place privacy issues and the sensitive information asset into the risk assessment process. The completed risk assessment will provide the framework for setting security policies.

The Phases & Steps to Risk Assessment With Highlights of Privacy Issues

STAGE 1: Project Preparation	
Step 1:	***Obtain support and Involvement from Sr. Management***
	Support and involvement from Sr. Management is necessary to focus on critical elements and systems of the organization, and provide approvals for the resources required. In privacy matters, this would entail the involvement of the CIO/CIO/CSO, legal counsel, and other organization sr. management.
Step 2:	***Choose a Team***
	The team should include personnel with power, technical and business expertise, and/or major focal points in the organization. To highlight privacy issues, representatives from the following departments will be necessary: legal counsel, IT technical and administration, human resources, facilities management, and divisional directors.
Step 3:	***Plan the Assessment Project***
	The steps, resources and scheduling to produce the risk assessment need to be considered. This is to ensure cooperation among the various organizational units, provide for applicable training and awareness of all decision-makers, and ensure schedules of activities are reasonable and adhered to.
STAGE 2: Risk Assessment Execution	
Step 4:	***Identify Potential Technology Risks***
	An identification of the potential risks to sensitive information and privacy concerns involves gathering information regarding the current information system architecture including all technology layers (hosts, servers, software, operating systems, etc.). The latest common vulnerabilities should be noted as well as the realization that they are constantly changing. The confidential information should be defined, where it is stored, who has logical and physical access, and how it flows.
Step 5:	***Identify the Potential "People, Process and Environmental" Risks***
	The risks associated with people, processes and the environment are often

	overlooked and must be considered for an effective risk assessment.
	***People** considerations include reviewing the organization structure and staff, and their documented responsibilities. The CIO/CPO/CSO documented responsibilities should be reviewed as well. Also, look at the IT security staff knowledge, continued education and ability to stay current. User security awareness and duties should be examined, including human resources knowledge of pre-employment, orientation, termination, and post-employment issues.*
	***Processes** include a review of the current documented policies, procedures, standards and guidelines, as well as the knowledge of the staff responsible for putting the appropriate processes in place. Flowchart and diagrams should be examined regarding the processes currently in place.*
	***Environmental** (physical security) includes a review of the physical facilities and controls (HVAC, IT room raised floors, fire compression, etc.). Security involving sensitive information should be examined by looking at physical record-keeping locations and procedures, as well as disposal policies for physical records and equipment (hard drives, tapes, laptops, etc.)*
Step 6:	***Analyze the Identified Risks***
	For each risk identified, a method should be composed to estimate the likelihood (probability) of a successful attack; frequency of the attack; and the impact of the attack. According to these estimates, the risks should be prioritized. This step will be the most demanding. (An example regarding sensitive information: a risk is identified whereas there are no procedures to follow when transferring or disposing of a laptop computer. The likelihood of the second-hand computer obtaining sensitive information would be very high since no one wipes the drive; the frequency, however is relatively low since turnover is low, computer procurements aren't current, and the laptops aren't disposed of often or don't change hands often. The impact although, could be astronomical depending on who obtains access to the laptop.)
Step 7:	***Identify Countermeasures to Reduce Risk to an Acceptable Level***
	There will most likely be various alternatives to securing potential risks. These alternatives should be evaluated and weighed against the priority of the risk assigned in Step 6. There will always be some risk; no security will be 100% in terms of practicality. However, questions to consider are the cost of the alternative v. the value of the asset (the priority placed on the risk), and the security of the asset v. the usability.
Step 8:	***Communicate the Risks***
	The findings and conclusions (priorities, alternatives, and countermeasure) should be compiled in a detailed report. The report should include the consequences of not implementing the desired countermeasure.
STAGE 3: Security Risk Assessment Follow-up	
Step 9:	***Assign Responsibility for Remediation***
	The countermeasures should be assigned to authoritative personnel, and reporting/tracking procedures put in place. Formulation of policies, procedures, standards, and guidelines should be assigned as well. The CPO/CIO/CSO should have oversight and final authority.
Step 10:	***Plan the Next Assessment***
	The IT security risks should be re-assessed on a regular basis and a policy should

	be constructed to schedule the frequency. Budgetary means should be provided for the frequent risk assessments. This will be the responsibility of the CPO/CIO/CSO to implement and adhere to.

The IT security risk assessment provides the framework to assess and implement the countermeasures to an acceptable risk, and to ensure sensitive information, critical equipment, and privacy issues are addressed. The applicable countermeasures and policies of the organization will provide the platform to ensure acceptable security.

Platform for IT Security: Policy

Just the mention of policy development gets the same reaction from even the most dedicated individuals as screeching sounds like fingernails down a chalkboard. Yet, without documented and authorized policies, no one has a platform to depend on, especially if sensitive information is exposed or privacy issues surface.

Implementing sound and thought-out IT security policies can be relatively new in the private business or home sector. "More than 60 percent of Fortune 500 companies do not have [IT security] policies," according to Linda Bramlett in the November 2002 SC Magazine article, *Chasing an Ounce of Prevention*."[13] This is not surprising though, with IT staff struggling to keep ahead of technical demands and the constant daily flux of vulnerabilities. Their time is spent on keeping the organization in productive operation. *Who has the time to document the security measures they do put in place?*

A complete and thorough documentation of IT security polices is not a simple task. Like risk assessments, there are numerous templates for guidance, IT consultants to analyze and write them, and additionally, software tools to automate the design, implementation and monitoring process. "These [policy software] tools help you manage the 'Lifecycle' of policy adoption by translating high-level guidelines into actionable and manageable rules on the device level."[14]

Instructions, templates, and assistance are available from many auditing firms or accounting websites (i.e., ITAudit.org), government publications, and technology journals and websites (i.e., SANS.org, SecurityFocus.com).
For example, SANS provides templates of action-specific policies in their "SANS Security Policy Project."[15] Concerning privacy issues, some helpful policy templates and examples from SANS includes: *Acceptable Encryption Policy, Acceptable Use Policy, Audit Policy, Information Sensitivity Policy,* and *Third Party Network Connection Agreement*; as well as guidance for complying with HIPAA.[15]

Assistance with IT security policies on technical issues can be found from the following:

- Internet Engineering Task Force (IETF), Network Working Group
  - *RFC: 2196 Site Security Handbook*[16]
  - *RFC: 2504 User's Security Handbook*[17]

- National Institute of Standards and Technology (NIST) Special Publications:
  - *SP800-27 Engineering Principles for IT Security (A Baseline for Achieving Security)*[18]
  - *SP800-14 Generally Accepted Principles and Practices for Securing IT Systems*.[19]

Constructing the Policies

NIST indicates that the "term *computer security policy* has more than one meaning,"[19] and introduces three different types of policy an organization should have. In essence, the computer security policy is used as a management directive to establish the security program, achieve its goals, and to assign responsibilities. The three types of policies as defined by NIST`[19], including privacy issue examples, are as follows:

- **Type 1: Program Policy**
  This higher-level policy consists of:
  1. Creating and defining the IT security program (defining resources/assets)
  2. Setting organizational strategic direction (defining the goals of the program)
  3. Assigning responsibility (implementation and monitoring)
  4. Addressing compliance issues including: requirements to establish the program and assignments, and specified penalties and disciplinary actions.

  In the Program Policy, the CPO/CIO/CSO would be assigned primary responsibilities of defining a program to ensure confidentiality of sensitive information and compliance with privacy-related regulations. The goals of protecting privacy assets would be clarified and a mission statement regarding due diligent in the protection of privacy concerns and sensitive information may be issued. The policy of classifying data would also be presented and the classifications defined. One example of the program policy could be illustrated by Privacy and Security Notices maintained on websites, as the one presented by Defense Technical Information Center (DTIC), *see* **Appendix A**.[20]

- **Type 2: Issue-Specific Policy**
  This midrange policy is characterized by:
  1. Addressing specific areas (topics of relevance; i.e., e-mail privacy)
  2. Requiring frequent updates (due to constant changes in technology)
  3. Declaring an issue (organization's position, applicability, roles and responsibilities, compliance, contacts)

  Policies of this type address specific subjects and are kept current with the constant flux in technology as deemed necessary. These policies would refer to expectations (or lack thereof), by: customers (i.e., trusting their social security number is kept confidential and not divulged to outsiders); employees (i.e.,

trusting their organization will not release their home phone number or address to anyone without permission), and employers (i.e., trusting employees use with PGP encryption on all classified information). Of course, sensitive and confidential information would be classified under a separate policy. Two examples of this policy would include an *Acceptable Use Policy* (*see* **Appendix B**) and a *Nondisclosure Agreement* (*see* **Appendix C**). All users handling sensitive information will be required to sign these documents.

- **System-Specific Policy**
  These detailed policies have the following attributes:
  1. Focus on decisions (actions deemed necessary to protect a system)
  2. Developed by management official (based on technical analysis)
  3. Vary from system to system (security objectives will range due to environmental and operational requirements, and acceptable risk)
  4. Expressed as rules (defining who, what, when, where, how)

  System-specific policies, like the issue-specific policy, are lower-level, but more technical and detailed according to the system being secured. These policies can be spelled out as rules and may rely on further documented procedures, standards, or guidelines. An example of the system-specific policy in accordance with maintaining security over sensitive information would be documentation instructing what classification level of data would require to have 128-bit encrypted format and to be backed up on a separate server (including who, what, when, and how).

  Another example of this type policy regarding privacy issues is a notification screen appearing each time a user accesses the network. This screen reminds the user that the computer and network are properties of the organization and that privacy is not to be expected. Notification that surveillance can be expected will be issued on this logon screen as well (*see* **Appendix D**).

- **All Types of Policies**
  Any of the three types of policies should be:
  1. Supplemented (i.e., procedures, standards, guidelines, checklists)
  2. Visible
  3. Supported by management
  4. Consistent

  In order to provide clear and concise and understandable guidance of expectations, policies must be thoughtfully documented and implemented according to the priority of risks as assessed.

Policies provide the guidance to achieve organizational IT security objectives, management directives, and expectations in order to minimize risks. To be effective, they must be well documented, distributed and understood. They can serve as a measure of compliance and meeting objectives. Yet they must be considered a "living" document. The risks, like the field of IT, are constantly changing.

Conclusion

In the ever-changing arena of IT, there are innumerable risks. One major factor affecting IT security risks is that of individual and entity privacy concerns of maintaining sensitive and confidential information. These privacy concerns can be attributed to customers, employees, partners, vendors/contractors, management, and the organization itself. Legal regulations and the organization as an on-going concern require the privacy issues to be addressed.

Organizational management must be attuned to these privacy issue risks. They must assess and prioritize them regularly to provide effective security countermeasures. This is best achieved through the consideration of privacy issues in an IT security risk assessment and the "living" policy. The IT security risk assessment can provide the framework, enabling the IT security policy to create a platform to communicate management's objectives and expectations.

APPENDIX A

Privacy and Security Notice

1. This World Wide Web (WWW) site is provided as a public service by the Defense Technical Information Center (DTIC®).

2. Information presented on this WWW site is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested.

3. For site management, information is collected for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

4. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with the National Archives and Records Administration's General Records Schedule 20 *(Electronic Records)*.

6. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

7. If you have any questions or comments about the information presented here, please forward them to us: bcporder@dtic.mil.

DISCLAIMER

Disclaimer of Liability: *With respect to documents available from this server, neither the United States Government nor any of its employees, makes any warranty, express or implied, including the warranties of merchantability and fitness for a particular purpose; nor assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed; nor represents that its use would not infringe privately owned rights.*

Disclaimer of Endorsement: *Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.*

Disclaimer for External Links: *The appearance of hyperlinks on this page does not constitute endorsement (by the Federal Government, Department of Defense, or the Defense Technical Information Center) of linked web sites or the information, products or services contained therein. For other than authorized activities, the Defense Technical Information Center does not exercise any editorial control over the information you may find at linked locations. External links are provided consistent with the stated purpose of this DoD web site.*

Defense Technical Information Center (DTIC) Policy & Security Notice[20]
Example of a program policy for maintained on the website.
http://www.dtic.mil/dtic/privacy.html

APPENDIX B

XYZ ORGANIZATION POLICY/PROCEDURE

Policy Number: XXX999 **Effective Date:** date
Revision Date: date

Subject: Acceptable Use Policy for Internet and E-Mail

Compliance Responsibility
The manager is responsible for ensuring that all employees are aware of the provisions of this policy, compliance by the employee is expected, and that inappropriate use of Internet and E-mail resources will result in disciplinary action including dismissal

.

Policy Maintenance: The XYZ Organization (XYZ) and XYZ Security Committee share the responsibility for the maintenance of this policy. This policy is to be adhered to by all agents and employees within XYZ. Employees are also to refer to their management's internal policy, which may have additional information or clarification of this XYZ policy. The XYZ Security Committee approves this Policy.

Policy:
XYZ furnishes the communications for users and acceptable practices must govern its use. This Acceptable Use Policy represents the set of guidelines to be followed when using communications or any other network equipment as a result of connection, including Internet and E-mail.

The acceptable use of Internet and E-mail represents the proper management of a business resource. Management is expected to work with employees to determine the appropriateness of using the Internet and E-mail for professional activities and career development. Using the Internet and E-mail for personal gain is prohibited.

This policy applies when XYZ Internet and E-mail resources are being used regardless of the time or location. Employees' use of electronic mail and the Internet will be monitored with the use of surveillance tools. Employees should have no expectation of privacy associated with E-mail, Internet or the information they store using XYZ resources.

Employee Responsibilities:

- Employees must use their access to the Internet and E-mail in a responsible

way, conforming to network etiquette, and any applicable laws or regulation.

- Copyright restrictions/regulations must be adhered to.

- Employees have the responsibility to notify management of any knowledge of breaches of this policy.

- Employees must represent themselves honestly through e-mail and Internet correspondence.

- Professionalism must be maintained as a representative for the reputation of XYZ.

Management Responsibilities:

- E-Mail and Internet use is for “appropriate business use" only.

- E-mails should contain a confidentiality statement for both employees and management.

- Management is responsible for their published information and actions of their employees.

Unacceptable Uses:

Use of XYZ Internet and E-mail resources is a privilege that may be revoked at any time for inappropriate conduct. Any abuse of acceptable use policies may result in revocation of access and disciplinary action up to and including dismissal. Examples of inappropriate conduct include, but are not limited to:

- Using the Internet and E-mail for personal gain or personal business activities.
- Engaging in illegal activities or using the Internet for any illegal purposes, including unlawful access to a computer. This includes malicious use, spreading of viruses, and hacking. Hacking is gaining or attempting to gain unauthorized access to any computers, computer networks, databases, data or electronically stored information.
- Transmitting materials that are reasonably likely to be perceived as offensive to others based on race, national origin, sex, sexual orientation, age, disability, religious or political beliefs.
- Using abusive or objectionable language in messages.
- Knowingly visiting pornographic or illegal sites, disseminating, soliciting or storing sexually oriented messages.
- Use of false or misleading subject headers and presentation of information in the distribution of E-mail or on the Internet as a misrepresentation of a user’s identity.

- Distributing, forwarding or sending chain letters or unsolicited E-mail.
- Creating or maintaining a personal web page on or from a XYZ device.
- Using any tools to distribute personal information that constitutes an invasion of personal privacy.
- Non-business activities that may cause congestion or disruption of networks or systems including, but not limited to, Internet games, online gaming, unnecessary Listserve subscriptions, E-mail attachments, chat rooms, or instant messaging on the Internet.

I, _____, certify that I have read and understand this Agreement and the restrictions contained therein.

_____ _____

Contractor, Vendor, Employee Name (Please Print) *Organization Represented*

_____ _____

Contractor, Vendor, Employee Signature *Date Signed*

_____ _____

XYZ Manager *XYZ CIO Signature*

_____

Userid assigned

APPENDIX C

XYZ Form #
Date

XYZ Organization
Acknowledgment of Confidentiality
And Non-disclosure Agreement

This Acknowledgment of Confidentiality and Non-disclosure Agreement outlines the responsibility of the Contractor, Vendor or Employee regarding the confidential nature of access to the XYZ Organization (XYZ) data resources.

The Contractor, Vendor, Employee may be granted appropriate access to XYZ pertinent data resources needed to fulfill his/her employment or contractual agreement. The Contractor, Vendor, Employee must maintain confidentiality and integrity of data and consult with, and follow classified information policies.

The Contractor, Vendor, Employee agrees that all creations made and works developed by him/her, or under his/her direction in connection with the XYZ contractual agreement is the property of XYZ and all copyrights and other proprietary interest belong to XYZ.

The Contractor, Vendor, Employee agree not to use or disclose any Confidential Information regardless of classification of XYZ, or its agents, without written permission from XYZ except as required to perform duties for XYZ. *Confidential Information* is data, information, or material that is sensitive in nature, (manual or electronic) and not generally known to the public. It may include any scientific or technical information, design, formula, process, or software (manual or electronic) that is valuable and not generally known to the public.

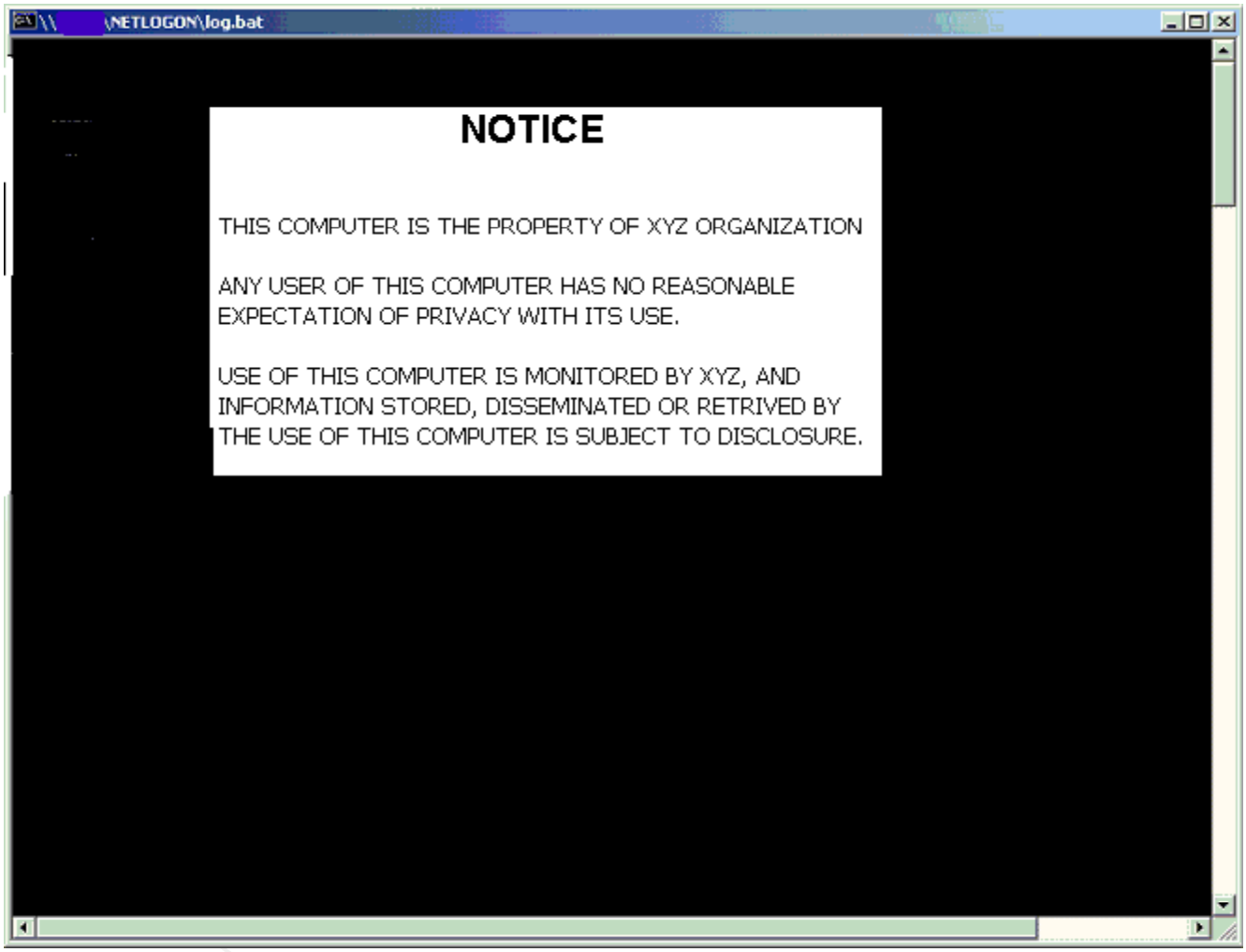
Violations of this Agreement will result in immediate termination of the Contractor, Vendor, and Employee. Upon the request of XYZ, and in any event, upon the termination of the employment or contract of the Contractor, Vendor, Employee; any confidential information (manual or electronic) pertaining to XYZ, including all copies thereof, are to remain with XYZ.

I, _____, certify that I have read and understand this Agreement and the restrictions contained therein.

_____	_____
Contractor, Vendor, Employee Name (Please Print)	*Organization Represented*
_____	_____
Contractor, Vendor, Employee Signature	*Date Signed*
_____	_____
XYZ Representative	*XYZ CIO Signature*

APPENDIX D

Example of Notification Screen at Logon



References

[1] Henderson, Harry. Privacy in the Information Age. New York: Facts on File, Inc., 1999.(pages 15-17).

[2] Keating, Stephen, and Smith, Richard M. "Top US Privacy Stories of 2000." Information Systems Control, Vol.3 (2001):29-31.

[3] Total Information Awareness (TIA) System. Information Awareness Office homepage. URL: http://www.arpa.mil/iao/TIASystems.htm (March 3, 2003).

[4] Security News. "Employees Looking for Tighter Security ." SC Magazine June 2002 (2002):18.

[5]Associated Press. "Latest ID Theft Scam: Fake Job Listings." CNN.com/Technology March 1, 2003. Url: http://www.cnn.com/2003/TECH/internet/02/28/monster.theft.ap/index.html (March 3, 2003)

[6] National Post's Financial Post & FP Investing. "Crucial Data Rescued After Hacker Raid: Key Server Stripped: 'It Was Akin to Hacking into the Pentagon'." OSAC (Overseas Security Advisory Council) February 24, 2003.
URL: http://www.ds-osac.org/view.cfm?KEY=7E4454404050&type=2B170C1E0A3A0F162820 (March 3, 2003).

[7] Fisher, Dennis. "ATM Encryption Weakness Leaves Accounts Vulnerable." eWeek March 3, 2003.
URL: http://security.ziffdavis.com/print_article/0,4281,a-38048,00.asp (March 5, 2003)

[8] Reuters. "British Intelligence PC Stolen." Wired.com/News March 2003.
URL: http://www.wired.com/news/business/0,1367,35185,00.html (March 4, 2003).

[9]. SANS.org. "Millions of Credit Card Numbers May Have Been Compromised." SANS NewsBites Vol.5, No.7 (Feb. 19, 2003). URL: http://www.sans.org/newsletters/newsbites/vol5_7.php (February 19, 2003).

[10] Leyden, John. "Personal Storage Sites are the Latest "Security Risk'." The Register (March 6, 2003).
URL: http://www.securityfocus.com/news/2919 (March 7, 2003).

[11] Doughty, Ken. "Business Continuity: A Business Survival Strategy." Information Systems Control, Vol.1 (2002):28-36.

[12] Veridyn, Inc. "The 10 Essential Steps to Effective Security Risk Assessments."
URL: http://www.veridyn.com/downloads/SRA_wp.pdf (February 17, 2003) .

[13] Bramlett, Linda. "Chasing an Ounce of Prevention." SC Magazine November 2002 (2002):74.

[14] Briney, Andrew. "Automating Policies." Information Security October 2002 (2002):54-56.
URL: http://www.infosecuritymag.com/2002/oct/policytools.shtml (January 18, 2003).

[15] SANS.org. "The SANS Security Policy Project." URL: http://www.sans.org/resources/policies/ (January 18, 2003).

[16] Fraser, B. "RFC:2196 Site Security Handbook." Internet Engineering Task Force. September 1997.
URL: http://www.ietf.org/rfc/rfc2196.txt?number=2196 (February 17, 2003).

[17] Guttman, E., Leong, L., Malkin, G. "RFC:2504 User's Security Handbook." Internet Engineering Task Force. February 1999. URL: http://www.ietf.org/rfc/rfc2504.txt?number=2504 (February 17, 2003).

[18] Stoneburger, Gary., Hayden, Clark., Feringa, Alexis. "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)." NIST Special Publication 800-27. June 2001. URL: http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf (February 17, 2003).

[19] Swanson, Marianne., Guttman, Barbara. "Generally Accepted Principles and Practices for Security Information Technology Systems." NIST Special Publication 800-14. September 1996. URL: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf (February 17, 2003).

[20] Defense Technology Information Center (DTIC). "Privacy and Security Notice." URL: http://www.dtic.mil/dtic/privacy.html (March 4, 2003).