Global Information Assurance Certification Paper

The Importance of Acceptable Use Agreements ... the Human Factor

thoughts from a Security newbie

GIAC Security Essentials Certification

Practical Assignment
Version 1.4b
Option 1

Greg Baker
September, 2004

Table of Contents

Abstract

Computer security is seen by many end users as an inconvenience, an impediment to the creative process and their productivity, and an infringement on their privacy. They question why they cannot access certain web sites, question the use of e-mail filtering and monitoring, and question why they are prevented from using devices such as USB drives or memory keys on their computers. Others see security as a necessary evil, somewhat hindering their freedoms but providing for a safe and reliable computing environment.

Whatever the view, the level of control exerted over a network has some effect on the final experience of the end user. While the majority of end users abide by the guidelines established by an Employer, there will, for whatever reason, always be individuals who continually seek a means to circumvent the rules.

The following is not meant to be a technical document, nor, is it a thesis on human behavior. It simply represents the views of the author formulated from observation of real world activities and supplemented through various readings. In the next few pages I will attempt to highlight what I believe to be the premise behind these behaviors. I will discuss options that an Employer can use to reign in errant employees. I will explain why it is important for an Employer to be explicit and fully explain the reasoning behind any restriction. Finally I will discuss the issue and importance of Executive buy-in.

Introduction

A viewpoint noted in an issue of Information Security magazine recently caught my eye. The author noted that "without enforcement of corporate security policy, any expected ROI in endpoint security components (AV, personal firewalls, anti-spyware, etc.) could be lost in a blink of an eye with only one non-compliant endpoint"[1][1]. I immediately reflected on the situation with my Employer. Significant investments of time and money in hardware, software, and data compromised just because one end user decided to ignore policy, connect a USB drive they brought from home, and uploaded files containing malicious code to their workstation.

Why would an individual take such a great risk? What is there to gain from violating policy? Did they consider the ramifications of their actions? Two answers came to mind:

- convenience
- lack of enforcement for policy violations.

---

[1] Patterson

For the end user it was more convenient to connect a USB drive and upload the files rather than send the files by e-mail where it would have been quarantined. It could also have given the end user a sense of satisfaction in knowing that they have just bypassed policy without getting caught.

What Policy!?!

In discussing possible scenarios with colleagues a consensus developed as to what end users will do and why they do it. Their behavior and attitude toward the computing environment in the workplace tends to be reflective of their:

- experience with computing (abilities);
- experience with the technical support staff;
- individual personality; and,
- position within the company.

Experience:
Admit it ... we have all done it before ... from the most seasoned IT professional to the individual who for the first time has just powered up a computer ... we are all guilty of blaming at least one computing misfortune on a computer, peripheral, or IT staffer. Closed a document you spent hours preparing and forgetting to save ... blame the computer; sent an e-mail with questionable content to a printer in another department ... blame the printer; infecting the corporate network with a Worm/Virus from media brought from home ... you got it ... blame IT for not providing full and unfettered access to the Internet.

Why do we do this? Why is it difficult to accept the consequences of our own actions (or inactions)? Why do we continually look to shift the blame elsewhere? We conveniently forget that the computer we use on a daily basis is only an amalgam of circuits, wires, and "magical" code used to accept input, process input, and provide a result. It is essentially a dumb machine until we provide it with instructions.

End Users also forget that the IT staffer is not enjoying an ego trip because they control your access to corporate computing resources. Tech Staff are no more than employees charged with the responsibility of ensuring the technology used by a company is suitable and effective, that employees are provided with an appropriate level of access to resources and data, and that the systems in place provide for the security and safety of data and personnel. They, like an Accountant or Civil Engineer, are only doing their assigned job.

Ultimately, whatever their opinion, responsibility for one's actions falls to the end user. We must realize that our experience with security and corporate operating policy is solely

dependant on our ability to extract from our computing experience what we put in to it.

If an individual's experience with corporate security and operating policy is negative the greater the probability that individual will attempt to circumvent the rules. If that individual were to succeed once, the curiosity will probably tempt them again.

Personality:

Humans are an peculiar lot. When exposed to chaos we expect and accept regulation. When we feel over-regulated we attempt to circumvent the very regulation we previously accepted. An attempt to circumvent established rules carries with it the risks associated with detection. Detection carries with it the risk of reprisal. The amount of risk that we are willing to accept is dependant on our personality.

There is an inverse relationship observed between the risk associated with evading a regulation and the number who those who attempt to evade it. If the risk of detection is low more individuals will attempt evasion (think of how many times you have used a cell phone while driving). Conversely, fewer individuals will attempt to circumvent regulation if the risk of detection or penalty is high (would you send an uncomplimentary e-mail to your boss from your own account?).

An amalgamation of many factors result in an individual's decision whether or not to skirt regulation, including but not limited to, personality type, the level of anonymity, the degree of penalty, and the perceived reward. Some end users accept the conditions of their employment and for the most follow an Employer's policy. Others may try to side step issues that they view as nominal and are very cautious of their actions.

Some individuals, regardless of the risk involved or penalties associated with an action, view their own convenience as priority. They both fail to see and are not threatened by the consequences of their actions. These are the types of end users that can down a network, significantly damage a company's reputation, or cost a company financially.

Position:

An individual's position within a company may also be a factor in an end user's outlook of security and policy. If a policy existed banning the use any modem not installed by the IT department, should a Vice President be able to evade the policy because she would like to trade stocks while in the office? Should a Receptionist be able to the same? As an IT Staffer, who would you be more inclined to report? Would there be any differences in the manner used to report the infraction?

The influence held by an individual over another is a significant factor in the decision to report an individual for breaking with policy. Many subordinates would hesitate to report a

policy infraction made by their supervisor. They would assume that a light penalty would have repercussions for them. In fact, some may view this breach as an opportunity to do the same.

An individual's position may also have a negative influence on Tech Support staff. Would a member of the IT staff report and follow up on an individual known to be breaking with policy if that individual could affect their within the organization? Some view these types of actions as career limiting moves. Others may provide a verbal reminder of the offending action and inform the end user of the accepted policy (sort of an informal warning). Some will report the individual's actions citing the policy without fear of reprisal.

In a perfect world fear of negative retribution should not be a factor in reporting policy violations. The individual who decides to bring forth valid claims of policy violations should be afforded the support of the organization.

Acceptable Use Agreements:

Many companies invest significant time and resources into developing formal business plans and mission statements that guide the direction and operation of the company. Likewise, many organizations spend significant energy and resources in developing policies, procedures, and guidelines for a variety of topics from sexual harassment to the use of the company car. In recent years, and with the proliferation of Internet/e-mail accessibility, documentation related to computer resource usage have been developed.

Primary to the development of any policy is the determination of responsibility ... who is responsible for what. With this determination made and in conjunction with the organization's business model, work on the formal documentation can commence.

Different companies have different visions of what can be considered as suitable documents related to policy, procedure, and guidelines. Although there may be overlap, the one consistency throughout all forms of documentation is the slow removal of subjectivity as one passes from a policy statement to a guideline. As an example, a policy statement may include the following:

> *Employees of Company X will use the resources allocated to them in an ethical manner.*

Although the preceding appear to be acceptable comments for a policy ... the Employer stating that the resources it provides and is liable for must be used in an ethical manner ... something is missing. What would happen if an Employer's vision of ethics differs from that of the employee? Enter the Acceptable Use Agreement.

An Acceptable Use Agreement can simply be defined as an addendum to both an employment contract and usage policy. It is essentially a contract signed between the two parties which explicitly defines the rights and responsibilities afforded to each stakeholder.

Rather than focusing on generalities an Acceptable Use Agreement defines specifics. It personalizes the usage policy for all parties involved. Instead of a vague statement related to ethical use, an Acceptable Use Agreement outlines the position of the organization and explicitly identifies what the organization holds to be ethical behavior. It might contain a statement as follows:

> *Employees provided with access to the Internet are prohibited from using the resources of Company X for personal profit, for activities that could prove liable to the company, or for activities that contravene local or national laws. These include, but are not limited to:*
>
> *- creation, maintenance, or operation of a personal website/FTP site/mail server.*
> *- visitation, participation, or support of websites depicting nudity, pornography, or sexually explicit images.*
> *- visitation, participation, or support of websites containing materials that are deemed to be hateful or detrimental of a person's race, sex, sexual orientation, or religious beliefs.*
> *- visitation, participation, or support of websites containing materials that depict or promote abuse of animals.*
>
> *Violation of any of the above statements would be considered as grounds for disciplinary action up to an including dismissal.*

The preceding explicitly identifies the Employer's expectations related to their on-line conduct. However, without the employee acknowledging the document through a signature the document is nothing more than an elaborate policy statement. By appending a signature the employee has accepted the responsibility that the document has been read, that suitable answers to any question has been provided, and that the consequences associated with violation of any portion of the company's statement has been acknowledged.

There will always be a number of end users who will remain suspicious of any Employer that requires them to sign a document outlining their rules of behavior. They see it as another means of control that can be used against them with even the slightest infraction. In certain instances this might be true; however, with the ever growing fear of legal action, many companies require these agreements for the protection of the company and its employees.

The manner in which an Acceptable Use Agreement has been phrased can assist in the degree to which it is accepted by a Company's staff. The use of negative phrasing immediately places an end user into a defensive mode. The use of the words "must", "will", and "don't" projects the image of a being dominated by the Employer. It seems to bypass the fact the employee is an adult. Employers are reluctant to reduce the use of negative phrasing as it is viewed as a weakening of their power over the affairs related to the governing of the business.

Individuals tend to respond to more moderate phrasing - "may", "shall", and "should". When combined with the reasoning for the statement, the more moderate phrasing possess greater influence over adherence to a policy.

The following provides an example of the differences between two negative and moderate phrasing:

Example 1) *When creating a password employees must not use english-based words (eg. flower, toyota, barbeque). Passwords must be a minimum of 8 characters in length and contain at least 1 number. All passwords will expire on the 60th day from their creation.*

Example 2) *Given the proliferation and sophistication of software used to crack passwords, employees are requested to create passwords that are more cryptic than plain english-based words. Passwords should be at least 8 characters long, and contain at least 1 number. This increases the ability of the password to remain private. As an added security feature all passwords are set to expire after 60 days. Although these measures may appear to some to be excessive they have been implemented to protect your access to the Company X's computing resources.*

While Example 1 is short and directive it does not provide any explanation why these restrictions are in place. An end user might think that the password restriction is the brain child of some executive trying to impress their boss. It is a statement that most will probably not follow or will easily forget.

Example 2 is more explanatory and contains the reasoning behind the restrictions on password creation. The end user is provided with knowledge that is of benefit to them outside of the workplace. They are shown that the Company has implemented preventative measures in order to protect its assets and employees. They are shown that the restrictions are not based on the whim of an executive. More thought and additional care will probably be given when creating a password.

Executive Acceptance and Managerial Support.

Throughout this paper I have used the words Employer and Employee. This separation was intentional. Some will view the Employer as the entity which created and then imposed regulation; the employee was probably viewed as the entity which must accept the will of the Employer. This type of relationship could only breed hostility and resentment.

It also allows us to identify a important factor in the acceptance of controls in the work place. Any Acceptable Use Agreement, Policy, procedure, or guideline MUST apply to ALL those employed by a company ... from the upper most echelons of the executive to the entry level positions. If it is a company policy to only grant Internet access to the IT staff and Development Engineers, a Clerk would probably be more accepting of the a lack of Internet access if that meant the Company's Executive were also without access.

Would that Clerk, or any other employee, continue to follow any Acceptable Use Agreement if it was known that an Executive member of the company subverted the process to gain access to a resource which Company policy stated they were not to have. Probably not. Further, if that member of the Executive is not subject to any disciplinary action established by the Employer for violations of the policy, the intent of the Acceptable Use Agreement is rendered null. Compliance with any rule established by an Employer has to be applied equally across the organization. An Employer should not be able to favour one group over another, especially when there is written policy.

As with any rule there will always be exceptions. Care should be taken to clearly identify the reason for any exception. Any change to the scope of an Acceptable use Agreement should be advertised and distributed throughout the organization (posted on bulletin boards, Intranet, corporate wide e-mail, etc.).

Organization's should also consider the establishment of a committee comprised of members from all ranks. If this is not feasible, then suggestions from all ranks of employees should be solicited and worked into any guideline. Allowing employees to share in the development of operating rules will provide a sense of worth and ownership (much like profit sharing or stock options). End users would tend not to violate rules that they helped developed.

Conclusion:

When discussing security issues technology-based solutions dominate. We tend to overlook how the end user will interact with the solutions implemented. We tend to forget that the end users are the ones that create the passwords that are key to a company's resources. We tend to forget that what may seem simple and ordinary to someone in a technology field may be beyond the scope of others.

Given the differences in abilities, personality types, and office politics it is difficult to implement solutions that will provide the same experience for all users involved. The best that an organization can do is implement policy, procedures and guidelines that assist the end user in helping the organization reach it's business goals with minimal disruption.

Embracing Acceptable Use Agreements allows for the recognition that the regulations and guidelines established has been accepted by all parties involved. Acceptance of an organization's operating guidelines is paramount to the success of any security plan to be implemented.

Sources and References:

Cantafio, Brent. “Security vs. Convenience, is RSA SecureID the Answer?” GIAC Security Essentials Certification, Practical Assignment, Version 1.4B (April 2, 2004)

Flynn, Nancy. “The ePolicy Handbook, Designing and Implementing Effective E-Mail, Internet, and Software Policies”.AMA Publications (2001)

SANS. “Mistakes People Make that Lead to Security Breaches”. (October 23, 2001) URL: http://www.sans.org/resources/mistakes.php

Information Technology and Telecommunication Services, Southern Cross University. “Information Security Management Program, Security Breaches and Incident Reporting”. (July 15, 2004). URL: http://www.scu.edu.au/admin/it/security/breaches.html

Patterson, Scott. “Your Number is Up”. Viewpoint, Information Security, p20 (July, 2004)

University of Toronto, Computing Center. “Computing Services, Policies and Guidelines”. (July 4, 2000). URL: http://www.utsc.utoronto.ca/~ccweb/staff/pg_security.html

Walsh, Lawrence M. "Pink slips motivate policy compliance". Security Wire Perspectives. (March 29, 2004). URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci957013,00.html

Wood, Charles C., CISSP. "Developing a policy your company can adhere to". (July 13, 2004)URL: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci992041,00.html

Wood, Charles C., CISSP. "How to build a corporate culture of policy compliance". (June 15, 2004). URL: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci968795,00.html

Last Updated: October 22nd, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive