Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

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

Humans... The Overlooked Asset

Humans often represent the most important component of the information system and are chronically responsible for either the failure or the robustness of the information system. Organizations frequently seek to evaluate, select and employ a variety of controls so as to maintain a secure Information System. In order to have the best operational information system, you must appreciate humans as the most valuable information asset. Pursuant to this perspective, we seek to understand the nature of humans when handling info...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Humans… The Overlooked Asset

GIAC (GSEC) Gold Certification

Author: Muhammad EL-Harmeel, Muhammad.Elharmeel@Gmail.com
Advisor: Becky Fowler

Accepted: November 1st 2009

Abstract

Humans often represent the most important component of the information system and are chronically responsible for either the failure or the robustness of the information system. Organizations frequently seek to evaluate, select and employ a variety of controls so as to maintain a secure Information System. In order to have the best operational information system, you must appreciate humans as the most valuable information asset. Pursuant to this perspective, we seek to understand the nature of humans when handling information. Factors to be considered include: vulnerabilities within humans, threats that could exploit those vulnerabilities, applicable controls and finally pondering them as a key element in an efficient information system. This assertion raises a question about what should be done in order to make the best use of humans as a business enabler supporting the pillars of a professional business environment.

© 2010 SANS Institute, Author retains full rights.

1. Introduction

1.1. "***When the map and the territory don't agree, always believe the territory***" Gause and Weinberg – describing Swedish Army Training.

The above quote describes a critical issue that we often face. When it comes to reality, you will be astonished of how far you are away from the ideal scenario. By mapping this to an operational information system, it is anticipated that the system will have deviation from the ideal posture. What is written in your security policy is not necessary what is implemented in the reality. Humans represent about sixty percent of the system; they are the operators of the system, assets in the system and at the same time controls that are supposed to secure the system. Thus, failure to successfully understand the nature of such asset will make the system deviate from its ideal secure posture and can seriously impact the system.

The purpose of this paper is to highlight controls that are applicable to humans from a risk management perspective and to help understand the nature of humans, which is critically important to secure an information system.

1.2. Limitations

The second and third sections of this paper discuss a sampling of possible human vulnerabilities and threats but do not represent an exhaustive list. This paper mainly addresses the applicable controls rather than vulnerabilities & threats.

1.3. Target Audience

This paper is meant for personnel who are charged with maintaining and operating the Information System within an organization and those who are responsible for providing information security awareness sessions for employees. The goal is to help information security professionals implement and manage the most appropriate controls applicable to humans to best meet the organization's mission and business needs.

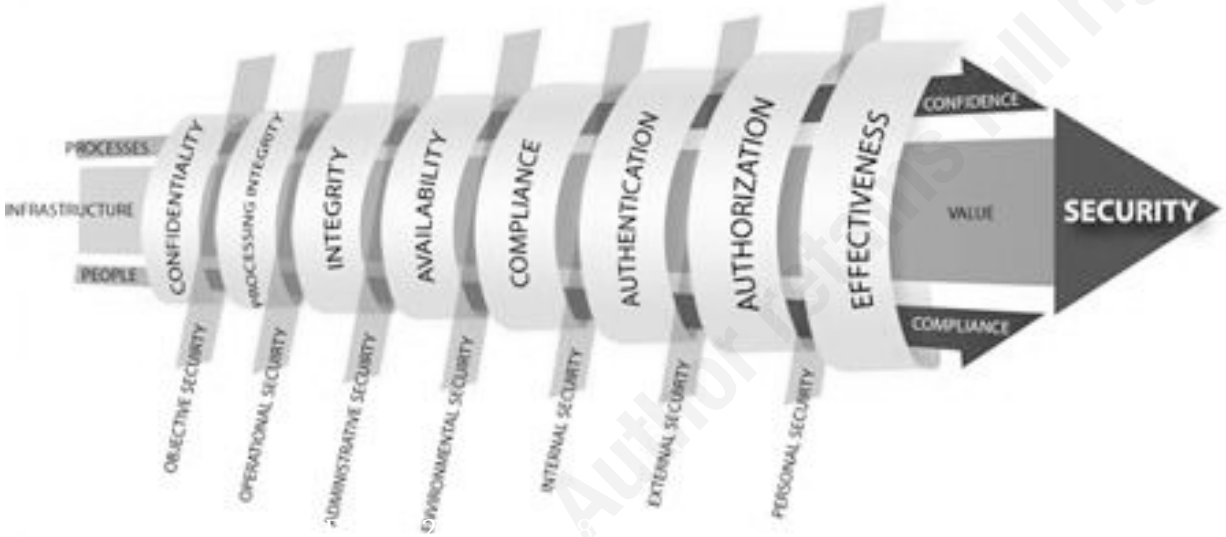
Muhammad EL-Harmeel, Muhammad.Elharmeel@Gmail.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

2. Human as Assets

2.1. Definitions

2.1.1. Information Security [1]



Information Security Model - (ATKTECHK, 2009)

Preservation of confidentiality, integrity and availability of information; in addition other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved. [BS ISO/IEC 27002:2005].

2.1.2. Asset

Anything that has value to the organization. [ISO/IEC 13335-1:2004].

[1] *Note*. From "BS ISO/IEC 27002:2005" by British Standards Institute, Terms and Definitions, p. 1. Copyright by BSI. Reprinted with permission

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

2.1.3. Vulnerability

A weakness of an asset or group of assets that can be exploited by one or more threats. [ISO/IEC 13335-1:2004].

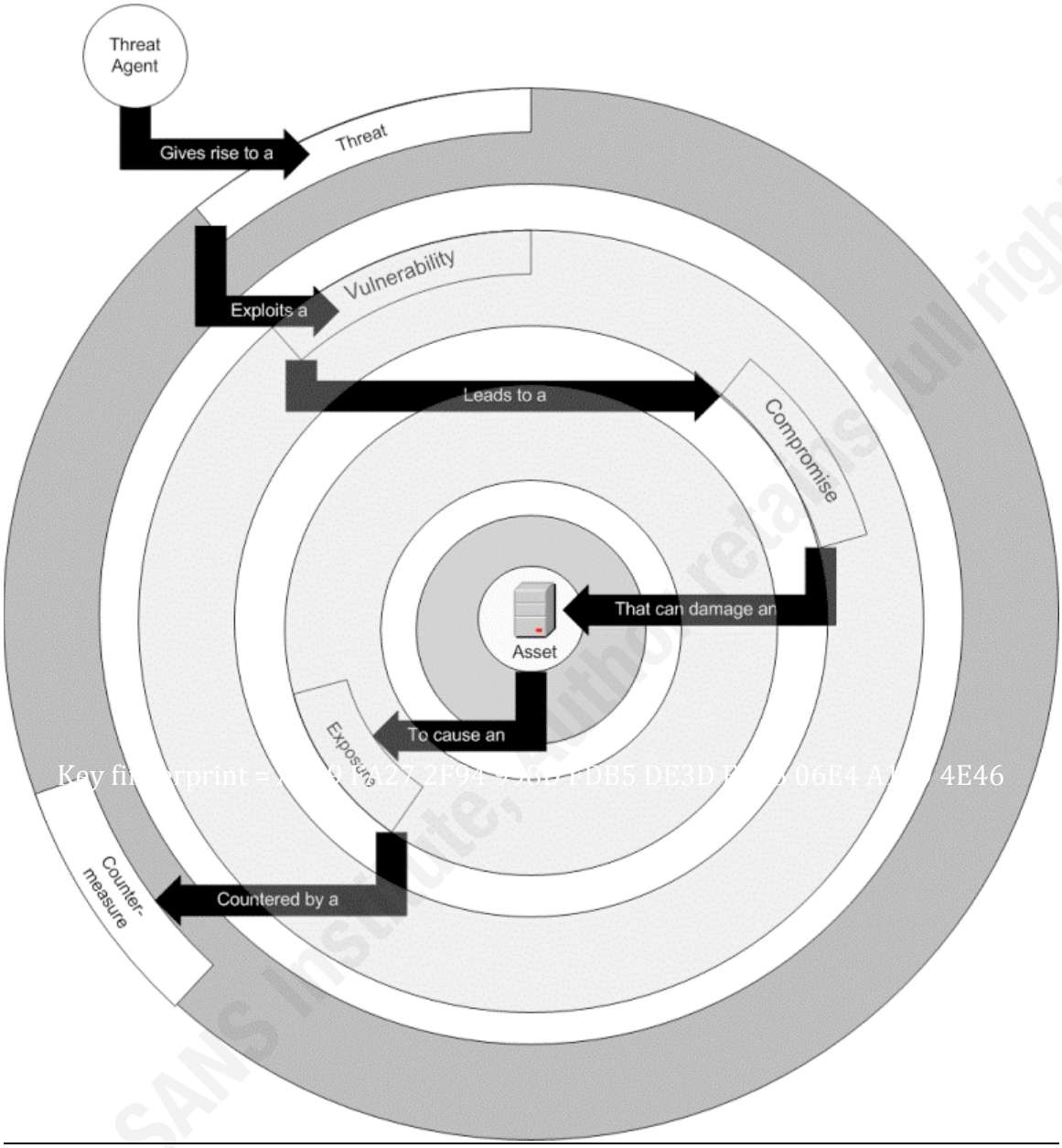
2.1.4. Threat

A potential cause of unwanted incident, which may result in harm to a system or organization. [ISO/IEC 13335-1:2004].

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

The following model demonstrates the relation between assets, vulnerabilities and threats.



Threat-Vulnerability-Asset Model - (Microsoft TechNet, 2009)

A single asset can have multiple vulnerabilities and the same concept applies to threats as a single vulnerability can be exploited by multiple threats. According to this perspective there are a vast diversity of patterns that should be analyzed on an individual basis to determine the risk.

Muhammad EL-Harmeel, Muhammad.Elharmeel@Gmail.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

2.1.5. Security Controls

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.. [NIST SP800-53].

2.1.6. Risk Management

Coordinated activities to direct and control an organization with regard to risk [ISO Guide 73:2002].

2.2. Human Vulnerabilities

Human vulnerabilities are common types of vulnerabilities that reside in the information system. The key characteristic of human vulnerabilities is that they are caused by humans. It can be defined as a shortcoming in a human's attitude or behavior that may lead to violation of the information system's security policy.

Human vulnerabilities are associated with bad habits and attitudes. Those habits and attitudes could be exploited by multiple threats, thus it is critical to evaluate humans in the information system from an attitude perspective. Bad habits such as carelessness, ignorance and low level of awareness are classic examples of such attitudes.

The following table will demonstrate some human vulnerabilities in addition to examples of threats that may exploit them. Needless to say a single vulnerability can be exploited by multiple threats.

Vulnerability	Could be exploited by
Negligence	**Technical threats, Worm.** A reckless administrator who has overlooked updating the antivirus engine will be infected with a newly developed worm. (Schoenberg, 2009)
Fear From Authority	**Spoofing & impersonation** An employee getting a call from an outsider who impersonates a high authority person – General Manager – requesting to reset his own password. Instead of asking this outsider to prove his identity by requesting a password reset through official mail, the employee responds to this request

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

	immediately especially if the intruder was pushing. (Gragg,2009)
Insufficient security training	**Phishing** The most common form of phishing is when a user receives an email that claims to be from his bank asking him to reset or confirm his credentials. Once the victim opens the link he will be redirected to a fake website exactly like the original banking website. He will be asked to enter his credentials which are sent directly to the attacker rather than the real account.
Unmotivated or disgruntled staff	**Misuse of information processing facilities** An angry former employee may try to do damage to the facilities or equipment of the organization as a way to seek revenge. (Kratt, 2009)
Natural Tendency to be Helpful	**Tailgating** There are a wide range of examples that can demonstrate how this vulnerability could affect physical security. One could be pretending to be carrying a heavy load and need help to open the door. Human nature and courtesy may cause someone to open the door without even checking an ID. (Stevens, 2009)

One last thing to highlight is the importance of having a methodology and a systematic way for identifying human vulnerabilities, especially in the dynamic information systems commonly found in large organizations. These organizations will probably be subject to frequent changes in workforce levels.

One proposed way for identifying human vulnerabilities is to conduct a human-based penetration test.

A human based penetration test follows the same methodology as a network based penetration test as defined in the below diagram

Muhammad EL-Harmeel, Muhammad.Elharmeel@Gmail.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

The main difference is the target. A human based penetration test targets humans only while a network based penetration test targets technical vulnerabilities such as those found in routers and switches. Human based penetration tests try to reveal critical security issues within humans (most probably bad habits) that may lead to a security breach. The following steps will show how this model could be applied to humans.

- **Reconnaissance:** getting as much information about the victim from public and social networking websites.
- **Scanning**: spotting the best entrance that matches the victim's character such as curiosity and natural tendency to be helpful.
- **Gaining Access**: using social engineering to exploit the addressed vulnerability.
- **Maintaining Access**: building a trust relationship with the victim for later use if needed.
- **Clearing Tracks**: getting rid of any evidence used earlier that might lead to the identity of the perpetrator

Muhammad EL-Harmeel, Muhammad.Elharmeel@Gmail.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

2.3. Threats Affecting Humans

Human threats can be defined as threats that, when triggered, will affect human beings regardless of their source (such as illness). It is important to highlight that a threat doesn't hold any potential impact or damage on the information system unless there is a vulnerability that can be exploited.

As stated previously, this paper's scope is risk management issues that are related to humans. As a result, we will highlight only possible threats that are applicable to the asset being evaluated which is humans.

Threat-Source	Motivation	Threat Actions
Hacker, Cracker	• Challenge • Ego • Rebellion	• Social Engineering
Computer Criminal	• Destruction of information • Illegal information disclosure • Monetary gain • Unauthorized data alteration	• Fraudulent act (e.g., impersonation) • Information bribery • Spoofing
Terrorist	• Black mail • Destruction • Exploitation • Revenge	• Bomb-terrorism • Information Warfare
Industrial espionage	• Competitive advantage • Economic espionage	• Information theft • Intrusion on

Muhammad EL-Harmeel, Muhammad.Elharmeel@Gmail.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

		personal privacy • Social engineering • Economic exploitation
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	• Curiosity • Ego • Intelligence • Monetary gain • Revenge • Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Browsing of proprietary information • Information bribery • Sale of personal information • Blackmail

Human Threats - (NIST Special Publication 800-30, 2009)

Different formulas are out there to calculate the risk (i.e. **Total Risk = Threats x Vulnerability x Asset Value= Probability X Consequence= Threat X Vulnerability X Consequences**…..etc). The above table spots a new factor that should be involved in calculating the overall risk which is **Motivation**.

It is unlikely that a threat can successfully exploit a vulnerability without motivation. Motivation is the engine that reinforces a threat to successfully penetrate the information system and exploit a vulnerability.

Muhammad EL-Harmeel, Muhammad.Elharmeel@Gmail.com

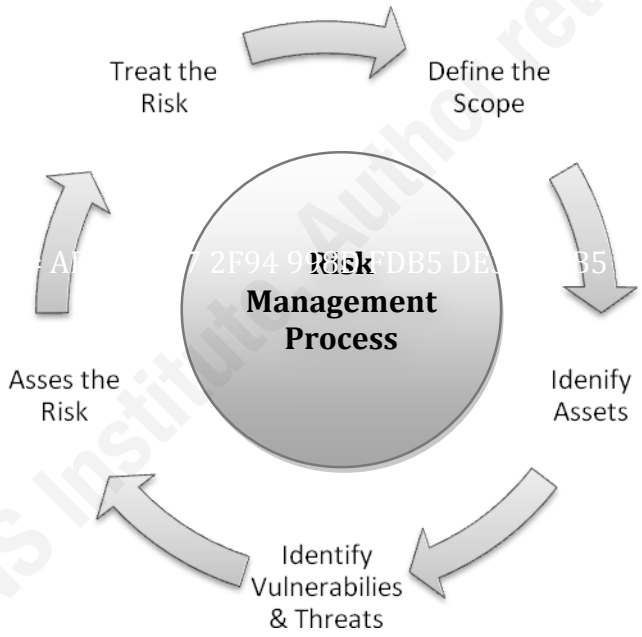
© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Why do hackers target highly sensitive and secure targets like military networks, security vendor's websites, and media websites? The simple answer is **motivation.** This category is alluring to hackers and generates a strong motivation to carry out the attack. Thus, we have to pay attention to **motivation** when carrying out the risk assessment.

It worth mentioning that the above list is a sample list and not an exhaustive one. Every organization has its own business circumstances that generate a unique spectrum of threats.

2.4. Handling Resultant Risks

Prior to discussing the options available to handle human based risks, it is necessary to understand the basics of the risk management process.



Risk Management Process Model - (IT Service Strategy, 2009)

2.4.1. The Process

The above diagram shows that there are four phases that govern the risk management process.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

- **Defining the scope**

  A predefined scope should exist before conducting the risk assessment. The scope sets the scene for what will be involved in the risk assessment. The scope can be the whole organization or even just a business process.

- **Identify assets**

  The assets that are within the scope of the information system, coupled to their owners, should be identified and placed in an asset inventory. Moreover, assets should properly valued against a predefined scale matrix.

- **Identify vulnerabilities & threats**

  Each asset is associated with one or multiple vulnerabilities and those vulnerabilities could be exploited by one or multiple threats. Vulnerabilities and threats associated with each asset should be listed.

- **Assess the risk**

  Each threat-vulnerability pair (the possibility of specific threat exploiting a specific vulnerability) - has an impact on the information system. This impact should be calculated and evaluated based on the likelihood of occurrence.

- **Treat the risk**

  At this stage, we are supposed to choose an option to handle the resultant risks associated with humans.

© 2010 SANS Institute, Author retains full rights.

2.4.2. Avoidance

Consider eliminating the key source of the risk. This may be associated with aggressive business decisions. One example could be to dismiss an employee in case of repeated failure to raise his information security awareness level. The employee might be

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

exercising bad security oriented- habits that are exposing the information system to a certain danger.

2.4.3. Reduction

Two options are available to reduce the risk:

- One is to reduce the likelihood of the vulnerability being exploited (i.e. consider a deterrent action for any employee behavior which breaches the policy. The goal of this option is to make people more advertent, hence, minimizing the possibility of being vulnerable).
- The second option is to reduce the impact. An example would be moving an employee who deals with sensitive date from one department to another department where he will deal with less sensitive data. By doing so, if a threat was able to exploit a vulnerable behavior within this employee, then, it will have less impact on the information system.

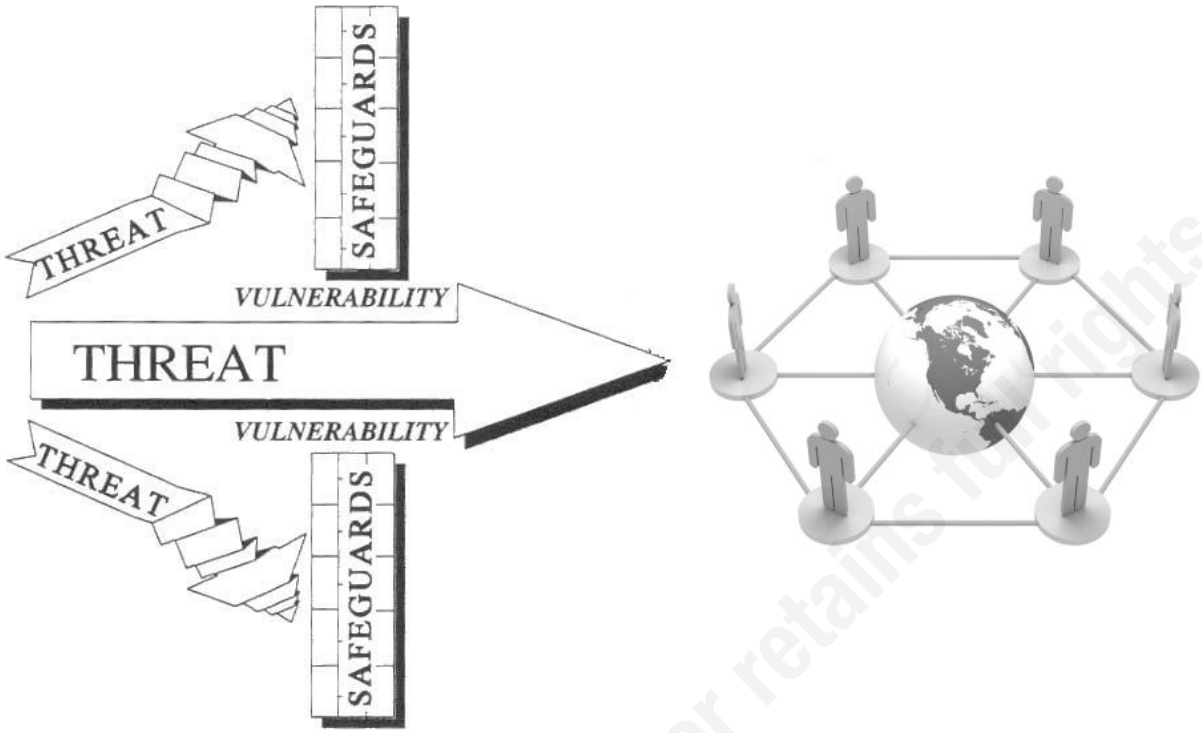
2.4.4. Retention

Another option is to accept the potential risk as it is. In certain cases the organization has no option rather than accepting the risk when dealing with human vulnerabilities. For example, a member of senior management may be unable or unwilling to completely abide by the security policy. In this scenario, this manager poses a potential risk for the organization and for business reasons it is not feasible to avoid (dismiss him) or reduce – (either punishing or moving him) the risk.

2.5. Applicable Controls

It is anticipated that each system will have its own vulnerabilities and threats. We are required to prevent threats from exploiting present vulnerabilities within the system. This is supposed to be accomplished using controls. The following chart illustrates how controls can prevent threats from exploiting present vulnerabilities in the information system.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.



Threat:Control Relation - (NIST SP 800-12, 2009)

Now that the security risks have been identified and categorized it is time to select the appropriate control if one makes the decision to reduce the risk.

Again, this section will handle different controls that are specific to humans. These are commonly referred as management security controls.

According to NIST SP 800-30 publication, the following categorizations can be applied to management security controls

Preventive Controls	Detective Controls	Recovery Controls
• Assigning security responsibility to ensure that adequate security is provided for the mission-critical IT	• Personnel clearance, background Investigations &	• Provide continuity of support and develop, test, and maintain the continuity of Personnel operations

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

personnel (i.e. firewall administrator) • Developing and maintaining personnel security plans to document current controls and address planned controls for personnel in support of the organization's mission. • Considering implementing Separation of duties and least privilege concepts. • Conducting security awareness and technical training to ensure that personnel are aware of the rules of behavior and their responsibilities in protecting the Organization's ission. • Authentication, authorization and non-repudiation (personnel oriented functions,	rotation of duties. • Conducting periodic review of security controls – previously applied to personnel- to ensure that the controls are effective. • Performing periodic information system audits (people oriented audit such as trying to navigate the building without the ID and see if this will be caught or not). • Conducting ongoing risk management to assess and mitigate risk related to personnel.	plan to provide for business resumption and ensure continuity of operations during emergencies or disasters (i.e. ensuring the existence of delegates who can do the job in case of the original employee unavailability) • Establishing an incident response capability to prepare for, recognize, report, and respond to the incident and return the employees to operational status.(i.e. after an earthquake, each employee must know what to do to continue operate critical functions)

Muhammad EL-Harmeel, Muhammad.Elharmeel@Gmail.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

such as verifying the identity of an employee by security guard and ensuring that he has the appropriate authority) • Controlling the humidity and temperature of the facility to ensure personnel safety (i.e., operation of air Conditioners, heat dispersal).	• Using motion detectors, closed circuit television monitoring, sensors and alarms to monitor and detect personnel activities.	

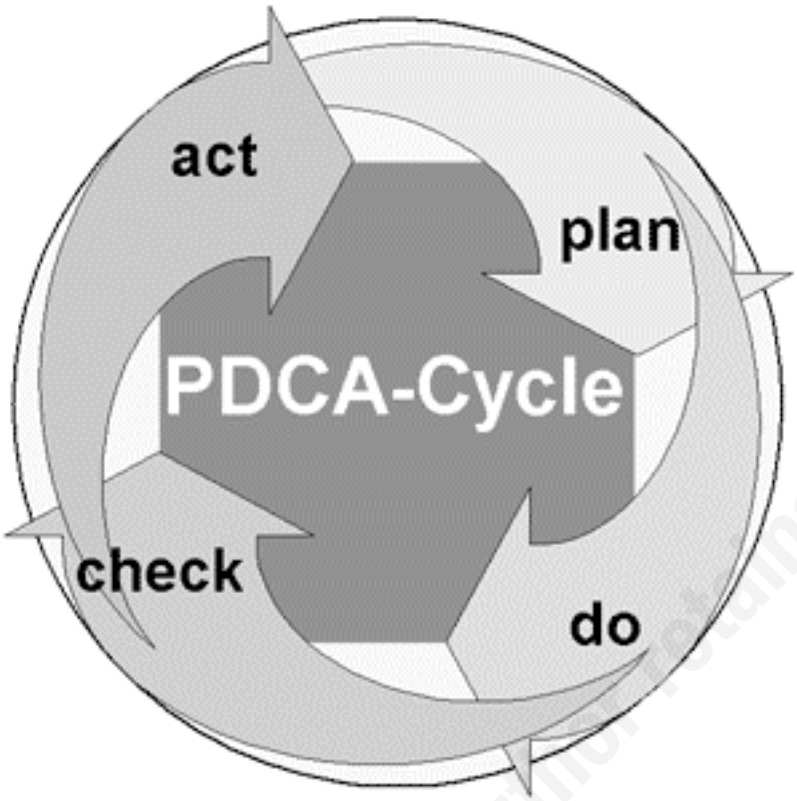
Operating one of the above controls requires continual improvement in order to reach the maturity level required of the information system.

2.6. Continual Improvements

Each system needs to reach a specific level of maturity. To get this done, continual improvement must be exercised. Moreover, with continual improvement in place we can expect quality enhancement.

The continual improvement lifecycle is composed of the following stages:

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.



PDCA Lifecycle - (DHM, 2009)

Plan: Identifying problems and proposing solutions.

Do: Implement the proposed solutions to better enhance the system performance and operations. Most probably on a small scale.

Check: Testing the system for the effectiveness of the deployed controls and implemented solutions.

Act: Involving other solutions and controls that are supposed boost the system operations, secure the system and at the same time excluding any solutions that proved to be inefficient in tackling current shortcomings in the system.

In most circumstances, the information system itself will continually be expanded (new hires), updated (continuing staff education) and its components changed or replaced (rotation of duties). Moreover, security policies are likely to change over time. These significant changes mean that new risks will surface and human-based risks previously

Muhammad EL-Harmeel, Muhammad.Elharmeel@Gmail.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

mitigated may again become a concern. Thus, the risk management process is ongoing and evolving.

3. Conclusion

Contrary to popular belief, humans should be considered the most valuable asset within the information system. Like any other asset, they should be identified, categorized based on threat-vulnerability analysis and decisions should be made about the best methodology to tackle the risk they present. It is unlikely that an effective and secured information system could exist without considering humans as the most valuable information asset in the system. Thus, it is imperative that organizations take this matter seriously by taking into consideration that a variety of controls could be applied to humans.

Through this paper we have pinpointed humans as a key element in the information system. Examples have been given of different types of vulnerabilities that might coexist with humans and how to highlight them by conducting a human based penetration test; this was followed by a detailed list of threats that might exploit human vulnerabilities and the relationship that could coexist between them. Also we have introduced a new function –motivation- that should be considered in the risk calculation formula. Finally we have gone through different options available to tackle human risks and how to maintain an efficient and healthy the information system by applying PDCA lifecycle.

Muhammad EL-Harmeel, Muhammad.Elharmeel@Gmail.com

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

4. References

Gulati, Radha. (2003). *The threat of social engineering and your defense against it*. SANS reading room. Retrieved from: http://www.sans.org/reading_room/whitepapers/engineering/the_threat_of_social_engineering_and_your_defense_against_it_1232

Arthurs, Wendy. (2001). *A proactive defense to social engineering*. SANS reading room. Retrieved from: http://www.sans.org/reading_room/whitepapers/engineering/a_proactive_defence_to_social_engineering_511

Jones, Chris. (2003). *Understanding and Auditing*. SANS reading room. Retrieved from: http://www.sans.org/reading_room/whitepapers/engineering/understanding_and_auditing_1332

Granger, Sarah. (2001). *Social Engineering Fundamentals*. Security Focus. Retrieved from: http://www.securityfocus.com/infocus/1527

Schoenberg, Carter. (n.d.) *Information Security & Negligence Targeting the C-Class*. Retrieved from: http://www.infosecwriters.com/text_resources/pdf/InformationSecurityCClass.pdf

Schneier, Bruce. (2009, January 9). *Impersonation*. Message posted to: http://www.schneier.com/blog/archives/2009/01/impersonation.html

HCi. *From problem-faced to problem-solved.* Retrieved from: http://www.documentation.com.au/hcisite2/toolkit/pdcacycl.htm

Gragg, David. (2002). *A Multi-Level Defense Against Social Engineering*. SANS reading room .Retrieved from: http://www.sans.org/reading_room/whitepapers/engineering/a_proactive_defence_to_social_engineering_511

Kratt, Heather. (2004). *The Inside Story: A Disgruntled Employee Gets His Revenge*. SANS reading room. Retrieved from:

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

http://www.sans.org/reading_room/whitepapers/engineering/the_inside_story_a_disgruntled_employee_gets_his_revenge_1548

Gause and Weinberg. (n.d.). *Describing Swedish Army Training*. Risk Management Quotes. Retrieved from: http://riskviews.wordpress.com/risk-management-quotes/

© 2010 SANS Institute, Author retains full rights.

Muhammad EL-Harmeel, Muhammad.Elharmeel@Gmail.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 1st, 2015

Upcoming SANS Training

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

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced