Hardening Corporate Information Security: Managing the Human Element

By George J. Silowash

Norwich University
Master of Science in Information Assurance Candidate June 2007

——

Seminar 3 Final Paper

Adjunct Professor Ed Piper

Executive Summary

Securing the information infrastructure is an ongoing process. The company must have the necessary support from senior management to implement a successful security program. A security program contains several key elements:

- Assessments
- Policies and Procedures
- Security Awareness Training
- Audits

Assessments allow an organization to determine its current posture and identify areas that need attention. Assessments cover a broad range of systems and are generally informal in nature.

After assessing the company's current security posture, the necessary policies and procedures must be developed and implemented. These policies will govern how an organization responds in a given situation. They also allow employees to understand the company's position on various topics.

Employees must receive the proper training in order for the policies and procedure to be successfully implemented. Training demonstrates to staff members the need for the policy as well as what to do in a given situation. Training must be ongoing. A successful security awareness program will have employees thinking about security continuously. They will be more security conscious and therefore increase the security posture of the company.

We must make sure that the processes we have in place to protect our infrastructure are working. An audit will allow us to determine if everything is functioning as it should. It will also identify areas where corrective action is need.

The above process is ongoing. It is repeated and the necessary corrective measures are implemented. This ongoing process allows an organization to be proactive in its security initiatives rather than only reacting when a security issue arises.

The policies and training modules contained herein are just the beginning foundation for a security program. These policies identify areas that are of concern to the company. When coupled with security awareness training, these policies will go a long way to increasing security. Further policies and training modules must be developed to address other areas of concern within the organization.

The company will have an improved security posture once the proper policies, procedures, and training are in place. The ongoing security process will enable us to take an active role in protecting the information infrastructure.

TABLE OF CONTENTS

The Ongoing Security Process

Bruce Schneier stated "Security is a process, not a product."[1] Organizations must be continuously involved in security. There are several steps in the security process:

- "Start with risk assessment
- Create appropriate information security policy
- Determine what procedures are required to implement the policy
- Put procedures in place
- Make employees aware of the policies
- Train employees in the procedures
- Use psychology, employment practices, [and] ethics to encourage behavior supportive of policies
- Audit to assess how well security is working
- Revisit risks and modify policies as needed"[2]

Security policies and awareness training are just part of the security process. To ensure that the process is working and to fully understand the information infrastructure, audits and assessments are needed.

> "To audit a system you must first map out the system, determine its size, scope, boundaries and functions. Then you document the controls that exist within the system. Next you attempt to determine whether or not the controls are adequate and effective. Beyond that, you must decide if the controls have been by-passed."[3]

Auditing and assessing a system are very similar. However, assessments are less formal and cover a broader scope. Generally, an assessment is process that determines the state of various systems at a given point in time.[4] "Auditing is both the process of checking to see if things are as they should be, and the process of making things as they should be. Audit controls are a way to prevent humans from cheating or making errors."[5]

An audit and assessment process will verify that security policies and procedures that are in place are functioning as they should. It will also identify any deficiencies with the current systems. Currently, the Information Systems Group utilizes assessments to

[1] Schneier, B. (2000, May 15). Computer Security: Will We Ever Learn?. Retrieved August 9, 2006, from http://www.schneier.com/crypto-gram-0005.html

[2] Cobb, S. (2006). PREVENTION: Human Factors Auditing, assessing, and the cycle of protection. Retrieved August 17, 2006 from http://norwichwebct.embanet.com/SCRIPT/MSIA8_Content_Repository/scripts/student/serve_page.pl/MSIA8_Content_Repository/8_msia_sem3/MSIA_S03_W10_webct.html?1948742616+1146691302+OFF+8_msia_sem3/impatica/MSIA_S3_W10_SLIDES.zip+

[3] Cobb, S. (2006). Audit, Assess, Test – What's the Diff? Retrieved August 17, 2006 from http://norwichwebct.embanet.com/SCRIPT/MSIA8_Content_Repository/scripts/student/serve_page.pl/MSIA8_Content_Repository/8_msia_sem3/MSIA_S03_W09_webct.html?1948742616+1146691301+OFF+8_msia_sem3/pdf/MSIA_S3_W09_LECTURE.PDF+

[4] Ibid.

[5] Ibid.

identify issues within the various computer systems. The results of these assessments are then shared with management to allow improvements to be made in the affected systems.[1]

The Information Systems Group utilizes its own auditing methods. The audits enable the ISG to identify problems within the organization before the annual external audit occurs. However, a conflict of interest exists. If a deficiency exists within the audited systems, the ISG may be reluctant to report it to management. In addition, the ISG may overlook the deficiency so that it goes undetected by management. The ISG should use the same auditing process and techniques as the external auditor. This will allow for discrepancies to be found and addressed.[2] Furthermore, the ISG must be encouraged to report security issues to management no matter the size. Doing so increases the company's security posture and employee morale.

Due to the limited resources of the company, it is suggested that a peer review team be formed consisting of members from the different departments in the organization. This peer review team can be used to review each department's work and provide audits or assessments. The team can also discuss new ideas that will strengthen the overall information infrastructure.

> "This team could meet once a month to discuss various company projects and their respective departments in order for others to provide feedback to each other about possible problems or enhancements. There should be minimal cost to start such a group, and the impact on employee workloads should be limited."[3]

A peer review team will allow the various departments within the company to discover flaws in the information infrastructure and allow the problems to be addressed before an external audit is conducted.

To have a successful security program, assessments must be conducted to fully understand the information infrastructure. Policies and procedures must then be developed and implemented. Awareness programs and training are needed to make sure employees fully understand the policies and procedures. Audits must then be conducted to see how well security measures are working. The results of these audits must then be used to implement changes. This process repeats as any environment is never completely free from security issues.

[1] Silowash, G.J. (2006) Auditing and Assessing Computer Systems. Norwich University MSIA Seminar 3, Week 9 Essay

[2] Ibid.

[3] Ibid.

Policies

Policies are designed to help employees understand what is and is not acceptable within an organization. Without policies, there are no guidelines and employees will not know what the leaders of the company expect from them. Essentially, policies are the "laws" within any company.

Policies are also required to protect the company from legal issues that may arise. When a company has a set of comprehensive policies in place, they are protecting themselves and it shows due diligence on behalf of the management of the company.

> "Policies define the position of a company on various issues. They also lay the foundation for training and define the organization's response to a violation of policy. Many organizations are required to abide by government regulations and therefore are required to have certain policies in place. Companies that implement policies for not only information systems, but for the other facets of the organization, demonstrate due diligence necessary for the protection of the company's employees and assets."[1,2]

Many laws also require companies to have guidelines in place. For example, the Health Insurance Portability and Accountability Act (HIPAA) requires policies and procedures be in place to prevent, detect, contain, and correct security violations.[3]

Even though an organization may not be required to comply with regulations regarding data security, it is in the organization's best interest to do so. If a company faces legal action, attorneys will compare security of the organization to accepted standards.

> "Should attorneys, public or private, decide to proceed with action against your company, they will try to establish that your security was not up to par. The best way to do this is a comparison with some accepted standard."[4]

Therefore, it is inherent that a company have policies in place to mitigate legal issues and to provide guidance for employees.

[1] Silowash, G.J. (June 2006). *Policy Presentation*, Norwich University MSIA Seminar 3, Week 1 Paper

[2] Kabay, M. E. (2002). Security Policy Guidelines. In S. Bosworth, & M. E. Kabay (Eds.), Computer Security Handbook (4th ed., pp. 28.1-28.22). New York, NY: John Wiley & Sons, Inc.. (p. 28.2)

[3] Cobb, S., & Cobb, C. (2006). *Dust Off Those Data Security Policies.* Retrieved July 27, 2006, from http://norwichwebct.embanet.com/SCRIPT/MSIA8_Content_Repository/scripts/student/serve_page.pl/MSIA8_Content_Repository/8_msia_sem3/MSIA_S03_W01_webct.html?1948742616+1146691293+OFF+8_msia_sem3/pdf/MSIA_S3_W01_LECTURE

[4] Ibid. (p. 3)

Management Support

Policies, like other company initiatives and programs, require support from management in order to be effective. When any policy is changed, management must announce the change. This shows support for the policy and not just a request by a particular person or department.[1]

> "Security is the result of corporate culture; therefore, management practices are critically important for successful information protection."[2]

Senior level management helps to define corporate culture. Their actions speak volumes to their peers and fellow coworkers. Employees look to their leaders for inspiration and guidance. Therefore, it is critically important that management adhere to information infrastructure guidelines. Managers who side step policies create security holes and do not lead by example. This undermines the company's information infrastructure strategy and demonstrates a lack of management support. Management must abide by the same policies as do all other employees.

Policy Design

Policies have the inherit trait of being lengthy and uninteresting. For this reason, it is important to include a brief policy summary so that employees can quickly find what they need.[3] This also allows them to quickly understand the company's position on a particular topic. However, this does not preclude the need for detailed policies. Detailed policies address specific company needs, while summaries convey the main ideas of the policy. Therefore, it is important to present both a summary and detailed policy.

People must also understand why the policy is needed.

> "Few people like to be ordered about with arbitrary rules. Trying to impose what appear to be senseless injunctions can generate a tide of rebellion among employees. It is far better to provide explanations of why policies make sense for the particular enterprise."[4]

Policies should contain an explanation as to why it is needed. This demonstrates to the employees how it fits into the company's information infrastructure strategy.

[1] Kabay, M. E. (2002). *Security Policy Guidelines*. In S. Bosworth, & M. E. Kabay (Eds.), Computer Security Handbook (4th ed., pp. 28.1-28.22). New York, NY: John Wiley & Sons, Inc..

[2] Kabay, M. E. (2002). *Employment Practices and Policies*. In S. Bosworth, & M. E. Kabay (Eds.), Computer Security Handbook (4th ed., pp. 31.1-31.14). New York, NY: John Wiley & Sons, Inc..

[3] Kabay, M. E. (2002). *Security Policy Guidelines*. In S. Bosworth, & M. E. Kabay (Eds.), Computer Security Handbook (4th ed., pp. 28.1-28.22). New York, NY: John Wiley & Sons, Inc..

[4] Ibid. (p. 28.17)

Policy Presentation

Polices do not need to take the common, everyday form of pages in a thick manual. Rather, organizations have many options for presenting policies at their disposal. Many organizations, such as ours, have an extensive Intranet. All policies can be converted to hypertext to allow employees to browse and reference policies easily. Other options include presenting policies in a multimedia format such as Adobe Flash.[1]

One of the main advantages to supplying policies using an electronic method is the ability to keep all policies updated. This also ensures that employees have access to the latest information to make an educated decision. Policies presented on the company Intranet eliminate the need to print and distribute an employee manual. They also eliminate the need to ensure that every employee has an updated policy manual.[2] Rather, employees can sign a statement indicating that they have received and read the policies on the Intranet and agree to review them whenever major changes are announced.

Policy Development

Rather than taking a reactive approach to security policy, the company must develop additional security policies in order to protect the information infrastructure. The policies contained in this document provide a starting point from which other polices can evolve. The company must carefully examine other sources for policies. This will allow the organization to become proactive rather than reactive. Typically, a policy is developed in response to something that has happened in the past. However, if the company reviews other sources of policies, it will have a more comprehensive set of guidelines to follow should a security incident occur. Other sources include:

- Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management by Thomas R. Peltier (ISBN: 0849311373)
    - This book provides a guide for developing security policies and a security awareness program. Sample policies are included as well.

- The SANS Institute Policy Project
    - The SANS Institute has a website dedicated to policy templates that it and others have developed. The templates cover a wide range of topics, many of which can be incorporated in the company’s security policy initiatives. Policies can be viewed at: http://www.sans.org/resources/policies/

- Computer Security Handbook, Fourth Edition edited by Seymour Bosworth and M.E. Kabay (ISBN: 0471412589)

[1] Kabay, M. E. (2002). *Security Policy Guidelines*. In S. Bosworth, & M. E. Kabay (Eds.), Computer Security Handbook (4th ed., pp. 28.1-28.22). New York, NY: John Wiley & Sons, Inc..
[2] Ibid.

  - The Computer Security Handbook includes many chapters about security policies and security awareness training. The book also covers many other facets of infrastructure security.

- The Art of Deception by Kevin D. Mitnick and William L. Simon (ISBN: 076454280X)
  - Kevin Mitnick offers a different perspective on security policies. Mr. Mitnick was a former computer hacker. His book provides realistic scenarios and advice on how to prevent it from happening to you. The book also includes suggested security policies.

Another good source to derive security policies from is ISO17799.

> "ISO/IEC 17799:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management."[1]

This international standard will provide the framework for developing security policies. It should be noted that the above book by Thomas R. Peltier includes information regarding the ISO17799 standard.

Sample Policies

The following policies are sample policies that the organization is currently lacking. Each policy addresses a security concern within the company. The policies start with a brief summary, followed by the detailed policy, and conclude with a detailed explanation of the policy. The detailed explanations of the policy are also suitable for inclusion in a security awareness training program.

There are also corresponding modules for some of the policies in the training section of this document that provide training suggestions as well as further commentary that can be included as part of the organization's security awareness training initiatives. Some policies also contain a slideshow presentation that is included as part of the appendices of this document.

The collection of policies and training modules in this document are not a complete solution in itself. Many additional policies and training modules are needed in order to have an effective security program. Some of these policies reference other documents

[1] International Organization for Standardization (2005). ISO/IEC 17799:2005 Retrieved August 15, 2006 from http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3=

that must be created in order to have a complete policy. This collection of policies was chosen to offer the organization a place to start. They also consist of policies that were identified by the Information Systems Group as having the most need. Additional policies and training materials can be modeled after those presented here. Every policy is a living document that must be reviewed and updated on at least an annual basis; these are no exception. These policies have been tailored to the company; however, they can be expanded upon to fill any void that management identifies.

Information Classification Policy Summary

The company utilizes various types of information to conduct business on a day to day basis. All of this information, in the form of printouts, files, and other media must be classified into four distinct groups in order to ensure that only authorized individuals have access to the information. These classification groups are:

- Public
- Internal
- Private
- Confidential

- Public information is any information that can be shared with anyone inside or outside of the company. Generally, this includes information that could be obtained from a public source, such as the media.

- Internal information is information that can be given to any company employee, contractor, or vendor. Contractors and vendors require a valid, signed confidentiality agreement on file. Information of this type is used in the everyday business of the company. Examples include cost center codes and phone directories.

- Private information is only to be used within the organization and cannot be shared with any third party (vendor, contractor, etc.) even with a valid confidentiality agreement. This information is sensitive and can only be shared with employees with a genuine need to know. Examples include salary history and health benefits.

- Confidential information is highly sensitive, and if it is disclosed to a third party, it may bring irreversible damage to the company, its reputation, its clients, and other stakeholders. Information of this type is shared with only a limited number of people with a genuine need to know. Examples of Confidential information include financial statements and business or marketing strategies.

Employees who create documents must determine the classification of the document and treat it accordingly. All employees must take appropriate measures to protect information according to its level of classification. The owner of the information may declassify confidential information when it is deemed no longer confidential.

Information Classification Policy

1.0 **Purpose**:

Information is a company asset that is owned by the company. Information, regardless of its form or storage medium must be protected. “Information that is electronically created, printed, filmed, typed, stored, or communicated by any means must be protected according to its sensitivity, criticality, and value.”[1] All information within the organization must be classified into specific groups to protect it from unauthorized use and disclosure. This policy classifies information into four (4) distinct groups.

2.0 Scope

All Company employees are responsible for complying with the Information Classification Policy

3.0 Responsibilities

3.1 All Employees are responsible for complying with the proper handling of data.
3.2 The owner or creator of any information asset is responsible for properly classifying the data into a category and defining an employee’s level of access, if any.
3.3 The Information Systems Group is responsible for configuring permissions that are necessary for a user as defined by the owner.

4.0 **Policy**:

All information must be reviewed by its owner and classified into one of the following categories:

- “Public: Any information that is designed to be released to the public and can be given to anyone.” [2] Such information is general knowledge and does not contain any proprietary or confidential information. An example would be a request for quote (RFQ) or a press release.

- Internal: Information of this nature is used in day-to-day business operations. This information may be provided to the Company employees freely.[2] Typically, company employees only know this type of information. This information may be disclosed to vendors or contractors with a valid and current Confidentiality Agreement. Examples of Internal company information include phone lists, server names, and cost center codes.[1]

[1] Peltier, T. R. (2002). Information Security Policies, Procedures, and Standards. Boca Raton, Florida: Auerbach Publications.
[2] Mitnick, K.D. (2002). The Art of Deception. Indianapolis, Indiana: John Wiley & Sons, Inc.

- Private: "Private information is any information that is of personal nature and is intended for use only within the organization. Disclosure of this information to unauthorized individuals could seriously impact employees, clients, and the company. Private information includes: salary history, banking information, health benefits, or any information that is not of public record."[1] This information may not be released to vendors or contractors regardless of any confidentiality agreements on file.

- Confidential: "If this information were disclosed, it would seriously affect the company, stakeholders, business partners, or clients. This information is only shared with a very limited number of people and is on a need to know basis. Such information includes client records, financial records, and business strategies."[1]

4.0 **Declassification**

- The owner of the data must review all data that is classified as "Confidential." Information that is no longer deemed "Confidential" must be reclassified or destroyed. If the owner of the data knows when the information will no longer be confidential in advance, it should be labeled as "Confidential until…"[2]

5.0 References

Policies:

Forms: Security Access Request Form, Confidentiality Agreement

[1] Mitnick, K.D. (2002). The Art of Deception. Indianapolis, Indiana: John Wiley & Sons, Inc.

[2] Peltier, T. R. (2002). Information Security Policies, Procedures, and Standards. Boca Raton, Florida: Auerbach Publications. (p. 118)

Information Classification Policy Explanation

The company uses information in many forms everyday to conduct business. This information may consist of press releases about our new products, or it may be something as sensitive as payroll information. Whatever the case, each piece of information must be treated with care. We must be careful to whom we disclose or discuss various types of information.

It is imperative to know what is appropriate to give to someone else and what is not. This policy provides for the framework for classifying information into four security levels. As we work from Public to Confidential data, each level further restricts who can view and access the information. In addition, further measures must be taken to protect Internal, Private, and Confidential information. These sensitive levels of classification contain information that could cause harm to the company either directly or indirectly. Any breach in security at any level will cause the company to be exposed to security incidents or lawsuits. Therefore, we must classify the information so that everyone knows who can access sensitive information.

It is best to practice a "least privilege" approach to security. Everyone should only have access to what is needed to perform his or her job duties and no more. This not only reduces the risks of unauthorized disclosure, but it also protects employees from unfounded distrust and suspicion.[1]

Subconsciously, we have treated information in different ways without the need to define specific classification categories. We relied on our best judgments as well as those of others to protect sensitive information. However, we must formally define these levels so that everyone knows how to handle certain types of information.

For example, if a brochure for a new product that was coming out six months from now were found in the lobby of the company, what would you do with it assuming it is not properly labeled? People not in the marketing department may believe that this product has already come out and would not think twice about it. However, if it were labeled (or watermarked) "Confidential" any employee spotting the material in the lobby would know that it does not belong there and return it to the appropriate personnel.

Without data classification, we would not know what information to protect and what is safe to disclose. Improper data classification will cause losses to the company and will create both legal and security exposures. Therefore, we must define information classification categories and assign all data that we handle one of these designations. Doing so improves security and reduces risks.

[1] Kabay, M. E. (2002). *Employment Practices and Policies*. In S. Bosworth, & M. E. Kabay (Eds.), Computer Security Handbook (4th ed., pp. 31.1-31.14). New York, NY: John Wiley & Sons, Inc..

E-mail Security Policy Summary

E-mail is a vital asset to any business in today's technologically advanced age. Employees are encouraged to use the e-mail system for business communications, however, there are some restrictions on what it may be used for.

- Any message sent, received or created using company resources is the property of the company. Employees have no expectation of privacy when communicating with any company system.

- Although we discourage employees from using company systems for personal communications, it is understood that occasional use of the system for personal communications is acceptable as long as it does not affect productivity or job performance.

- Employees are not to use the e-mail systems for commercial gain, religious or political causes, outside organizations or other non-job related solicitations. Furthermore, the e-mail system cannot be used for subscribing to mailing lists. Company e-mail address are also not to be used to participate in online discussion forums regardless of the purpose.

- Unencrypted Confidential, Private, or Internal information may not be sent using the e-mail system. Information of a sensitive nature must be encrypted and sent using an approved method as defined by senior management and the Information Systems Group.

- Employees may not use the systems to transmit, retrieve, or store any communication that is discriminatory or harassing, derogatory toward any individual or group, obscene, defamatory or threatening, in violation of any license governing the use of software, or for any purpose that is illegal or contrary to the company's business interests or policies.

- All staff members are not to participate in chain e-mail, mass forwarding, or messages that communicate a virus warning.

- All company e-mail is monitored to ensure compliance with various laws and company policies.

E-mail Security Policy[1]

1.0 Objective

To establish e-mail policies for the security and confidentiality of client and company sensitive information and to protect company assets.

2.0 Scope

All Company employees must abide by the E-mail Security Policy

3.0 Responsibilities

3.1 All employees are responsible for complying with the E-mail Security Policy.

3.2 All employees are responsible for maintaining a positive representation of the company when using information technology.

3.3 The Information Systems Group (ISG) is responsible for monitoring and reviewing employee communication and use of information technology to ensure compliance with all laws and company policies.

4.0 **Policy**

4.1 E-mail is for business purposes only. The Company owns the e-mail system and all messages that are created, sent or received are the property of the Company. Employees are encouraged to use e-mail for efficient and effective communication.

4.2 The e-mail system may not be used to solicit for commercial ventures, religious or political causes, outside organizations or other non-job related solicitations. We discourage the use of business e-mail for personal use. However, in the event that personal e-mail either is sent or received using Company’s system, employees should be aware that these personal e-mails become the property of the Company.

4.3 Information technology cannot be used for knowingly transmitting, retrieving or storing any communication that is:

4.3.1 Discriminatory or harassing
4.3.2 Derogatory to any individual or group
4.3.3 Obscene, sexually explicit or pornographic
4.3.4 Defamatory or threatening
4.3.5 In violation of any license governing the use of software

[1] Silowash, G.J. (2003) *E-mail Security and Confidentiality Policy*, includes updated and new policies

4.3.6 Engaged in for any purpose that is illegal or contrary to Company's policy or business interests.

4.4 "Employees who receive any emails with prohibited content from any company employee should report the matter to their supervisor immediately."[1]

4.5 The ISG is responsible for monitoring and reviewing employee communication, electronic files, messages and use of electronic media to ensure they are being used in compliance with the law, this policy and other company policies. **"**The Company may monitor messages without prior notice. The Company is not obliged to monitor email messages."[2]

4.6 Employees have no expectation of privacy when using any of the telecommunication equipment or services provided by Company.

4.7 Employees should not transmit confidential information, such as client names, addresses, or social security numbers, via Internet or email under any circumstances unless the information is encrypted and approved by a member of senior management and the manager of the Information Systems Group.

4.8 E-mail and website addresses must be verified as accurate and the identity of the receiving party known before information is transmitted via the Internet or E-mail.

4.9 Employees are not to send email or other electronic communications that attempt to hide the identity of the sender or represent the sender as someone else.

4.10 The company e-mail systems and any e-mail address associated with a user are not to be used for subscribing to mailing lists or for posting messages in public forums whether for professional or personal reasons.

4.11 Information technology and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system. (i.e., SPAM, chain letters)

4.12 "Virus or other malware warnings from the Company shall be approved by the ISG before sending."[3]

[1] SANS Institute (2006). Email Use Policy. Retrieved July 25, 2006, from http://www.sans.org/resources/policies/Email_Policy.pdf?portal=d20be36f6efa3f6fcd74d665fe9b26bf
[2] Ibid.
[3] Ibid.

4.13 Any employee who does not abide by this policy will be subject to the provisions defined in the Employee Conduct Manual.

5.0 Definitions

5.1 "E-Mail: The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.

5.2 Forwarded E-mail: Any e-mail that is resent without significant changes from one person to another either internally, externally, or any combination thereof. Clicking the forward button within an e-mail client and entering someone's e-mail address with or without a brief note is an example of a forward.

5.3 Chain e-mail or letter: Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.

5.4 Virus Warning: Email containing warnings about a virus or malware. The overwhelming majority of these e-mails turn out to be a hoax and contain bogus information usually only intent on frightening or misleading users."[1]

6.0 References

Policy: E-Mail Security Policy, Employee Conduct Manual

Forms:

[1] SANS Institute (2006). Email Use Policy. Retrieved July 25, 2006, from http://www.sans.org/resources/policies/Email_Policy.pdf?portal=d20be36f6efa3f6fcd74d665fe9b26bf

E-Mail Security Policy Explanation

E-mail communication is a fast and efficient way for us to communicate with our co-workers, clients, vendors, and others for business purposes. However, the company assumes some risks (viruses, data leaks, etc.) when communicating via e-mail. This policy was designed to reduce those risks and provide employees with a safe and effective communication tool.

Like any other form of communication, employees are responsible for maintaining a positive representation of the company when using the e-mail systems. Employees communicating through e-mail act as a spokesperson for the company. When someone sees an e-mail address of our company, they expect to be treated with professionalism and respect. Anything less tarnishes the company's reputation.

The company monitors the e-mail systems to ensure compliance with various laws and other company policies. Therefore, all communications on the company network are subject to monitoring without notice and have no expectation of privacy. However, we are also not obligated to monitor e-mail messages. This may sound contradictory. Essentially, we will not record e-mail communications for employee use, tracking and journaling. All e-mail logs are property of the company and are to be used for compliance purposes.

Company computer systems are for business purposes only. Any other use degrades system performance and reduces availability for legitimate business purposes. However, since we live in an advanced society that now recognizes e-mail as a valuable communications medium, it is acceptable to send a limited amount of personal e-mail using company systems; however, these e-mails do become the property of the company and are subject to company policy.

E-mail that is of a discriminatory, derogatory, harassing, obscene, or defamatory in nature is not tolerated. In addition, messages that are for illegal purposes or are contrary to company policy or business interests are not permitted. These types of messages are unlawful and violate the company's code of ethics.

We must protect our sensitive information from misuse. E-mail is very much a public communications method and does not offer any method for ensuring privacy. E-mail can be intercepted and read by anyone with the technology and skills to do so. Therefore, sensitive information is not to be communicated using e-mail or the Internet without using approved encryption methods authorized by senior management and the Information Systems Group.

It is also critical to know who someone is and verify their identity where possible before sending any information to them via e-mail or the Internet. E-mail and websites can easily be spoofed to fool you into believing that they are from legitimate people or companies.

Employees must properly represent themselves to all computer systems. E-mail is no exception. You are not permitted to conceal your identity or use someone else's identity to transmit data or misrepresent yourself.

Mailing lists and forums can be effective ways to obtain information quickly. However, these same sources may hamper system performance. Company e-mail addressess are not to be used for participation in any forum. An e-mail address identifies the company. Therefore, any person making any statement that can be linked to a company e-mail address may unknowingly act as a policy maker or spokesman for the company. This also may lead to a data leak without the employee even knowing that it has occurred.

Our systems often receive spam or junk e-mail. Some of this mail includes chain letters and mass forwarded e-mail that causes a decrease in system performance and an increase employee downtime. We ask that you do not participate in any mass forwarding or chain letters.

Virus warnings and other malware warnings are not to be sent using our systems unless authorized by the Information Systems Group. These messages are typically hoaxes and cause users undue stress and a large volume of calls to the helpdesk. Please do not participate in these types of messages.

E-mail communication is a fast and effective way to convey business information to others. However, we must protect our systems from harm. We must also protect the company and its reputation in the online world.

Internet Acceptable Use Policy Summary

Internet access in today's business environment allows for efficient communications and further enhances our ability to find information when needed on demand. However, the Internet does contain material that can cause harm to the company and its information infrastructure.

Employees are reminded that Internet access is a privilege that can be revoked at anytime. All Internet communications are monitored and employees have not expectation of privacy.

The Internet is to be used for business purposes as defined by management. All employees are expected to maintain the highest level of professionalism when using the Internet. Therefore, there are several categories of websites that are prohibited. These sites include, but are not limited to:

- Violence/Hate/Racism
- Pornography
- Cult/Occult
- Sex Education
- Chat/Instant Messaging
- Personals and Dating
- Pay to Surf Sites
- Intimate Apparel
- Weapons
- Drugs/Illegal Drugs
- Gambling
- Games
- Humor/Jokes
- Nudism
- Adult/Mature Content
- Illegal Skills
- Alcohol/Tobacco
- Hacking
- MP3/Streaming

Essentially, if you would not view a particular website with your manager watching, it is safe to assume that this type of website is prohibited. Employees are not permitted to download and install any software from the Internet without the approval of the Information Systems Group.

Employees are permitted to browse the Internet during lunch breaks and at other management-designated times. This casual browsing must not interfere with job performance or productivity. Individuals are reminded that all company policies apply while browsing during these times.

The Internet is an effective business tool. We must limit what we use it for in order to ensure productivity and quality work. The Internet does have content that needs restricted in order to protect the organization from legal and security issues.

Internet Acceptable Use Policy

1.0 **Objective**

To define acceptable uses for accessing Internet resources using company owned systems.

2.0 **Scope**

All employees are responsible for complying with the Internet Acceptable Use policy.

3.0 **Responsibilities**

3.1 All employees are responsible for complying with the E-Mail Security Policy.

3.2 All employees are responsible for maintaining a positive representation of the company when using information technology.

3.3 The Information Systems Group (ISG) is responsible for monitoring and reviewing employee use of information technology to ensure compliance with all laws and company policies.

3.4 Senior Management will define websites that are acceptable and unacceptable.

3.5 Any employee wanting to access the Internet must complete an *Internet Access Request* form and submit it to their manager for approval.

3.6 The Information Systems Group is responsible for creating access for approved Internet Access Request forms.

4.0 **Policy**

4.1 All devices, including workstations, servers, firewall, printers, and other peripherals are company property and must be protected from misuse.

4.2 Employees have no expectation of privacy when using any company system. By using company resources, all employees consent to monitoring.

4.3 The company reserves the right to monitor Internet usage as well as any network resource usage. This includes, but is not limited to logs that contain: websites visited, number of visits in any timeframe, pages visited at a website, amount of bandwidth consumed, and time and date of visit. Employees have no expectation of privacy when using any company system.

4.4 All information traveling on any data or voice network is company property and therefore must be used appropriately.

4.5 The company also owns the bandwidth used for all communications on the company network and the bandwidth for communications to and from the network. This bandwidth is vital to business communications and must be reserved for business purposes.

4.6 The company will use technological measures to ensure a safe and efficient computing environment. These measures include, but are not limited to: content filtering, malicious code blocking, firewalls, network traffic analyzers, and bandwidth shapers.

4.7 “The use of company-provided access to the Internet is intended exclusively for management-approved activities.”[1]

4.8 The following types of websites are prohibited regardless of whether or not the content filtering software and hardware permit it:

4.8.1 Discriminatory or harassing
4.8.2 Derogatory to any individual or group
4.8.3 Obscene, sexually explicit or pornographic
4.8.4 Defamatory or threatening
4.8.5 In violation of any license governing the use of software
4.8.6 Engaged in for any purpose that is illegal or contrary to Company’s policy or business interests.

4.8.6.1 The below categories of websites are prohibited. Management reserves the right to modify this list at anytime:

- Violence/Hate/Racism
- Pornography
- Cult/Occult
- Sex Education
- Chat/Instant Messaging
- Personals and Dating
- Pay to Surf Sites
- Intimate Apparel
- Weapons
- Drugs/Illegal Drugs
- Gambling
- Games
- Humor/Jokes
- Nudism
- Adult/Mature Content
- Illegal Skills
- Alcohol/Tobacco
- Hacking
- MP3/Streaming

[1] Peltier, T. R. (2002). Information Security Policies, Procedures, and Standards. Boca Raton, Florida: Auerbach Publ ications. (p. 39)

4.9 Downloading of any software from any Internet source is prohibited. All software must be approved and installed by the Information Systems Group.

4.10 E-mail and website addresses must be verified as accurate and the identity of the receiving party known before information is transmitted via the Internet or E-mail.

4.11 Casual browsing of the Internet is permitted during lunch breaks and at other management-designated times. However, personal browsing must not interfere with your job performance and productivity. All company policies apply while browsing during these times.

4.12 Any employee who does not abide by this policy will be subject to the provisions defined in the Employee Conduct Manual.

5.0 **References**

Policy: E-Mail Security Policy, Employee Conduct Manual

Forms: Internet Access Request

Internet Acceptable Use Policy Explanation

The Internet is a great business tool to find information quickly. However, there are some risks with using the Internet in a business environment. Therefore, we must have policies in place to protect our company, employees, and the information infrastructure.

Internet access is a privilege that may be revoked at anytime. Employees are responsible for requesting Internet access as some do not require it during their normal course of business. Managers must approve the access request before the Information Systems Group will enable Internet access. All employees must maintain a professional image of the company at all times while using Internet resources.

The company reserves the right to monitor all Internet communications to ensure compliance with applicable laws, regulations, and company policy. Therefore, employees have no expectation of privacy when using any company provided information system.

It is essential to limit all traffic on the company's networks to business communications. Any other use degrades network performance by reducing available bandwidth and consuming other network resources. The company does employ the use of content filtering, malicious code blocking, firewalls, traffic analyzers, and other equipment to ensure a high quality of service for business communications.

Various websites are prohibited and most of them blocked by the content filtering service. However, if the content filter does not restrict a site, it does not necessarily mean the site is permitted. Employees must ensure that they are not viewing any websites that contain discriminatory, harassing, derogatory, obscene, defamatory, threatening, or illegal information. These types of site are prohibited due to legal reasons as well as the company's code of business ethics. Other sites are blocked because they have the potential to induce security problems into the company's information infrastructure.

Users are prohibited from downloading computer software from any Internet source. Malicious code may be introduced to the computing environment if this is done. In addition, we must make sure that the organization is in compliance with all software licenses.

The Internet allows us to communicate with people all over the world. However, we must make sure that we verify a person's credentials before using any information to make a business decision or before information is transmitted to another individual.

Casual browsing of the Internet allows staff to communicate with others as well as to keep up to date with world news. Casual browsing is permitted during lunch breaks and management defined times. However, any browsing must not affect the employee's job performance or productivity. All company policies apply during these times.

By following a few simple rules, the Internet will be a safer resource for the company's business needs. We will also ensure a safer computing environment for all.

Security Awareness

Security awareness training is an essential part to any security program. Employees are able to ask questions and are able to better understand the policies.

> "The training program complements existing policies and allows management to reinforce the importance of security. Proper security awareness training empowers employees to identify security issues and risks. Training also allows companies to send a personal message to every employee. A successful training program will allow employees to take what they learned and apply it to their job and even their personal lives."[1]

The organization must enhance its current training efforts. Currently, training is not part of the company's overall security plan.[2] Staff must receive training continuously in order to have an effective security program.

However, before any training program can be put into place, senior management must recognize the need for it as well as support the training initiatives. If management does not support security policies, security awareness training will not be supported and well received.

The company must recognize that employees are the first line of defense against security violations. Employees are usually the first affected by a security incident. If they know how to respond or know the proper policies to be followed, security will be greatly heightened.[3]

In addition, an effective security awareness program must address the different learning styles that every employee possesses. There are three types of learning styles:

- Auditory
- Visual
- Kinesthetic

> "An auditory learner picks up information from hearing it and is effectively reached by lectures and written material. A visual learner wants to see what is being taught and refers to diagrams, charts, and pictures. A kinesthetic learner responds well to tactile input and needs to walk through the steps by physically doing the task."[4]

[1] Silowash, G.J. (2006), *Security Awareness,* Norwich University, MSIA Seminar 3, Week 2 Essay

[2] Ibid.

[3] Rudolph, K., Warshawsky, G., & Numkin, L. (2002). Security Awareness. In S. Bosworth, & M. E. Kabay (Eds.), Computer Security Handbook (4th ed., pp. 29.1-29.19). New York, NY: John Wiley & Sons, Inc.. (p. 29.15)

[4] Cobb, C. (2006). Psychology and Effective Security-Awareness Training. Retrieved August 5, 2006, from http://norwichwebct.embanet.com/SCRIPT/MSIA8_Content_Repository/scripts/student/serve_page.pl/MSIA8_Content_Repository/8_msia_sem3/MSIA_S03_W08_webct.html?1948742616+1146691300+OFF+8_msia_sem3/pdf/MSIA_S3_W08_LECTURE.PDF+

All security awareness training initiatives should include a mixture of the three learning styles in order to be effective. A training program may consist of a lecture that includes handout and charts. In addition, role playing exercises can be utilized.

Continuous Training

Not all training events must be formal. Rather, the company may use various ways to communicate security concerns to its staff.

Screensavers that use animated text and/or graphics to convey security message are effective.[1] Messages may state simple things like "Don't share your password." or "Secure all sensitive information when leaving for the day." The screensaver will also function as a lock so if an employee steps away from the computer for too long and forgets to lock their machine, the screensaver will do it for them. Text based screen savers are fairly simple to configure since the company currently uses Windows 2003 Server with Active Directory and Group Policies. A group policy object can be created to enable the same screensaver on every machine with a simple message. A timeout can also be specified. This process will not incur any additional costs and will only require a few minutes of the Information Systems Group time.

Posters also allow the company to target specific security issues in a cost effective manner.[2] Posters containing security messages should be displayed in areas where employees tend to congregate, such as break rooms, water coolers, copiers, and other high traffic areas. The company or a third party could design the posters. The marketing department and the ISG could work together to develop the posters. Our copy machines are capable of printing on tabloid size paper. This will keep costs of production low while further enhancing the training program.

Security awareness videos can also be screened by employees during their lunch break.[3] Staff can then discuss the material in an informal environment. Several sources exist for professionally made awareness videos:

The United States Postal Inspectors produce several movies that can apply to both the professional and personal lives of the staff. They are available free of charge at: http://www.usps.com/postalinspectors/dvdorder.htm. Titles in this series include:

- *Delivering Justice: Identity Crisis*
    - The film shows how people's lives can be ruined due to identity theft. It also offers tips to help reduce identity theft. When used in an Awareness program, the film can also be used to identify Information Classification problems as well as what can happen to

[1] Rudolph, K., Warshawsky, G., & Numkin, L. (2002). Security Awareness. In S. Bosworth, & M. E. Kabay (Eds.), Computer Security Handbook (4th ed., pp. 29.1-29.19). New York, NY: John Wiley & Sons, Inc.. (p. 29.15)Ibid.
[2] Ibid.
[3] Ibid.

    - information if the wrong people receive more access than what they need.
- *Delivering Justice: Web of Deceit*
    - The video discusses Phishing scams and how to protect yourself online. This video would fit into any Internet Awareness program video. The information it contains will help protect company information and it will be useful to staff in their personal lives as well.
- *Delivering Justice: All The King's Men*
    - This video is a follow up to the previous two videos. It discusses how victim suffer in identity theft scams.

There are several other videos in the series that do not necessarily relate to corporate security, but they may help employees recognize scams. All of the videos in the series include posters that may be used as part of the security awareness program.

Another company, Commonwealth Films, produces videos that address security topics that will fit into the company's security awareness program. Videos of interest include:

- The Plugged in Mailbox
- Look Out for Your Laptop
- Computer Virus Attack
- get.net.smart
- Under Wraps
- The Best Defense

These titles, as well as information about many others are available at http://www.commonwealthfilms.com. These films would compliment the company's security policies as they are developed and provide employees with more information about security initiatives.

Another excellent yearlong security awareness event would allow employees to become involved with corporate security. The company could host a "spy game" competition where teams of employees try to find security errors made by other staff members. The errors are reported back to a member of the Information Systems Group. Each team must not get caught and other teams will be spying on each other. At the end of every quarter, a mock trial takes place that highlights the security errors that were discovered. At the end of the year, the winning spy team will receive a certificate and an award that may include a gift certificate to a local establishment.[1]

[1] Cobb, C. (2006). Psychology and Effective Security-Awareness Training. Retrieved August 2, 2006, from http://norwichwebct.embanet.com/SCRIPT/MSIA8_Content_Repository/scripts/student/serve_page.pl/MSIA8_Content_Repository/8_msia_sem3/MSIA_S03_W08_webct.html?1948742616+1146691300+OFF+8_msia_sem3/pdf/MSIA_S3_W08_LECTURE.PDF+

A member of the Information Systems Group may also design a security awareness newsletter that is sent out to staff on a monthly or more frequent basis. The newsletter may contain security tips and other information that will improve security. A special section of the newsletter may also be dedicated to questions and answers. Staff could ask any type of security question or issue that may be on their mind and practical answers, solutions, and advice would be provided.[1]

By utilizing the above programs, the company will have an excellent ongoing security awareness program that will involve all staff members.

[1] Silowash, G.J. (2006) *Using Social Psychology to Implement Security Policies*, Norwich University MSIA Seminar 3, Week 8 Essay

Information Classification Policy Training

Materials Needed: Laptop, LCD Projector, copies of the notes view of Appendix A PowerPoint presentation for every staff member, room for role playing exercise, whiteboard with dry erase markers, items to pass out for rewards (stickers, candy, coffee mugs, pens, etc.), "Delivering Justice: Identity Crisis"

Time Needed: 45-60 Minutes with question and answer session. More time if the video is used.

Notes: Whenever a staff member answers a question correctly, recognize them with a reward item. Answers that require more thought should be rewarded with a larger prize. Always offer positive reinforcement no matter the answer. Offer a Certificate of Completion to those who complete the training program. You may wish to include a simple multiple choice test.

1. Information Classification Intro Slide

2. Today we will discuss:

    - The importance of classifying information
    - The classification groups
    - Handling sensitive documents
    - Declassifying information

3. What are the company's information assets?

    - Information that is electronically created, printed, filmed, typed, stored, or communicated by any means
    - Examples include, but are not limited to:
        - Financial Statements
        - Client Records
        - Market Materials
        - Employee Records

4. Why we classify our information

    - We must protect information from unauthorized access or disclosure
    - We need to protect our data from destruction and misuse
    - We must prevent competitors from gaining a competitive edge
    - Our clients rely on us to prevent access to personal, sensitive information

☑ ***<u>Training Tip</u>:*** As a supplement to the above bullets, include information about why having access to too much information may be a bad thing. If data turns up deleted or stolen, the first suspects will be those who have access to that data. Employees must be protected from unfounded suspicion and distrust.[1]

5. The Classification Groups

- Public
- Internal
- Private
- Confidential

☑ ***Training Tip:*** Before proceeding to the next slide ask staff members if they can identify where the following types of information may fit:
–Expense Report (Internal) –Phone Directory (Internal)
–Products in Development Information (Confidential) –Salary Histories (Private)

6. The Classification Groups: Public

- Any information that is designed to be released to the public and can be given to anyone.
- Examples:
  - Press Release
  - Request for Quote (RFQ)
  - Website Materials

☑ ***Training Tip:*** Ask staff to identify any information they work with on a day-to-day basis that may be classified as Public.

7. The Classification Groups: Internal

- Information of this nature is used in day-to-day business operations. This information may be provided to the company employees freely.
- Examples:
  - Server Names
  - Phone Lists
  - Cost Center Codes

☑ ***Training Tip:*** Ask staff why cost center codes and phone directories are classified as Internal. Answers may include items related to social engineering and preventing fraud.

8. The Classification Groups: Private

- Private information is any information that is of a personal nature and is intended for use only within the organization.

[1] Kabay, M. E. (2002). *Employment Practices and Policies*. In S. Bosworth, & M. E. Kabay (Eds.), Computer Security Handbook (4th ed., pp. 31.1-31.14). New York, NY: John Wiley & Sons, Inc..

- Cannot be released to any third party regardless of any agreements on file
- Examples:
  - Salary History
  - Banking Information
  - Health Benefits
  - Information that is not public record

☑ ***Training Tip:*** Ask staff to identify any information they work with on a day-to-day basis that may be classified as Private.

9. The Classification Groups: Confidential

- Highest level of classification
- Highest level of security
- If this information were disclosed, it would seriously affect the company, stakeholders, business partners, or clients.
- Examples:
  - Client Records
  - Financial Records
  - Business Strategies

☑ ***Training Tip:*** Ask staff why business strategies must be classified as confidential. Answers may include "competitive advantage" or future business plans.

10. Handling Sensitive Information (2 Slides)

- Information classified higher than the public level must be distributed with care.
  - If distributing a document, person receiving document must have permission from data owner
- Information must be kept in a secure location when not in use.
  - Lock file cabinets and desk drawers
  - All desktops must not contain any sensitive documents at the end of the day

11. (continued)

- Information that is no longer used or needed must be destroyed in an appropriate manner.
  - Must consult data owner if the information is an original and not a copy
  - Proper destruction techniques must be followed
    - Documents and CDs must be shredded
    - Information Systems Group will destroy other media

☑ ***Training Tip:*** Inform staff that anyone who can access their office after business hours (cleaning crew, intruder) can view anything on their desk. All Internal, Private, and Confidential information must be secured when leaving for the day.

12. Declassification

- Information that no longer needs classified must be either reclassified or destroyed.
- End of its useful life
  - Will not hurt the organization if released to a lower classification group
  - If it is no longer needed, it should be destroyed.

13. Today we discussed:

- The importance of classifying information
- The classification groups
- Handling sensitive documents
- Declassifying information

14. Questions?

- If you have any questions, please contact your manager.

☑ ***Training Tip:*** Encourage employees to ask management questions about proper classification. They must never assume and always err on the side of caution. Encourage employees to find information that may not fit in its current classification.

15. Thank You!

- *Thank you for your attention!*
- *Have an excellent day!*

☑ ***Training Tip:*** To further reinforce this message, you may want to role-play different scenarios involving the classification of company data and unauthorized disclosure. An example would be to role-play the situation outlined in the *Information Classification Policy Explanation* section of this document:

> "If a brochure for a new product that was coming out six months from now were found in the lobby of the company, what would you do with it assuming it is not properly labeled? People not in the marketing department may believe that this product has already come out and would not think twice about it. However, if it were labeled (or watermarked) 'Confidential' any employee spotting the material in the lobby would know that it does not belong there and return it to the appropriate personnel"

☑ ***VIDEO:*** In addition, you may want to include the “Delivering Justice: Identity Crisis” video offered free of charge by the United States Postal Inspectors at: http://www.usps.com/postalinspectors/dvdorder.htm

Discuss two scenes in the Movie:

Access to the ISP’s e-mail system

- Too much access is bad thing to give to all employees

Employment Applications

- How should they be classified?

E-Mail Security Policy Training

Materials Needed: Laptop, LCD Projector, copies of the notes view of Appendix B PowerPoint presentation for every staff member, postcards, whiteboard with dry erase markers, items to pass out for rewards (stickers, candy, coffee mugs, pens, etc.), "Delivering Justice: Identity Crisis"

Time Needed: 90 Minutes with question and answer session and video (13:45)

Notes: Whenever a staff member answers a question correctly, recognize them with a reward item. Answers that require more thought should be rewarded with a larger prize. Always offer positive reinforcement no matter the answer. Offer a Certificate of Completion to those who complete the training program. You may wish to include a simple multiple choice test.

1. E-mail Security Policy Training Intro Slide

2. Today you will learn about:

    - E-Mail Security Policies
    - How to protect yourself from e-mail scams

3. E-mail Security Policies

    - E-Mail is for business purposes
        - "Confirm appointments and meetings
        - Remind others of deadlines
        - Provide informal and brief progress reports
        - Convey non-confidential information to others quickly
        - Stay in touch with business partners
        - Share concerns and suggestions with others"[1]

4. E-mail Security Policies (cont'd)

    - E-mail systems are monitored
        - Compliance with laws, regulations, and company policies
        - All messages belong to the company
        - No expectation of privacy
    - Systems can be used for personal mail
        - Limited amount
        - Cannot affect job duties or productivity

[1] Peltier, T. R. (2002). Information Security Policies, Procedures, and Standards. Boca Raton, Florida: Auerbach Publications. (pp. 244-245)

☑ ***Training Tip:*** Explain to staff the company's stance on reviewing e-mail.

- Is all e-mail read?
- Who initiates the monitoring process?
- When and why is e-mail read?
    - Suspected of violating policy / law?

5. E-mail Security Policies (cont'd)

    - Unencrypted e-mail classified as Confidential, Private, or Internal must not be communicated via e-mail
        - Client Names
        - Addresses
        - Social Security Numbers
        - Financial Information
    - Encryption must be approved by senior management and the ISG

☑ ***Training Tip:*** Pass out postcards to all those in attendance. Ask each person to write down their name on the postcard and something that everyone may not know about them. Have them pass the cards around the room. This is not only an icebreaker, but it demonstrates that messages sent through e-mail are like postcards, whatever you write on them can be seen by anyone else. You may want to pass out a postcard that contains a scrambled message. This would be an example of encryption.

6. E-mail Security Policies (cont'd)

    - E-mail addresses represent you as an employee of the organization
    - A positive, professional representation of the company must be maintained at all times.
    - You must also properly identify your self to all computer systems.
        - Do not attempt to conceal your identity
        - Do not misrepresent the sender as someone else

7. E-mail Security Policies (cont'd)

    - E-mail cannot be used for transmitting, storing, or retrieving any communication that is:
        - Discriminatory or harassing
        - Derogatory to any individual or group
        - Obscene, sexually explicit or pornographic
        - Defamatory or threatening
        - In violation of any license governing the use of software
        - Engaged in for any purpose that is illegal or contrary to Company's policy or business interests.

☑ ***Training Tip:*** Explain to staff that these types of e-mail are illegal and violate the company's code of ethics. Advise them that they should treat others the way they would want to be treated even in e-mail.

8. E-mail Security Policies (cont'd)

- Your e-mail address must not be used in any online discussion forums or message boards
  - Your statements can be construed as representing the company's position
  - May cause unintentional data leaks
    - Reveals the organization for which you work

☑ ***Training Tip:*** Advise employees that when they use company e-mail, they are representing the company. For example: If Mike Rophone were to post a message in a message forum stating that he dislikes the new Widget that the company just released, then people may draw the conclusion that the company does not support the new product even though the exact opposite is true. In addition, if someone in the ISG were to post a message stating that they needed help with the latest vulnerability on a web server, then people know that our company has a security flaw on the web server and opens us to attacks.

9. E-mail Security Policies (cont'd)

- Please do not participate in any of the following:
  - Chain Letters
    - Consume resources and your valuable time
  - Mass Forwarding
    - Consume resources and your valuable time
  - Virus or Malware warnings
    - Usually a hoax
    - Verify at http://www.snopes.com
    - Contact the ISG

☑ ***Training Tip:*** Discuss how virus warnings are usually hoaxes. A good example is available at: http://www.snopes.com/computer/virus/jdbgmgr.htm or at http://www.trendmicro-middleeast.com/smb/vinfo/hoaxes.php?vHoax=75

10. E-mail Security Policy Q&A

- Question and Answer Time
- Consult your manager should you have any questions that are not addressed here.

11. Protecting Yourself from e-mail scams and Identity Theft

- Video Presentation of:
    - *Delivering Justice: Identity Crisis*
- Brought to you by the
    - United State Postal Inspection Service
- Obtain your free copy at: http://www.usps.com/postalinspectors/dvdorder.htm

☑ ***VIDEO:*** Play the video "Delivering Justice: Identity Crisis"

- Discuss ways for staff to prevent identity theft.

☑ ***Training Tip:*** Advise staff that they can Opt-Out of credit card offers sent to their home by calling: 1-888-5-OPTOUT (1-888-567-8688) or by visiting https://www.optoutprescreen.com/

12. Phishing Scams

- Phishing as defined by the wikipedia:
    - (http://en.wikipedia.org/wiki/Phishing)
    - "In computing, phishing is a form of criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using email or an instant message, although phone contact has been used as well. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, and technical measures."

13. Spotting a Phishing Scam

- Slide Contains a picture of a fraudulent e-mail

☑ ***Training Tip:*** Ask staff if they know how to spot a phishing scam before moving on to the next slide.

14. Spotting a Phishing Scam

- Slide contains a fraudulent e-mail with certain details that identify it as fraudulent.

☑ ***Training Tip:*** Point out all the fraudulent indicators in the e-mail message. As a supplement to this, you may wish to find a similar e-mail and pass out the fraudulent header information and show staff how to see header information. This may be very technical for some, but it may be beneficial to others.

15. What do I do?
    - Delete the e-mail, do not respond
    - Do not click on links in the e-mail
        - Type the address into the address bar
    - Banks typically do not send you this type of request in the e-mail
        - May receive notification via phone or postal mail

☑ ***Training Tip:*** Staff should know that banks or other companies do not usually send out this kind of a request in e-mail. Staff should contact the company by telephone directly. They should also only call the number listed on the official website, billing statement, credit card, or phone book. Staff should also know that they should not respond to any questions from someone claiming to be a bank unless they initiated the call. Always off to call the company back at a number that can be publicly found from a legitimate source.

16. How to protect yourself:

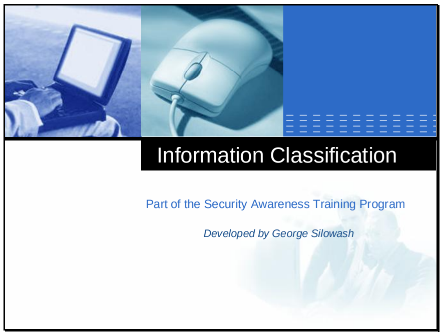
    - If you fear that you may have fallen for this trick, contact:
        - Your Banks
        - Credit Reporting Agencies
            - Experian: 1-888-397-3742
            - Trans Union: 1-800-888-4213
            - Equifax: 1-800-685-1111
    - Request a free credit report every year at: http://www.annualcreditreport.com

17. Questions and Answers

    - Questions & Answers
    - If you have further questions regarding Phishing or any e-mail or Internet Scam, please contact the Information Security Team

Appendix A: Data Classification Training Slides

Slide 1

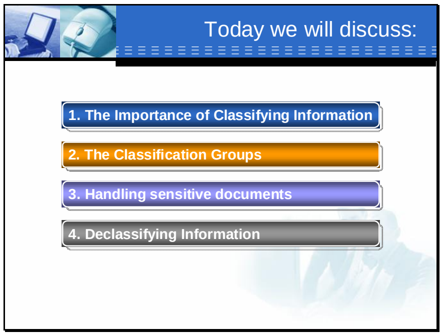


Information Classification

Part of the Security Awareness Training Program

Developed by George Silowash

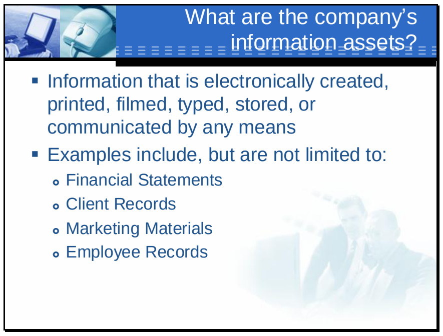
Slide 2



Today we will discuss:

1. The Importance of Classifying Information
2. The Classification Groups
3. Handling sensitive documents
4. Declassifying Information

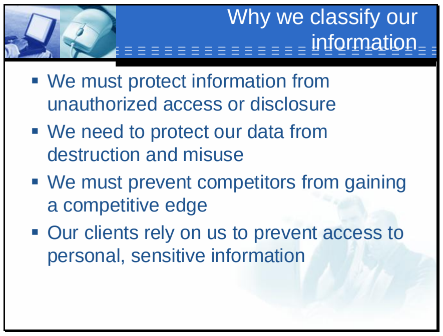
Slide 3



What are the company's information assets?

- Information that is electronically created, printed, filmed, typed, stored, or communicated by any means
- Examples include, but are not limited to:
  - Financial Statements
  - Client Records
  - Marketing Materials
  - Employee Records

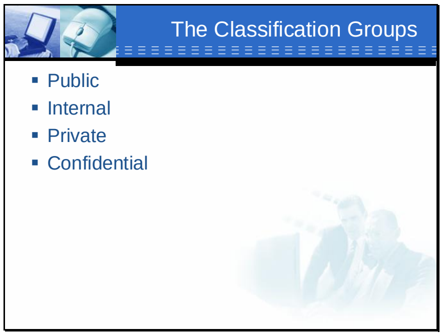
Slide 4



Why we classify our information

- We must protect information from unauthorized access or disclosure
- We need to protect our data from destruction and misuse
- We must prevent competitors from gaining a competitive edge
- Our clients rely on us to prevent access to personal, sensitive information

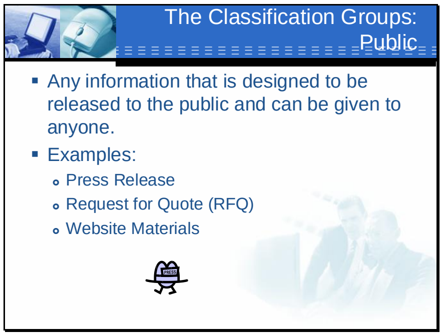
Slide 5



The Classification Groups

- Public
- Internal
- Private
- Confidential

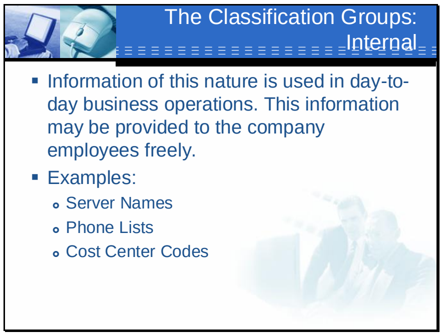
Slide 6



The Classification Groups: Public

- Any information that is designed to be released to the public and can be given to anyone.
- Examples:
  - Press Release
  - Request for Quote (RFQ)
  - Website Materials

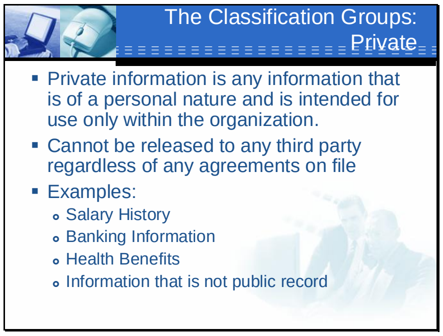
Slide 7



The Classification Groups: Internal

- Information of this nature is used in day-to-day business operations. This information may be provided to the company employees freely.
- Examples:
  - Server Names
  - Phone Lists
  - Cost Center Codes

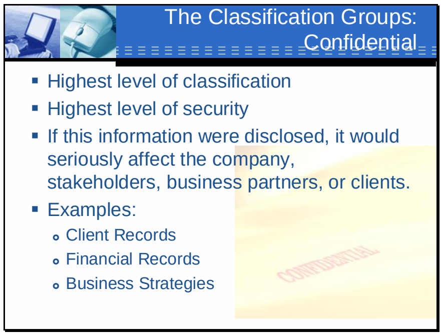
Slide 8



The Classification Groups: Private

- Private information is any information that is of a personal nature and is intended for use only within the organization.
- Cannot be released to any third party regardless of any agreements on file
- Examples:
  - Salary History
  - Banking Information
  - Health Benefits
  - Information that is not public record

Slide 9

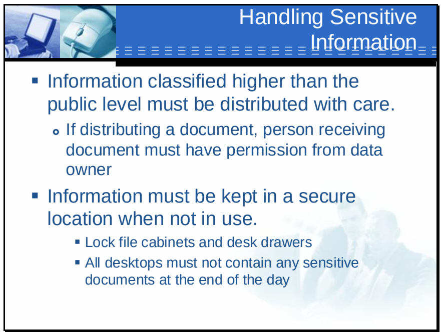


The Classification Groups: Confidential

- Highest level of classification
- Highest level of security
- If this information were disclosed, it would seriously affect the company, stakeholders, business partners, or clients.
- Examples:
  - Client Records
  - Financial Records
  - Business Strategies

CONFIDENTIAL

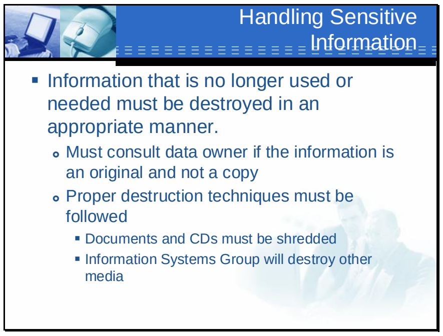
Slide 10



Handling Sensitive Information

- Information classified higher than the public level must be distributed with care.
  - If distributing a document, person receiving document must have permission from data owner
- Information must be kept in a secure location when not in use.
  - Lock file cabinets and desk drawers
  - All desktops must not contain any sensitive documents at the end of the day

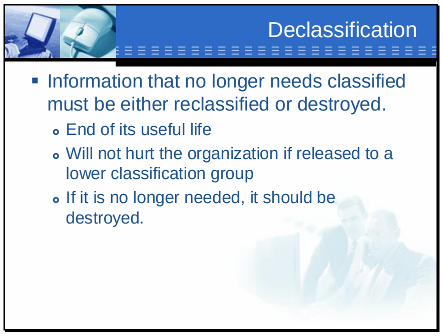
Slide 11



Handling Sensitive Information

- Information that is no longer used or needed must be destroyed in an appropriate manner.
  - Must consult data owner if the information is an original and not a copy
  - Proper destruction techniques must be followed
    - Documents and CDs must be shredded
    - Information Systems Group will destroy other media

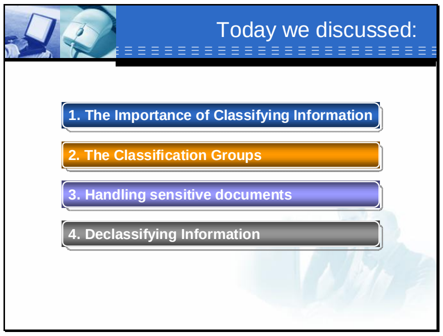
Slide 12



Declassification

- Information that no longer needs classified must be either reclassified or destroyed.
  - End of its useful life
  - Will not hurt the organization if released to a lower classification group
  - If it is no longer needed, it should be destroyed.

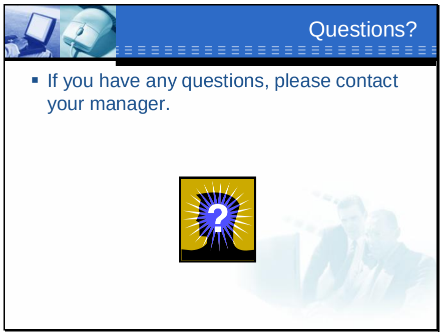
Slide 13



Today we discussed:

1. The Importance of Classifying Information
2. The Classification Groups
3. Handling sensitive documents
4. Declassifying Information

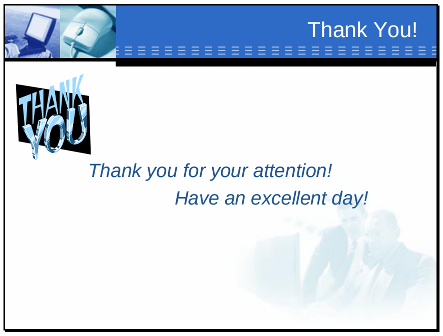
Slide 14



Questions?

- If you have any questions, please contact your manager.

Slide 15



Thank You!

Thank you for your attention!

Have an excellent day!

Appendix B: E-Mail Security Policy Training Slides

Slide 1

E-mail Security Policy Training

Part of the Security Awareness Training Program

Developed by George Silowash

Slide 2

Today you will learn about:

- E-Mail Security Policies
- How to protect yourself from e-mail scams

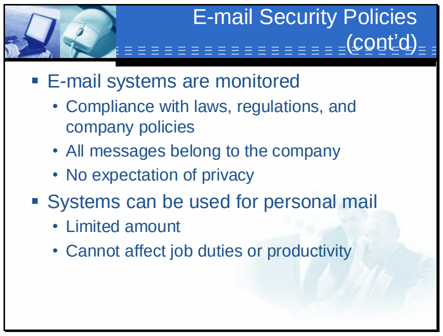
Slide 3

E-mail Security Policies

- E-Mail is for business purposes
  - “Confirm appointments and meetings
  - Remind others of deadlines
  - Provide informal and brief progress reports
  - Convey non-confidential information to others quickly
  - Stay in touch with business partners
  - Share concerns and suggestions with others”[1]

1- Peltier, T. R. (2002). Information Security Policies, Procedures, and Standards. Boca Raton, Florida: Auerbach Publications. (p. 244-245)

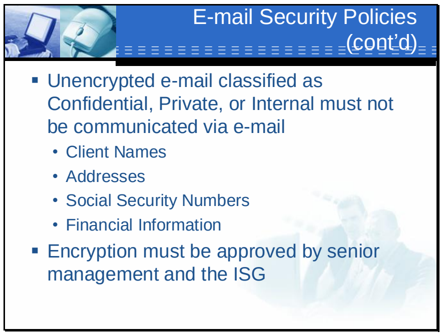
Slide 4



E-mail Security Policies (cont'd)

- E-mail systems are monitored
  - Compliance with laws, regulations, and company policies
  - All messages belong to the company
  - No expectation of privacy
- Systems can be used for personal mail
  - Limited amount
  - Cannot affect job duties or productivity

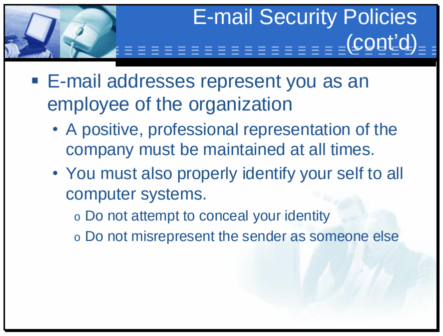
Slide 5



E-mail Security Policies (cont'd)

- Unencrypted e-mail classified as Confidential, Private, or Internal must not be communicated via e-mail
  - Client Names
  - Addresses
  - Social Security Numbers
  - Financial Information
- Encryption must be approved by senior management and the ISG

Slide 6



E-mail Security Policies (cont'd)

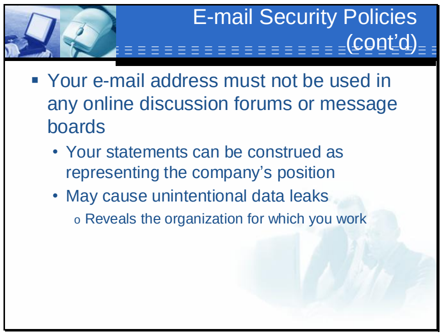
- E-mail addresses represent you as an employee of the organization
  - A positive, professional representation of the company must be maintained at all times.
  - You must also properly identify your self to all computer systems.
    - Do not attempt to conceal your identity
    - Do not misrepresent the sender as someone else

Slide 7

E-mail Security Policies (cont'd)

- E-mail cannot be used for transmitting, storing, or retrieving any communication that is:
  - Discriminatory or harassing
  - Derogatory to any individual or group
  - Obscene, sexually explicit or pornographic
  - Defamatory or threatening
  - In violation of any license governing the use of software
  - Engaged in for any purpose that is illegal or contrary to Company's policy or business interests.

Slide 8



E-mail Security Policies (cont'd)

- Your e-mail address must not be used in any online discussion forums or message boards
  - Your statements can be construed as representing the company's position
  - May cause unintentional data leaks
    - Reveals the organization for which you work

Slide 9

E-mail Security Policies (cont'd)

- Please do not participate in any of the following:
  - Chain Letters
    - Consume resources and your valuable time
  - Mass Forwarding
    - Consume resources and your valuable time
  - Virus or Malware warnings
    - Usually a hoax
    - Verify at http://www.snopes.com
    - Contact the ISG

Slide 10

E-mail Security Policy Q&A

- Question and Answer Time
- Consult your manager should you have any questions that are not addressed here.

Slide 11

Protecting Yourself from e-mail scams & Identity Theft

- Video Presentation of:
  - *Delivering Justice: Identity Crisis*

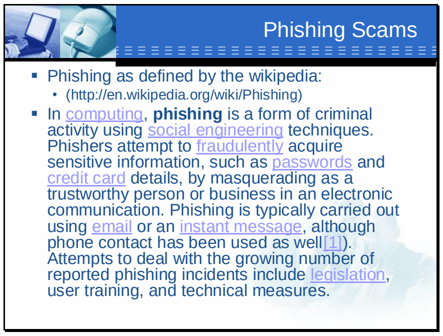
Brought to you by the

United State Postal Inspection Service

Obtain your free copy at:

http://www.usps.com/postalinspectors/dvdorder.htm

Slide 12

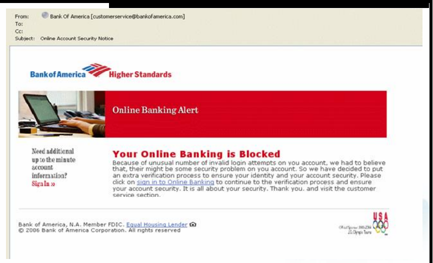


Phishing Scams

- Phishing as defined by the wikipedia:
  - (http://en.wikipedia.org/wiki/Phishing)
- In computing, **phishing** is a form of criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using email or an instant message, although phone contact has been used as well[1]). Attempts to deal with the growing number of reported phishing incidents include legislation, user training, and technical measures.

Slide 13

Spotting a Phishing Scam



From: Bank Of America [customerservice@bankofamerica.com]
To:
Cc:
Subject: Online Account Security Notice

Bank of America Higher Standards

Online Banking Alert

Need additional up to the minute account information?
Sign In »

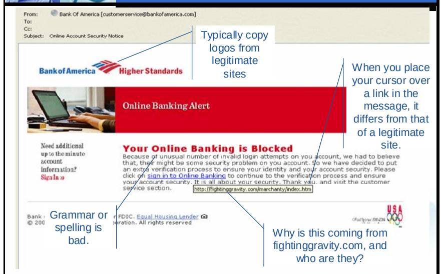
Your Online Banking is Blocked

Because of unusual number of invalid login attempts on you account, we had to believe that, their might be some security problem on you account. So we have decided to put an extra verification process to ensure your identity and your account security. Please click on sign in to Online Banking to continue to the verification process and ensure your account security. It is all about your security. Thank you. and visit the customer service section.

Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2006 Bank of America Corporation. All rights reserved

Slide 14

Spotting a Phishing Scam



From: Bank Of America [customerservice@bankofamerica.com]
To:
Cc:
Subject: Online Account Security Notice

Bank of America Higher Standards

Online Banking Alert

Need additional up to the minute account information?
Sign In »

Your Online Banking is Blocked

Because of unusual number of invalid login attempts on you account, we had to believe that, their might be some security problem on you account. So we have decided to put an extra verification process to ensure your identity and your account security. Please click on sign in to Online Banking to continue to the verification process and ensure your account security. It is all about your security. Thank you. and visit the customer service section.

Bank FDIC. Equal Housing Lender
© 200 ration. All rights reserved

http://fightinggravity.com/marchanty/index.htm

Typically copy logos from legitimate sites

When you place your cursor over a link in the message, it differs from that of a legitimate site.

Grammar or spelling is bad.

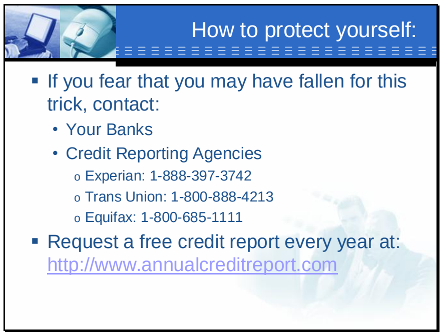
Why is this coming from fightinggravity.com, and who are they?

Slide 15

What do I do?

- Delete the e-mail, do not respond
- Do not click on links in the e-mail
  - Type the address into the address bar
- Banks typically do not send you this type of request in the e-mail
  - May receive notification via phone or postal mail

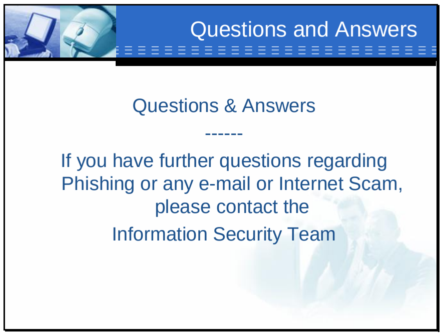
Slide 16



How to protect yourself:

- If you fear that you may have fallen for this trick, contact:
  - Your Banks
  - Credit Reporting Agencies
    - Experian: 1-888-397-3742
    - Trans Union: 1-800-888-4213
    - Equifax: 1-800-685-1111
- Request a free credit report every year at: http://www.annualcreditreport.com

Slide 17



Questions and Answers

Questions & Answers

If you have further questions regarding Phishing or any e-mail or Internet Scam, please contact the

Information Security Team