A Energy Company – IT Department Policy Audit

Joette Damo

Western Governors University

Table of Contents

A Energy Company – IT Department Policy Audit

Introduction

I conducted an audit for A Energy Company IT department policy specifically to audit the policy evaluation of ethical issues with discussions in unethical use internally and unethical uses externally. The second of policy evaluations were made on security issues with further discussions on security threats internally and security threats externally. Updated company policies required rewording specific policy statements. Discussions were made on mitigation of unethical uses. Final discussions were made on mitigation security threats.

A. Policy Evaluation – Ethical Issues

The first policy in discussion will be the “Employer Security Policy” in how policy relates to the acceptable use of company technology and data for both internal and external parties given access to the technology and data for business purposes. In the policy new employees will receive training on both computer and organizational security. After this training, the new employee must agree to requirements of security before receiving user ID and security pass. All computer activity by the new employee will be tracked by this user ID. The training, user ID, and security pass were effective ethical policies ensuring that the new employee is aware and can be held accountable for ethical behavior. In the “Employer Security Policy” is states that email accounts can be reviewed at any time; but an exception can be made when a personal mail is sent from the work account marking the email as personal can be set aside during the monitoring process. Yet on the other hand the policy suggests email etiquette to portray professional image for the company. I do find this policy of email exception as an unethical ineffective statement because of possible threat of unethical behavior of the employee for misuse of A Energy’s business documents. Another statement given by the “Employer

Security Policy" states that all computers that VPN access requires authentication with an approved user ID and password to tunnel through computer firewall when using internal and external network. This policy ethical statement could be possible unethical threat because it does not impose procedures for authentication nor provide protections from unsecure connection through the internet, firewall, and or encryption of data in transmission.

The second policy "Data Security Policy" promotes ethical policy for the privacy of employees and clients ensuring protection of corporate and client data from security breaches. This privacy is an effective policy statement when upper management effectively communicates and promotes such ethical policy. In another section of the "Data Security Policy" statement was made on public/unclassified data in which employees may send or communicate such data with anyone inside or outside. I find such statement ineffective policy statement because of possible threat to external users or clients for data ethical concerns like privacy or else data breaches. Yet on the other hand another policy statement conflicts the above statement stating access to such data may be limited to specific department and cannot be distributed outside of work. This policy statement poses an internal ethical threat of an employee compromising personal accountability if the employee discloses private information to even a current employee of the company. The policy states that is the responsibility of everyone to protect the data. The policy states management personnel are responsible for ensuring that team members who directly report to them understand the scope of the "Data Security Policy" with implications of unethical behavior. The policy ensures enforcement of data security through access controls, strong passwords, system monitoring, and trend analysis; furthermore, after employee training the employee acknowledges the effective policy by endorsing the employee acknowledgment statement.

The third policy discussion on "Accounting Security Policy" in how it relates to acceptable use of company technology and data for both internal and external parties given access to the technology and data. The policy is provided in training orientation to the new employee after the acceptance of the job offer. In the training it specifies that audits for compliance are budgeted annually to ensure ethical enforcement of the policy. The accounting controls do not permit or deny access for the purpose of collecting resource usage information on trend analysis, auditing, billing, or cost allocation; the employee has ethical personal accountability for such controls. Furthermore, the policy states that information about users of A Energy website and network collects, stores, secures to protect the user's personal information and privacy. For this policy statement I foresee a threat external unethical behavior compromising the privacy of personal information through factors like privacy violations or else likelihood of data not encrypted and hackers stealing data. The last policy statement for "Accounting Security Policy" is that A Energy's website uses cookies to transfer pieces of information to user's hard drive to store settings for record keeping purposes. The information from cookies tracks several types of activities. I find this unethical policy statement with possibility of a threat to both A Energy and the user because of privacy issues and internal unethical behavior compromising data by anyone.

A1. Unethical uses – internal

There are two potential internal unethical uses by employees of A Energy. First in the "Employer Security Policy" (reference 1) it states that email accounts can be reviewed at any time; therefore, an exception can be made when a personal email is sent from work account such email can be marked as personal to avoid the email being opened during the monitoring process; yet the polity also states email etiquette is suggested to portray the professional image for A

Energy. The internal unethical behavior is when the employee uses the company email for personal matters. According to the reading “Legal and Illegal Activities” (Brennan, 2004, chp. 16) the business has a right to monitor employees accordingly under current law, employees are held liable if the employee as an agent of employee uses employer’s computer for improper purposes in illegal matters. The second internal unethical behavior of the A Energy employee would be in the “Data Security Policy” (reference 2) in the statement depicting employees may not disclose private data to anyone who is not a current employee of the company. The threat of internal unethical behavior would be an employee disclosing such data to current employee who is trying to get information for insider data information not pertinent to his/her job position. The employee disclosing such information would be compromising the personal accountability of ethical behavior to A Energy along with trust, honesty, and loyalty. According to the reading “Personal Accountability” (Harold, 2007, chp. 32.6.1) an employee can be breaching accountability based on the standard of product prevention loss due to solicited disclosure.

A2. Unethical uses – External

There are two potential external unethical uses by employees of A Energy. First in the “Data Security Policy” (reference 3) for public/unclassified data employees may send or communicate this data with anyone inside or outside of the company. In this case what happens when an employee gives information to a person outside of the company? According to the reading “Compliance with data management laws” (Brennan, 2004, chp. 15) states that data has no ethics, therefore; a data set does not care how it is used. It will not stop if span occurs nor share personal details with third parties. The reading states the CIO is the one who develops guidelines on how to manage data; therefore, company policies should clearly state types of data being collected with the appropriate logistics. The harm in this example would be if an employee gives the data to an external source and in turn that external source claims the data has compromised their business in general terms. The second potential external unethical use by an employee from the example from the "Accounting Security Policy" (reference 4) statement about information about users of services provided in A Energy's website and network is collected, stored, and secured to protect the user's personal information addressing in privacy of the external user. According to the reading "Compliance with data management laws" (Brennan, 2004, chp. 15) the reading states that security and privacy are not the same secure systems which are needed to ensure "privacy." The CPO Chief Privacy Officer must work with the CSO Chief Security Officer to work out the details ensuring policy of privacy. Likewise, there are few software tools that exist to help businesses manage privacy issues which has damaged businesses' reputations by failing to carry such privacy policies. In this case an employee could pose external unethical behavior by selling privacy information to external source and that user uses privacy information to harass A Energy.

B. Policy Evaluation – Security Issues

Discussions will be made on security issues for the three policies of Employer Security, Data Security, and Accounting Security. First, I will start off with the "Employer Security Policy" security issue statement that all the hardware including the computers, projector, external hard disk drives, and printers contain tracking mechanisms in case of loss or theft. Also, that internet browsing has managed to safeguard bandwidth with certain internet site are blocked using web filtering software. There is a security threat in the above statement because according to the reading "A new Breed of Hacker Tools Defenses" (Harold, 2007, chp. 73) there is a possibility of hacker attack on insufficient bandwidth on computer system by external forces. Also, according to reading "Insight to Intrusion Prevention System" (Brennan, 2004, chp. 16) states that intrusions on information system security are attempts or actions of unauthorized entry into the system stating the best defenses is firewall step in security for IT network which performs to counter intrusion attempts in IT system or network. The "Employer Security Policy" statements were made on the physical securities to the environment such as monitoring with digital camera to entrances to the building following movements of employee such monitoring is structured to respond to any unauthorized access to the facility and network. Monitoring of the location and assets of A Energy can detect any security threats which worked effectively. The policy made statement about the confidentiality of trade secrets that are essential for a competitive edge whereas every employee must help to protect the company. There is a possibility of internal security threat in which unauthorized access by someone who can cause the loss of sensitive information such as trade secrets by information tampering or else use of malware. Controls for detecting loss of trade secrets can be data classifications and handling procedures for the sensitive information plus encryption for sensitive information such as trade secrets. Another security issue discussion statement would be that of passwords must be changed every 90 days that must be a minimum of eight characters in length and must contain at least three of the four following like a capital letter, lowercase letter, a symbol, or a number. This statement poses an internal security threat according to the reading "Hacker Tools and Techniques" (Harold, 2007, chp.72) in this section "The Art and Science of Password Cracking" the defense for password security is for the password with greater than eight characters with security practitioners checking system passwords periodically using password cracking tools.

The next section for discussion is security issues for the "Data Security Policy." The policy made a statement that privacy commitment to protecting personal data yet states that employees may only share confidential data with relative department or else name distribution.

There is an internal security threat of privacy when the employee does not give choice or else get consent for opting in or opting out on privacy data information to be used by employee of A Energy. There should be security to secure against loss for unauthorized access, destruction, or disclosure according to the reading “Business Requirements for Enabling Privacy” (Harold, 2007, chp. 182). The last issue for security for internal secret/restricted sensitive data would be threat to security when such data is not encrypted when unauthorized access user stole secret/restricted sensitive data. According to reading “Wireless Security” (Harold, 2007, chp. 167) states that weak encryption control and inefficient security have forced corporations to investigate add-in solutions.

The final third section for discussion is “Accounting Security Policy” security issues. This policy states that information about users of services provided by A Energy website and network collected, stored, and secured to protect the user’s personal information and privacy. A Energy must abide by law such as GLBA Gramn Leach Bliley Act 1999 which states that the law required both stored and transmitted information be encrypted if security cannot be guaranteed. The policy made a statement about use information is analyzed for billing and cost allocation to external and internal costs center; therefore, usage information is shared only in aggregate to evaluation to appropriate for management staff for confirmation of acceptable use for such policy which would not pose any security issue. Lastly the “Accounting Security Policy” made a statement regarding data transmissions that are not completed through an SSL connection between the website and the user may not be completely secure with the user must bear the risk of data transfer via the internet. The policy poses an external security threat because such transmissions should be made via internet through a firewall filtering data to be secure.

B1. Security Threats – Internal

There are two potential internal security threats by employees of A Energy. In the policy “Employer Security Policy” (reference 5) states that the confidentiality of trade secrets is essential for a competitive edge where employee must help to protect the company. There is a possible internal security threat imposed by an employee wanting to personally sell a trade secret to a competitor of A Energy in which such an employee would be accountable for unethical behavior causing a security threat. The second security threat would be within the “Data Security Policy” (reference 6) which states a privacy policy outlines commitment to protecting personal data in which employees may only share confidential data with associated department or name distribution. In a security breach a threat which an employee violated such privacy shared privacy personal information for profit, for example with another employee such an employee should be personally accountable for posing threat on privacy information.

B2. Security Threats – External

There are two potential external security threats by employees of A Energy. In the policy “Employer Security Policy” (reference 7) states that hardware which includes computer, projector, external hard disk devices, and printer contain tracking mechanisms in case of loss or theft whereas internet browsing has managed to safeguard with bandwidth with selected internet sites blocked using web filtering software. There is threat when an employee externally when not at work uses hacking tools to alter the bandwidth or else access the computer on an unauthorized segment to compromise the firewall proxy for filtering data. The second potential security external issue was stated in the “Accounting Security Policy” (reference 8) states that data transmissions that are not completed through an SSL connection between the website and the user may not be completely secure, and the user must bear the risk of data transfer via internet. The employee externally can be such the user with knowledge can access the information through SSL and alter the transmission which causes losses to A Energy product revenue or cost of products.

C. Updated company policies by internal and external users

1. Employer Security Policy

   Section – Network and resource usage monitoring

   E-mail accounts can be reviewed at any time. Email and voicemails are business documents. (reference 1)

2. Data Security Policy

   Section – Data Classifications #2 Private

   Employees may not disclose private data to anyone. (reference 2)

3. Data Security Policy

   Section – Data types #1 Public/unclassified

   Employees may not send or communicate a public/unclassified piece of data with anyone inside or outside of the company. (reference 3)

4. Accounting Security Policy

   Section – in the middle of page

   Information about users of services provided by A Energy website and network is collected, stored, and secured to protect the user's personal information and privacy secured through encryption. (reference 4)

5. Employer Security Policy

   Section – Network and resource usage monitoring

   Confidentiality of trade secrets is essential for competitive edge; all employees must secure the integrity of trade secrets from harm to protect A Energy's assets.

(reference 5)

6. Data Security Policy

   Section – Data classifications #3 Confidential

   Employees may not share confidential data prior approval from upper management is needed first with advisement. (reference 6)

7. Employer Security Policy

   Section in middle of first page

   All hardware including computers, projectors, external hard disk drives, and printers contain tracking mechanisms in case of loss or theft; also, hardware system must have anti-virus, firewall, and encryption software applications for securing data. (reference 7)

8. Accounting Security Policy

   Section - in middle of second page

   Those data transmissions that are not completed through SSL connection between the website and user not secure use encrypt data for data transfer to reduce risk via internet. (reference 8)

C1. Mitigation of changes

Mitigation of the four identified unethical uses of computer technology and data promotes risk mitigation as follows:

- Access control improved such as intrusion detection.
- Assessment such electronic access history.
- Protection through prevention.
- Controls:
- Security and safety conscious employees.

- Routine audits.
- Awareness of warning signs.
- Preventative maintenance necessary.
- UPS
- Encryption
- Storing backup media offsite
- Strong authentication access controls

These risk mitigation controls and assessments can be applied to reference 1 for email as business documents for routine audits. In reference 2 for private data through protection through prevention. Reference 3 public/unclassified data in need for encryption. Reference 4 about information for access control improved intrusion detection.

C2. Mitigation of changes

Mitigation of the four identified security threats to company technology and data promotes mitigation plan for security risks as follows:

Threat opportunities mitigated good security practices, proper training, regular patching, virus updates regarding reference 7 regarding system hardware that must have anti-virus. Firewall, and encryption software applications for securing data. The need to define a security architecture through accountability, assurance, authentication, availability, confidentiality, identification, and integrity appliable to references 5, 6, 8. Preventative controls can be made as backups of data, applying critical patches (software), use of firewalls as in reference 7 for system hardware with data encryption for securing with anti-virus, addressing issues for wireless attacks such as in reference 5 hackers can access trade secrets. The issue of privacy should be mitigated through controls of notice, choice/consent by user, access, security, limitation, accountability, traceability, and anonymity with pseudonymity.

References

Brennan, L. L., & Johnson, V. (2004). *Social, Ethical and Policy Implications of Information Technology*. IGI Global.

Harold F. Tipton, Micki Krause - 85h 24m85hours 24minutes Publisher: CRC Press © 2007 Information Security Management Handbook, Sixth Edition, Volume 1