Information Technology Policy and Procedures

INFORMATION SECURITY PROGRAM

Overview

Hantz Group recognizes the need to maintain an appropriate level of security to safeguard its client's personal information and records. Senior management and the technology staff are responsible for identifying, assessing, prioritizing, managing, and controlling risks. They ensure necessary resources are devoted to creating, maintaining, and testing the program. The senior management fulfills its planning responsibilities by setting policy, prioritizing critical business functions, allocating sufficient resources and personnel, providing oversight, approving the plan, reviewing test results, and ensuring maintenance of a current plan. This program will cover both physical and non-physical issues surrounding the information security for the organization.

Our information security policy outlines a proactive and ongoing program incorporating three components:

- Prevention
- Detection
- Response

Prevention measures include sound security policies, well-designed system architecture, properly configured firewalls, and strong authentication programs. Using vulnerability assessment tools and performing regular penetration analyses will assist Hantz Group in determining what security weaknesses exist in its information systems.

Detection measures involve analyzing available information to determine if an information system has been compromised, misused, or accessed by unauthorized individuals.

Another key area involves a response program to handle suspected intrusions and system misuse once they are detected. This response program will be outlined in another section of this document.

RISK ASSESSMENT/MANAGEMENT

A thorough and proactive risk assessment is the first step in establishing a sound security program. This is the ongoing process of evaluating threats and vulnerabilities, and establishing an appropriate risk management program to mitigate potential monetary losses and harm to the reputation of the Hantz Group. Threats have the potential to harm the company, while vulnerabilities are weaknesses that can be exploited.

The extent of the information security program is commensurate with the degree of risk associated with our systems, networks, and information assets. The extent to which we will contract with third-party vendors will also affect the nature of the risk assessment program.

Performing the Risk Assessment and Determining Vulnerabilities

Performing a sound risk assessment is critical to establishing an effective information security program. The risk assessment provides a framework for establishing policy guidelines and identifying the risk assessment tools and practices that may be appropriate for an institution.

Under certain circumstances the Hantz Group will contract with third-party providers for information system services. When this occurs there are sound oversight programs in place. At a minimum, the security-related clauses of a written contract define the responsibilities of both parties with respect to data confidentiality, system security, and notification procedures in the event of data or system compromise. Hantz Group will conduct a sufficient analysis of the provider's security program, including how the provider uses available risk assessment tools and practices when possible this will include obtaining results of a penetration test.

Items included in our risk assessment program:

- Identifying mission-critical information systems, and determining the effectiveness of current information security programs. For example, a vulnerability might involve critical systems that are not reasonably isolated from the Internet and external access via

modem. Having up-to-date inventory listings of hardware and software, as well as system topologies, is important in this process.

- Assessing the importance and sensitivity of information, and the likelihood of outside break-ins (e.g., by hackers) and insider misuse of information. For example, if a large depositor list were made public, that disclosure could expose the company to reputation risk and the potential loss of deposits. Further, the institution could be harmed if human resource data (e.g., salaries and personnel Files) were made public. The assessment should identify systems that allow the transfer of funds, other assets, or sensitive data/confidential information, and review the appropriateness of access controls and other security policy settings.
- Assessing the risks posed by electronic connections with business partners. The other entity may have poor access controls that could potentially lead to an indirect compromise of the firm's system. Another example involves vendors that may be allowed to access the firm's system without proper security safeguards, such as firewalls. This could result in open access to critical information that the vendor may have "no need to know."
- Determining legal implications and contingent liability concerns associated with any of the above. For example, if hackers successfully access a firm's system and use it to subsequently attack others, the firm may be liable for damages incurred by the party that is attacked.

Our potential threats

Serious hackers, interested computer novices, dishonest vendors or competitors, disgruntled current or former employees, organized crime, or even agents of espionage pose a potential threat to the Hantz Groups computer security. The Internet provides a wealth of information to hackers on known security flaws in hardware and software. Using almost any search engine, average Internet users can quickly find information describing how to break into various systems by exploiting known security flaws and software bugs. Hackers also may breach security by misusing vulnerability assessment tools to probe network systems, then exploiting any identified weaknesses to gain unauthorized access to a system. Internal misuse of information systems remains an ever-present security threat.

Systems can be vulnerable to a variety of threats, including the misuse or theft of passwords. Hackers may use password cracking programs to figure out poorly selected passwords. The passwords may then be used to access other parts of the system. By monitoring network traffic, unauthorized users can easily steal unencrypted passwords. Employees or hackers may also attempt to compromise system administrator access (root access), tamper with critical Files, read confidential e-mail, or initiate unauthorized e-mails or transactions.

Hackers may use "social engineering," a scheme using social techniques to obtain technical information required to access a system. A hacker may claim to be someone authorized to access the system such as an employee or a certain vendor or contractor. The hacker may then attempt to get a real employee to reveal user names or passwords, or even set up new computer accounts. Another threat involves the practice of "war dialing," in which hackers use a program that automatically dials telephone numbers and searches for modem lines that bypass network firewalls and other security measures. A few other common forms of system attack include:

- Denial of service (system failure), which is any action preventing a system from operating as intended. It may be the unauthorized destruction, modification, or delay of service. For example, in a "SYN Flood" attack, a system can be flooded with requests to establish a connection, leaving the system with more open connections than it can support. Then, legitimate users of the system being attacked are not allowed to connect until the open connections are closed or can time out.
- Internet Protocol (IP) spoofing, which allows an intruder via the Internet to effectively impersonate a local system's IP address in an attempt to gain access to that system. If other local systems perform session authentication based on a connection's IP address, those systems may misinterpret incoming connections from the intruder as originating from a local trusted host and not require a password.
- Malware, which are computer programs that may be embedded in other code and can self-replicate. Once active, they may take unwanted and unexpected actions that can result in either nondestructive or destructive outcomes in the host computer programs. The malware program may also move into multiple platforms, data files, or devices on a system and spread through multiple systems in a network. Malware programs may be contained in an e-mail attachment and become active when the attachment is opened.

CONCLUSION

A security program includes effective security policies and system architecture, which may be supported by the risk assessment tools and practices discussed in this paper and appendix. Information security threats and vulnerabilities, as well as their countermeasures, will continue to evolve. As such, the firm should have a proactive risk assessment process that identifies emerging threats and vulnerabilities to information systems.

A sound information security policy identifies prevention, detection, and response measures. The appendix provides more details on risk assessment tools and practices that may be used to improve information security programs. Preventive measures may include regularly using vulnerability assessment tools and conducting periodic penetration analyses. Intrusion detection tools can be effective in detecting potential intrusions or system misuse. However the firm feels that a good response program is as important as prevention and detection.

Intrusion Response

Intrusion detection by itself does not mitigate risks of an intrusion. Risk mitigation only occurs through an effective and timely response. The goal of the response is to minimize damage to the firm and its customers through containment of the intrusion, and restoration of systems

The Network team will be responsible for setting the direction of the intrusion response.

Actions to be taken can include

- Denying access to an intruder, possibly by disconnecting the affected system from the network and shutting down the system
- Containing an intrusion and limiting the actions of an intruder
- Continuing operation to gather additional information
- Restoring the affected system.

Containment Strategy

- Analyzing all available information to characterize the intrusion, including assessing the damage and extent of an intrusion and an intruder's activities.
- Search for additional compromised systems
- Communicate with all parties that need to be aware of an intrusion and participate in handling it, taking into account that an intruder may be able to access and monitor our means of communication.
- Collect and protect information associated with an intrusion.
- Contain the intrusion and determine what actions to take.

Restoration Strategy

- Eliminate the intruder's means of access and any related vulnerabilities.
- Restoration of systems, programs and data to known good state.
- Returning the systems to normal operation.
- Follow up including performing a post mortem review of events as they occurred and reviewing your policies and procedures

Password Policy

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Hantz Group's entire corporate network. As such, all Hantz Group employees (including contractors and vendors with access to Hantz Group systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Hantz Group facility, has access to the Hantz Group network, or stores any non-public Hantz Group information.

Policy General

- All production system-level passwords must be part of the InfoSec administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.
- No user-level password can be reused for 5 consecutive resets.

General Password Construction Guidelines

Passwords are used for various purposes at Hantz Group. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. The firm’s policy is to require a separate log in to access customer data then to log on to the network. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than six characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "Hantz Group", "Southfield", "Michigan" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the
- password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Required elements for a Hantz Group password:

- The password is at least eight characters long.
- The password cannot contain three or more characters from your account name.

Password must contain characters from at least three of the following four categories:

- English uppercase characters (A – Z)

- English lowercase characters (a – z)
- Base 10 digits (0 – 9)
- Non-alphanumeric (for example: !, $, #, or %)

NOTE: Do not use either of these examples as passwords!

Password Protection Standards

Do not use the same password for Hantz Group accounts as for other non-Hantz Group access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Hantz Group access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share Hantz Group passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Hantz Group information. Working on computer that you are not logged on to is the same as using someone else's password.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system

(including Palm Pilots or similar devices) without encryption.

Change passwords at least once every three months. The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to InfoSec and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by InfoSec or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Application Development Standards

Application developers must ensure their programs contain the following security precautions.
Applications:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

Passwords and HIPPA

Access Control Standard
The unique user identification implementation specification is part of the access control standard. The access control standard seeks to ensure that only authorized individuals have the ability to access the Personal Health Information (PHI) that is stored on a covered entities computer systems. Note that this standard is classified as a technical safeguard and is intended to be applied to electronic methods of access (as opposed to physical, which is covered in its own section). The text from the final rule that describes access controls is as follows: (a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in

§ 164.308(a)(4). The reference to § 164.308(a)(4) discusses that the access controls implemented are expected to be used to enforce the access permitted by the administrative safeguards. In short, this means that only individuals who have been given the administrative authority to view PHI are able to do so and that when accessed electronically, this access is enforced based upon the implementation specifications that the Access Control Standard requires.
Unique User Identification (Required) – Implementation Specification
The specification requires that users have a unique login account for electronic access to PHI. The text from the HIPAA legislation reads as follows:
(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.
The intent with this implementation specification is that each user has a unique login account. The point of doing this is so that electronic audit logs that identify PHI access can be tied to a single user to assist in identifying individuals who are attempting to or who have accessed PHI despite no administrative authority to do so and to be able to enforce this administrative authority. Related implementation specifications include termination procedures, log-in monitoring, password management, access authorization and access establishment and modification.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Response to a compromised password

The Network administrator will be responsible for setting the direction of the intrusion response.

Actions to be taken can include

- Denying access to the effected employees, by locking them out of the system
- Limiting the effected employee’s access.
- Continuing operation to gather additional information
- Restoring the affected employees system.

Containment Strategy

- Analyzing all available information to characterize of the situation including assessing the damage and extent of possible intrusion and an intruder's activities.
- Search for additional compromised systems
- Communicate with all parties that need to be aware of a compromise and participate in handling it, taking into account that an parties may be able to access and monitor our means of communication.
- Collect and protect information associated with the compromise.
- Contain the compromised systems and determine what actions to take.

Restoration Strategy

- Eliminate the employee’s means of access and any related vulnerabilities.
- Restoration of systems, programs and data to known good state.
- Returning the systems to normal operation.
- Follow up including performing a post mortem review of events as they occurred and reviewing your policies and procedures

Assessment of policy

By industry standards the firm’s policy would be considered a strong policy. When implemented correctly it offers a very good level of security, although it does have some inherent risk. Forced to change passwords often and to make them complex on some occasions promotes documenting passwords and leaving them in plain site. Management will need to be observant and discourage this practice.

There are other methods available today that would be considered a higher level of security than our current policy. These methods would add significant cost for little additional security at this time.