ETHICAL ISSUES, ATTACKS, AND SOLUTIONS IN INFORMATION SECURITY

Kristen Jones and Young B. Choi
Department of Business, Leadership, and Information Systems
College of Arts & Sciences
Regent University
1000 Regent University Drive
Virginia Beach, VA 23464
USA
e-mail: krisjon@mail.regent.edu, ychoi@regent.edu
Tel: (757) 352-4949

Abstract

Ethical behaviors and attacks that lie with the information security environment can be difficult for an organization to detect, assess, and recover from. In this paper, we will discuss the importance of policy in order to maintain information security and to deter unethical incidents and other forms of attacks, as well as stating proper procedures employees must endure in the event of an incident. In addition, several types of systems attacks and purpose of attacks will be further discussed in detail.

In every person's life, one must make a decision to choose from right or wrong and usually more than once a day. Whether it is in their personal or professional life, sometimes right and wrong can be hard to distinguish from one another. In information technology, and more specifically information security, withholding an ethical character in a career is essential, as well as providing a strong security system and policy to support possible incidents from unethical behavior or attacks that arise from unawareness.There are several ethical issues and types of attacks that are common and extremely prevalent in information security. Many problems are internal, such as a decision the company must make or an employee that is unreliable or unfaithful. However, there are also many external security demoralizations that derive from attacks and things of that nature. With each ethical issue and form of attack, there is sure to be a solution that can be customized to fit company policies and standards. When companies and their employees maintain a strong ethical character and provide extraordinary security procedures, the business becomes much more trustworthy to clients and overall more secure.

In order to promote the ethical character in each employee, a company must provide policies and guidelines that are to be distributed after each altercation and enforced. "A policy is typically a document that outlines specific requirements or rules that must be met… [And] a guideline is typically a collection of system specific or procedural specific 'suggestions' for best practice," (SANS). In a company's policy, they should cover expected behaviors when using company property and assets, as well as when information is and can be accessed. For example, it is considered ethical accessing information on a need to know basis during work hours. However, if the information leaves the building or is distributed without permission, especially after hours, it becomes a serious ethical issue. Policies should establish other behavioral and company standards and guidelines that should be complied with throughout any circumstance that occurs to the organization.

In any given situation in life, laws and ethics are present. While law is generally enforced by authorities, ethics is ruled by one's moral views. Ethics is a rule of behavior that is based on ideas about what is morally good and bad in a particular circumstance. Unfortunately, unlike a law, ethics can be flexible depending on a person's background, age, or religion. Where one person may find an action to be good and just, another may find the exact

action to be offensive and wrong. Thus, it can be hard to set guidelines on what should be considered right and wrong. However, in a professional environment dealing with information security, ethics should typically come from common sense that may derive from the company's policy. Once again, unfortunately problems will still arise; some may be small issues, others may be costly to the company or the employee's career.

There are three main causes or purposes to unethical or illegal behaviors in the work environment including ignorance, accident, and intent. Ignorance generally originates from lack of education or awareness whether it is about the newest security risk or how to use a specific technological device. However often it also occurs when one does not desire to put in their efforts to learn or complete their tasks completely and thoroughly. Ignorance of an employee can be reduced if the organization provides training and awareness programs, unless it is caused by apathy, then the organization should reconsider their employment. Accidents, on the other hand, are bound to happen to a company no matter how experienced an employee is or the precautions they take. "Careful planning and control helps prevent accidental modification to systems and data," (Whitman, Mattord, 2012). Lastly, intention of unethical behavior is not something that can be prevented, except for through intensive interview processes, as intent of attack occurs by "the state of mind of the person performing the act; it is often necessary to establish criminal intent to successfully prosecute offenders," (Whitman, Mattord, 2012). The only way to protect the company from this type of behavior is to secure systems and networks with access controls, Incident Detection and Prevention Systems (IDPS), and well prepared contingency plans. These three types of behaviors will be prevalent throughout many ethical problems in information security discussed in further detail.

"Frequently, naïve users can unintentionally cause a world of problems for an organization. They may not be aware of policies that are in place, and even though their activities may be legal, they do not understand how it can hurt company resources, as well as productivity," (Durgin, 2007). Often incidents deriving from ignorance can form because of a lack of awareness or potentially not educated in a particular field. For example, using a computer or other device that is secured, specifically a work device of some form, on a public network can be threatening to the information that is stored on that particular device and vice versa. Another person using that public network in a public location can gain access to the IP address, location, or other forms of data and manipulate the system to enter it. "Cyber-attacks aren't just becoming more frequent, they are also occurring on an expanding array of 'surfaces'. As well as what might be termed 'regular' website hacks, cyber-attacks are now targeting social media services and sites, cloud-based computing systems, and mobile networks and devices, (Williamson, 2013). In addition, those who use social media sites or email services for personal or professional use might fall for a social engineering attack. Social engineering is "the use of social skills to convince people to reveal access credentials or other valuable information," (Whitman, Mattord, 2010). For example, an external source may send an email to an employee with a targeted organization claiming to be someone else that works within the corporation saying that they have lost information and needs this particular information to be returned to them so that they can store it in their files. If this employee is gullible or ignorant, they will most likely gladly send the information without confirming the identity of the recipient.

The first obvious solution to this form of attack is to personally confirm that the sender of a suspicious email is authentic. If the receiver of the message at least searched in the company directory to determine if it was true, that would be a better, more secure approach than automatically accepting the email. However, it is always best to check in person with the sender in the event of receiving emails that deal with the transmission of confidential information. The next plausible and more important step for the organization as a whole to take is to implement security education, training, and awareness programs for its employees to stay in the loop on threats and vulnerabilities that are current within the firm. Awareness of types of attacks will allow this particular employee to identify that the email is a fraud, rather than giving in without any background research. "The purpose of computer security awareness, training, and education is to enhance security by: improving awareness of the need to protect system resources; developing skills and knowledge so computer users can perform their jobs more securely; and building in-depth knowledge, as needed, to design, implements, or operate security programs for organizations and systems," (NIST, 2007). The following graph, courtesy of *nist.gov* (2007), displays the purpose, importance, and methods of each element of SETA.

	AWARENESS	**TRAINING**	**EDUCATION**
Attribute:	"What"	"How"	"Why"
Level:	Information	Knowledge	Insight
Objective:	Recognition	Skill	Understanding
Teaching Method:	Media - Video - Newsletters - Posters, etc.	Practical Instruction - Lecture - Case study workshop - Hands-on practice	Theoretical Instruction - Discussion seminar - Background reading
Test Measure:	True/False Multiple Choice (identify learning)	Problem Solving (apply learning)	Essay (interpret learning)
Impact Timeframe:	Short-term	Intermediate	Long-term

Awareness answers the question of what by informing employees what attacks and information is and how it relates to their business. Training answers how each user can attribute to bringing information security to their organization by physical displaying the way each task is done and assigning specific roles to employees. Lastly, education answers why by explaining the true need of information security, how it works, types of attacks and the proper solutions and strategies that should follow. Together, if each employee has at least one of the three elements, the security of information and the overall company will greatly enhance. Therefore, to avoid ignorant incidents, an organization should require that SETA programs must be present and enforced upon each individual.

Accidental incidents do not occur due to the lack of knowledge or awareness of security improvement methods as incidents caused by ignorance do. Instead, they arise from pure accidents that do not normally originate from unethical behaviors and are often unavoidable for organizations. "The survey of 400 chief experience officers (CXOs) in the UK, France, Germany and the USE found that the insider security threats that caused the largest number of instances, such as unintentional data loss through employee negligence, and the greatest financial impact of for example out-of-date or excessive privileges and access control rights for users, were accidental," (InfoSecurity, 2009). Employees must be conscience of their actions on company networks and systems. For example, using the previous instance, the employee that received a social engineering attack email, specifically a phishing attack, may accidentally click the link provided while trying to delete an email. A phishing attack is "a specialize social engineering attack in which the attacker uses an e-mail or forged Web site to attempt to extract personal information from a user," (Whitman, Mattord, 2010). It is not often likely of accidental clicks, especially when users are careful of their surroundings and actions; however, accidents happen every day. Therefore, a user can never be mindful of activities that go on around them. Otherwise, the simple incident could cost the company their information, integrity, trustworthiness, money, and most importantly to the employee, their job.

The best solution for identifying and mending accidental incidents in an organization is to implement Intrusion Detection and Prevention Systems (IDPS). They are able to identify possible attacks that could have gained access to the system do to an employee accident. IDPS are generally used to recognize attacks and policy misuses, deter employees or even external sources from violating set company policies, and document each current threat and vulnerability to a system or network. "In addition to monitoring and analyzing events to identify

undesirable activity, all types of IDPS technologies typically perform the following functions: recording information related to observed events, notifying security administrators of important observed events, [and] producing reports. Some IDPSs are also able to change their security profile when a new threat is detected." (NIST). Another great practice a company can take to avoid common mistakes that happen from one employee always being assigned to working on the same project is to implement separation of duties, as well as job and task rotation. "Separation of duties is a classic security method to manage conflict of interest, the appearance of conflict of interest, and fraud. It restricts the amount of power held by any one individual. It puts a barrier in place to prevent fraud that may be perpetrated by one individual," (Gregg, Nam, Northcutt, Pokladnik). Separation of duties will bring thoroughness, authentication, and truthfulness to each task being completed namely because there are at least two people assigned to a project where they can double check each other's work. Job rotation is required by organizations that employees know how to perform at least two areas of work in the company, while task rotation is centered on one task but is performed by several individuals. All of these elements of assigning jobs, duties, and tasks are critical for corporations so that the security of their information is stronger and more thorough. The saying two is better than one definitely applies when confidentiality is an important element to their work.

In information security, there will come a time in which either an internal or external source will intentionally attempt and/or succeed in compromising a company. This generally occurs when a person seeks revenge, information, or some form of asset. Attacks of this nature, if successful, are almost always crippling for an organization. Common forms of intentional attacks include brute force, denial-of-service, back door, malicious code, man-in-the middle, and spoofing. The list is extensive and new attacks are formed daily, making the present list of attacks never ending. Since there are numerous amounts of attacks available and the intentions of many people are unfortunately demeaning, it can be impossible for an organization to avoid such infections to networks, servers, and computer systems.

Internal attacks originate from within a company and aregenerally geared against the exact company the employee or one that has authorized access to it works for. "Research conducted by the US Computer Emergency Response Team (CERT) estimates that almost 40 percent of IT security breaches are perpetrated by people inside the company," (Whittle, 2008). There are several forms of workers in most organizations that can be granted access to the network which should be carefully monitored, including temporary workers, contractors, consultants, business partners, as well as full-time workers. This could be hard to keep up with and monitor as there is a lot of activity occurring on several parts of a signal network. Just as incidents such as social engineering and phishing as likely to occur by ignorance or accidents by employees, it can also be an intentional attack that comes from within a company. The employee may be upset with the organization for various reasons and decide to purposely click and open one of the links that were sent in an e-mail to hack the system and access very important information about the company and its employees and customers. Another reason an internal source may unethically produce an incident to an organization is because they were hired by an external company to gain trust and entry to a competitive firm so that they can compromise their business. Ethically this is not sound for several reasons including personally, socially, and professionally. No matter what the circumstances are for going through with an internal attack, ethics will never be a point in the cause. Thus, procedures and other solutions must be implemented, just the same as they are needed for external attacks.

External attacks are unethical threats against companies that occur most from people from outside sources that wish to retrieve confidential information or ruin the organization of its advantage, sustainability, and trustworthiness. Viruses, malicious code, and denial-of-service attacks are most common in a business environment. Viruses are a type of program that has been designed with the intention of infecting a system so that the way a computer operates is manipulated. The several types of viruses can do anything from altering and replacing stored information to attaching itself to certain documents and avoiding antivirus software detection systems. The most commonly referred external attack, however, would be the denial-of service attack. "A Denial of Service (DoS) attack can come in a variety of forms, but the main intent is to prevent users from having access to your application. One method is to flood your server with a large amount of requests, tying up your server's resources and preventing legitimate requests from being fulfilled," (Barnes, 2013). A Web site or server will begin to fail when a DoS attack occurs because of the mass amounts of activity it brings to the server. Generally the server will crash because it cannot handle this flood. While these are a few typical external attacks, there are thousands of forms of attacks that range from slight manipulation and damage to catastrophic damage that will absolutely cripple an organization.

Solutions to both internal and external attacks are one and the same even though there are two separate entrances of attack that involve multitude amounts of attacks. Ultimately the ethical issues will result back to a company's policies. Whether it is an intentional internal, ignorant, or accidental attack or a pure intentional external attack, policies and procedures must be implemented, followed, and ensured. By doing so, employees that caused for incidents to occur can be handled and/or prosecuted as needed and accordingly. Otherwise, for general threats and attacks, procedures for recovery plans can began to restore the information and systems that were affected.

> "Many security professionals understand the technology aspect of protection but underestimate the value of policy. However, laws and policies and their associated penalties only deter if three conditions are present: fear of penalty- potential offenders must fear the penalty, probability of being caught- potential offenders must believe there is a strong possibility of being caught, and probability of penalty being administered," (Whitman, Mattord, 2012).

Among the several intrusion, detection, and recovery systems available to track and capture attacks and viruses, such as firewalls, IDPS, and even physical security, it all comes down to following policies and these three simple deterrence examples that will begin to eliminate ignorant, accidental, and intentional attacks of all kinds. Fear can essentially be a person's biggest deterrence, if their conscience is in the right mind. Therefore, all incidents that arise from unethical behavior, specifically within a company's borders, will begin to decrease for fear of consequences and being caught in action. For others, on the other hand, who do not care about anything other than hurting the company, programs for detecting, blocking, and removing attacks must be put into practice, as well as thoroughly planned contingency plans and policies and procedures for employees to follow in the event of such incident. Above all else, policies are extremely essential for companies to create, enforce, and comply with because it will save them much hassle, time, money, and loss of data in the long run of the business.

Ethical issues, as well as general attacks, in a company can be difficult for an organization to deal and recover from. However, even in everyday life, incidents are bound to happen and must be assessed, removed, and recovered. With this in mind, ethical behavior and proper policies are to be present and intact within each company. This will aid in avoidance of potential incidents that may originate from ignorance, accidents, or merely pure intentions from internal or external sources. In conclusion, sustaining these elements will ultimately enhance information security because of the reduction and elimination of common unethical behaviors and attacks that occur within an organization.

Works Cited

Barnes, D. (2013). *Node Security*. Birmingham, UK: Packt Publishing

Durgin, M. (2007). Understanding the Importance of and Implementing Internal Security Measures. Retrieved from https://www.sans.org/reading- room/whitepapers/policyissues/understanding-importance-implementing-internal-security- measures-1901

Gregg, J., Nam, M., Northcutt, S., &Pokladnik, M. (n.d.).Separation of Duties in Information Technology. Retrieved from http://www.sans.edu/research/security-laboratory/article/it- separation-duties

InfoSecurity.Accidental Insider Security Incidents More Frequent Than Malicious Attacks. (2009). Retrieved from http://www.infosecurity-magazine.com/view/3573/accidental-insider- security-incidents-more-frequent-than-malicious-attacks

NIST.(2007). AWARENESS, TRAINING, AND EDUCATION. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter13.html

SANS.(n.d.).Information Security Policy Templates. Retrieved fromhttp://www.sans.org/security-resources/policies/

Whitman, M., &Mattord, H. (2010). *Management of Information Security* (3rd ed.). Boston, MA: Course Technology.

Whitman, M., &Mattord, H. (2012). *Principles of Information Security* (4th ed.). Boston, MA: Course Technology.

Whittle, S. (2008). The Top Five Internal Security Threats. Retrieved from http://www.zdnet.com/the-top-five-internal-security-threats-3039363097/

Williamson, J. (2013). Managing Data: How to Combat Cyber Threats. *TM Forum*.