International Journal of Computer and Information Technology (ISSN: 2279 – 0764)
Volume 04 – Issue 05, September 2015

Human Factors in Information Security

Alphonso Price
College of Arts & Sciences, Regent University
1000 Regent University Drive
Virginia Beach, VA 23464-9800 U.S.A

Young B. Choi
College of Arts & Sciences, Regent University
1000 Regent University Drive
Virginia Beach, VA 23464-9800 U.S.A
Email: ychoi [AT] regent.edu

Abstract— **We will look at some important issues concerning insider threats to information security from employees who may unwillingly played a crucial role in causing major accidents to an organizations information systems. A computer security system, no matter how flawlessly designed and implemented, there will be human error involved. We will address some appropriate technical measures to implement in protecting an organizations information system and ways in designing and creating healthy security policies for all staff members. We will briefly cover personality mannerisms, individual differences, mental abilities and behavior risks. We will also focus on the training and education level, and information security awareness among company employees and staff members.**

Keywords-human factors; information security; computer security; insider threats; information systems protection

I. INSIDER THREATS

Many organizations from the past have been trying to develop techniques to safeguard corporate data from data breaches and any other occurrences where information is taken without authorization. "While many businesses have focused on improving their protections against external cyber-attacks, far fewer have adequate internal protection in place to guard against malicious actions by their own staff" [1]. It's hard enough for organizations to come up with a game plan to try and stop cyber-attacks and hackers from breaching their firewalls, gaining access to their networks and stealing vital information. The financial strain that is placed on many of these corporations is overwhelming. General consensus has the majority of society think threats too many of the businesses would come from malicious hackers who are prowling the wire looking for a way in. Businesses will spend majority of their emphasis on trying to keep the enemy out while the enemy is actually an insider, an employee, staff member or contractor who has been granted access to the company networks who is in the position to become an even greater threat to the corporation. "Late 2013, Vodafone Germany confirmed that an attacker with insider knowledge had stolen the personal data of two million of its customers from a server located in Germany. Customer name and address and date-of-birth information and some bank account details were taken. In this case Vodafone identified the perpetrator as an insider with knowledge of its most sensitive internal systems. Vodafone claims to have up-to-date and well maintained security systems, but still fell victim to what the company described as "a highly complex attack that was conducted with inside knowledge of its most secure internal systems [1]. Employees of corporations who have access to highly sensitive and classified data have the greatest advantage to cause harm, whether it's accidental or malicious. They are the trusted employees, staff members and contractors who are given access to all sorts of information and they are expected to protect and not misuse that information. "Organizations must balance the need to access information for conducting business with protecting this information from unauthorized misuse by trusted personnel. Unauthorized access to sensitive information is routinely considered as an external threat [2]. Plus there is the notion that accidents happen which can lead to an accidental breach, misplaced classified data, or vital information may have been compromised. "The insider threat takes two forms: accidental and malicious, both can compromise corporate assets, including its information [2]. Then there are the unintentional threats "such as walking away from a workstation without locking a session, not securing passwords, or misuse of system procedures due to improper training, which can lead more serious compromises [2]. Accidental threats are not uncommon in the work place; they are bound to happen anytime, anyplace and anywhere. "A recent survey of Defense Department IT professionals found that 55 percent said careless and untrained insiders are the greatest source of threats to their agencies' IT security. And while 66 percent said malicious insider threats could be as damaging or more than external attacks, 56 percent also said the damage done by careless insiders could be just as bad those caused by malicious insiders [3]. Most of the data breaches that occur are pretty much caused by accidental and carelessness on part of an employee of that organization or a contractor; it is even noted that there has been a rise in this phenomenon. "The FBI this week issued a warning to companies about a rise in hacking by current and former employees. Insider threats, both intentional and accidental, were cited by more than 70 percent of information security managers as their biggest

concern in an April survey [4]. Having careless and untrained employees can be considered a great threat to organizations; some workers may be naive or susceptible to social engineering attacks or victimized by other employees who may have reprimanded, looked over for a promotion or terminated. These individuals could quite easily become targets of malicious software and hacking techniques inflicted on by disgruntle employees. Some may even use their co-workers computer that may have been compromised and used the compromised machine as some sort of a launching pad to further attack unprotected systems and cause harm and financial damage to the organization. "The most costly data breaches are usually those that are created by a malicious insider. These people normally have access to things external hackers generally don't have access to [4]. Having to deal with colleagues who display malicious intent creates a toxic work environment; thus making it difficult for employees to perform their assigned tasks is hard to prove to supervisors and upper management sometimes of what is going on. "Nearly two-thirds (64%) believe malicious insider threats to be as damaging as or more damaging than malicious external threats, such as terrorist attacks or hacks by foreign governments. Further, 57 percent believe breaches caused by accidental or careless insiders to be as damaging as or more damaging than those caused by malicious insiders [5]. Malicious insiders come in all sorts of shapes, sizes and colors, but there are a number of ways of detecting these callous frauds. Let's take a look at some ways a malicious insider can be detected, both non-technical and technical: **"**The not-so model employee – This individual has been consistently the first in and last out of the office lately. There's a lot of work to do so this individual is pulling some long hours. If there isn't a project due soon, this could be an indicator that the individual is working on a little *extra-curricular* malicious work [6]. Then there is **"**The Ironman streak – An individual who hasn't taken a vacation in a long time may not have had the opportunity to share his or her work with others. If they are keeping their work to themselves without collaborating or having others review, there is a chance that their project is of that *extra-curricular* malicious nature [6]. These are the types of threats most co-workers and executive staff would have such a hard time detecting, let alone suspect that there was a threat from inside coming from one of their own. Countless organizations are mindful of the numerous external threats that constantly tries to attack from outside. Fortunately these organizations are stepping up their efforts in combatting this movement of illegal activity. Many have put in place the typical countermeasures such as Intrusion Detection Systems (IDS), antivirus software, and firewalls, which are all directed at these unwanted threats. However these counter measures offer so little to counter that unsuspecting greater threat, which is that malicious insider who has no morals or ethics and who will stop at nothing in trying to sabotage the organization. Unintentional threat has become an increasing problem for many organizations. Let's take a look at the definition of what an Unintentional Insider Threat (UIT) is "An unintentional insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information of information systems [8]. "For example, about a year ago, spear phishers from China infiltrated the *New York Times* website in hopes of gaining access to names and sources that Times reporters had used in a story. A year earlier, Google pulled more than 22 malicious Android apps from the market after they were found to be infected with malware. This year, security blogger Brian Krebs reported that "The breach at Target Corp. that exposed credit card and personal data on more than 110 million consumers appears to have begun with a malware-laced email phishing attack sent to employees at an HVAC firm that did business with the nationwide retailer, according to sources close to the investigation. The Target breach spear phishing attack is an example of social engineering and illustrates how an unintentional threat can cause harm to any organization [7]. It is not easy to know the details of an organization can stop these threats and/or mitigate the risks posed by these individuals. We certainly hope the right kind of technical and non-technical combination is utilized to thwart this unorthodox behavior. "Security awareness training needs to be updated on a constant basis and implemented throughout the organization; this should be something that is mandatory. Employees and all contractors should be directed to sit through some form of training. There are also unintentional threats that are uncontrollable due to certain circumstances which may include employees being tricked into providing classified information, hardware and software failures in which the equipment may not work properly, human errors known as mistakes that employees may make by leaving their accounts open or losing company provided laptops and the most destructive unintentional threat of them all are natural disasters like hurricanes, tornadoes and blizzards [9].

II. COMPUTER SECURITY SYSTEMS

"When it comes to computer security, the problems most companies experience can be traced to the biological units that interface with their systems. Otherwise known as humans, and with humans come errors [10]. Human operator error has been the cause of many failures and loss of data in numerous IT departments of major corporations. It seems as though computer security is either not strong enough or personnel using the computers are inadequately trained. "Only 54% of companies offer some form of cybersecurity training, with the format most often being new employee orientation or some kind of annual refresher course [10]. These mistakes have cost corporations millions in finances, corporate unpredictability, and communications paths have been

disrupted; "heavily regulated fields including healthcare, finance and pharmaceuticals incurred breach costs that were 70% higher than other industries [11]. Investing in infrastructures that can handle human errors should be near the top of the priority list, but lately in the media they have mostly been discussing all the data breaches that have been caused by human errors, inadvertent data dumps, and transfers. "Together, human errors and system problems account for 64% of data breaches in the global study, while prior research shows that 62% of employees think it is acceptable to transfer corporate data outside the company – and the majority never deletes the data, leaving it vulnerable to leaks [11]. Having a strong computer security defense on your computers, networks and maybe even your smart phone should help protect against accidental or unauthorized access from anyone. There are a vast amount of threats to computer security that can cause serious damage unfortunately most of these threats come from human error. "Trojan is one of the most complicated threats among all. Most of the popular banking threats come from the Trojan family such as Zeus and SpyEye [12]. "A Trojan has the ability hide itself from antivirus detection and steal important banking data to compromise your bank account [12]. "Looking back 10 years in technology, virus is something really popular. It is a malicious program where it replicates itself and aim to only destroy a computer. The ultimate goal of a virus is to ensure that the victim's computer will never be able to operate properly or even at all (12]. "Worms, one of the most harmless threats where it is program designed only to spread. It does not alter your system to cause you to have a nightmare with your computer, but it can spread from one computer to another computer within a network or even the internet [12]. "Spyware is a Malware which is designed to spy on the victim's computer. If you are infected with it, probably your daily activity or certain activity will be spied by the spyware and it will find itself a way to contact the host of this malware. Mostly, the use of this spyware is to know what your daily activity is so that the attacker can make use of your information [12]. "Scareware is something that plants into your system and immediately informs you that you have hundreds of infections which you don't have. The idea here is to trick you into purchasing a bogus anti-malware where it claims to remove those threats [12]. "Keylogger is something that keeps a record of every keystroke you made on your keyboard, stealing login credentials [12]. These are just a handful of threats listed.

III. INFORMATION SYSTEMS PROTECTION

It seems like organization's information systems are either probed or under attack on a constant basis. Unfortunately there are many computer systems with theoretical and actual weaknesses that need attention and the proper remedy to be administered. The three most aspects of computer security are Confidentiality, Integrity and Availability, and these three addresses security in computing. With the involving changes of the computer industry and advancing changes of the Internet means only one thing and that is a need for new and improve security measures implemented and policies amended to reflect the latest changes. There are a couple of ways a company can use security measures to "help prevent and respond to insider's intentional or inadvertent disclosure or confidential company information [13]. Let's take a look at five privacy and data security measures that can protect your company against unauthorized access and possible theft. 1. "*Internal Privacy and Data Security Principles*: By specifying how the company collects, uses, discloses, and protects personal data of its customers and employees, internal privacy and data security policies can help companies identify who needs access to confidential data, how this data should be secured, and procedures for effectively deleting or destroying data once it is no longer needed by the company [13]

2. "*Internet Access and Use Policies*: Many companies implemented employee policies in the 90s governing how employees may access and use the Internet and the company's computer networks. However, these policies should be updated as new technologies that may increase the disclosure of confidential company information, such as peer-to-peer programs and third-party mobile applications, emerge [13].

3. "*Social Media Policies*: Social media policies typically govern how employees may use social media for work purposes, and, in some cases, set forth guidelines for employee use of personal social media accounts as well. While these policies help to remind employees that they should be cautious when using social media to avoid the disclosure of confidential or proprietary company information, employers need to ensure that these policies are consistent with federal labor laws and state laws restricting an employer's ability to request access to an employee's personal online accounts [13].

4. "*Robust Protections in Service Provider Agreements*: Confidentiality clauses and nondisclosure agreements with service providers are common and important. But robust privacy and data security provisions can provide additional protection and mitigate the risk of a breach, especially where the service provider will handle your customer's personal information [13].

5. "*Bring Your Own Device ("BYOD") Policies*: Employers increasingly are allowing employees to use their personal smartphones, tablets, and other devices to access work e-mail accounts and the employer's computer network. While both employers and employees can benefit from this approach, companies need to make sure that their bring-your-own-device policies provide employees adequate notice and allow employers to implement appropriate data security measures, such as remote wiping tools [13].

IV. INDIVIDUAL PERSONALITIES

Do organizations do enough when it comes to background checks on newly hired individuals? Is there enough being done to ensure individuals who have chosen the IT field have the right personality traits like teamwork, drive, dedication, assertiveness and optimism just to name a few? "A successful team of IT professionals represents a necessary piece of building a successful enterprise. Selecting the right candidates for IT positions includes identifying those who possess the personality traits that provide IT professionals with a solid framework for success within the field [14]. IT professionals must have the right chemistry to work with one another in order to accomplish the task at hand. "IT professionals should possess a desire for continual learning and achievement within the field of IT. Other personality traits you should look for in an IT professional include dependability and the ability to adapt to a changing work environment, such as the need to come in on weekends to address critical systems issues [14]. Having the necessary characteristics to deal with customers on a daily basis justifies the need for IT personnel to be thoroughly checked out. Customer service is a big part of the IT field, you are going to speak and deal with people who come from all over the world with various backgrounds who may have an above normal social status.

V. TRAINING AND EDUCATION

When someone is trying to establish themselves in the IT field they must consider the copious amount of hours and training that is involved in order to certify in one of many certifications that is offered in the IT professional field. "Training today's cyber professionals requires the use of a broad range of venues to prepare these personnel to operate in a technically challenging environment [15]. The technical environment is constantly changing requiring schools to continuously update their training material and enhance learning objectives. Security awareness is a very important issue and topic. There are several employees who are not receiving the proper training in this subject and when adequate training is not receive then human error mistakes will start to take place. "Security awareness training is a formal process for educating employees about corporate policies and procedures for working with IT. A good security awareness program should educate employees about corporate policies and procedures for working with IT. Employees should receive information about who to contact if they discover a security threat and be taught that data as a valuable corporate asset. Regular training is particularly necessary in organizations with high turnover rates and those that rely heavily on contract or temporary staff (Rouse, 2015)." Responsibilities for making sure employees are trained rest on the shoulders of the CSO (Chief Security Officer) who is pretty much responsible for the company's information systems. "A CSO is the highest-level executive directly responsible for an organization's entire security function. Increasingly, CSOs are not only responsible for their organizations' physical security needs but also their digital or electronic security requirements, including computer networks. Originally a title used to designate the person most responsible for IT security, the new CSO executive looks at all threats and institutes appropriate security programs (Guerra, 2015)." So as CSO training is on point and that all staff, employees, and contractors should receive the proper training that they are required to receive.

VI. CONCLUSION

We described some important issues regarding insider threats to information security, protection of information systems and computer security systems, individual personalities, education and training. Information security systems will forever need human interaction and the employees and staff members who manage these systems sometimes unknowing and unwillingly play a crucial role in causing major accidents to information systems because of human error or malicious intent. One thing for sure is that personality characteristics, individual differences, mental abilities and behaviors are a very important part in having the necessary skills in becoming an IT professional.

RERFERENCES

[1] Groenfeldt, T. (2014). *Insiders Pose a Serious Threat To Corporate Information.* Retrieved from http://www.forbes.com/sites/tomgroenfeldt/2014/05/08/insiders-pose-a-serious-threat-to-corporate-information/

[2] Info security. (2012). *The Good, the Bad, and the Ugly Insider Threats*. Retrieved from https://www.infosecurity-magazine.com/magazine-features/the-good-the-bad-and-the-ugly-insider-threats/

[3] McCaney, K. (2015). *The accidental hackers: Insiders pose the top threat to DOD networks.* Retrieved from http://defensesystems.com/articles/2015/01/29/dod-insider-threats-it-security-survey.aspx

[4] Strohm, C., & Robertson, J. (2014). *Companies' Worst Hacking Threat May Be Their Own Workers*. Retrieved from http://www.bloomberg.com/news/articles/2014-09-26/companies-worst-hacking-threat-may-be-their-own-workers

[5] Darkreading. (2015). *Ed Survey Results: Insider Threats*. Retrieved from http://www.darkreading.com/vulnerabilities---threats/ed-survey-results-insider-threats/d/d-id/1318850

[6] Khimji, I. (2015). *The Malicious Insider.* Retrieved from http://www.tripwire.com/state-of-security/security-awareness/the-malicious-insider/

[7] Mundie, D. (2014). *Unintentional Insider Threat and Social Engineering.* Retrieved from http://blog.sei.cmu.edu/post.cfm/unintentional-insider-threat-social-engineering-090

[8] Cert Team. (2013). *Unintentional Insider Threats: A Foundation Study*. Retrieved from http://www.sei.cmu.edu/reports/13tn022.pdf

[9] Karabat, B. Ç., & Karabat, C. (2012). Increasing Awareness of Insider Information Security Threats in Human Resource Department. *International Journal of Business and Management Studies, Yıl*, *4*.

[10] Berr, J. (2015). *Computer security's weak link: Humans*. Retrieved from http://www.cbsnews.com/news/the-human-element-and-computer-security/

[11] Infosecurity. (2013). *Human error and system glitches drive nearly two-thirds of data breaches*. Retrieved from http://www.infosecurity-magazine.com/news/human-error-and-system-glitches-drive-nearly-two/

[12] Martino. (2013). *28 Types of Computer Security Threats and Risks*. Retrieved from http://forums.iobit.com/forum/iobit-security-software/iobit-security-softwares-general-discussions/other-security-discussions/15251-28-types-of-computer-security-threats-and-risks

[13] Tonsager, L. (2013). *5 Privacy and Data Security Measures That Can Protect Your Company Against Trade Secret Theft*. Retrieved from http://www.insideprivacy.com/data-security/5-privacy-and-data-security-measures-that-can-protect-your-company-against-trade-secret-theft/

[14] Long, N. (2015). *Personalities that do well in the IT industry*. Retrieved from http://smallbusiness.chron.com/personalities-well-industry-10591.html

[15] Welsh, W. (2014). *Cyber warriors: The next generation*. Retrieved from http://defensesystems.com/articles/2014/01/23/next-generation-cyber-warriors.aspx

[16] Rouse, M. (2015). *Security awareness training*. Retrieved from http://searchconsumerization.techtarget.com/definition/security-awareness-training

[17] Guerra, T. (20145). *Roles & Responsibilities of a Chief Security Officer*. Retrieved from http://webcache.googleusercontent.com/search?q=cache:BSdr0uSSMkgJ:work.chron.com/roles-responsibilities-chief-security-officer-19479.html+&cd=4&hl=en&ct=clnk&gl=us