GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Security Awareness: Trials, Tribulations, and Truths

Lance Lahr

INTRODUCTION

Many security practitioners focus on information security policy, the need for it, and the continual debate of what it should actually entail. On the other hand, many of us intimately involved in the information security realm often overlook making the policies available and the associated education of our users. The security awareness of an organization's users—whether they are employees, consultants, contractors, partners, clients or any additional group of users—is of paramount importance. The time has come to maintain a focus on security awareness training. This includes performing activities outside of the normal security team group, to whom security policies and guidelines are only commonly communicated. Within this practical, the author has laid out the scope of security awareness into the awareness training itself ("Trials"), the issues encountered thereafter ("Tribulations"), and the reality of the struggle we will continue to face with educating our heterogeneous user groups in information security ("Truths").

SECURITY AWARENESS

Awareness is defined by Webster's online dictionary as *Having knowledge or cognizance.*

Knowledge is defined by Webster's online dictionary as *the state or fact of knowing or the familiarity, awareness, or understanding gained through experience or study.*

This knowledge speaks volumes for the improvement of data security and the experience or study surrounding it. What follows is the breakdown of critical components of experience or study that security professionals should invoke on their peers who specialize in other fields.

Key Awareness Topics

The leading awareness topics for our end users should include:

- Passwords;
- Data or Asset Classification;
- Viruses;
- Software and Desktop Policy;
- Data Backups;
- Incident Reporting and Response;
- Inclusion in systems analysis & design;
- Physical Security.

<u>Passwords</u>

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

For most organizations, the number one key to accessing information systems is the password. Consequently, when we choose to use them versus stronger authentication, we must strive for them to be 'secure', changed on a regular basis, and not re-usable for a defined duration of time. What is the 'secure' mentioned above? It is generally a combination of upper case, lower case, number and special character in a random sequence with a minimum of seven-to-eight characters. The concept of social engineering must be taught and sample techniques must be demonstrated to participants of the awareness program.

Many users will resist with 'why must I do this?' and 'why is the password requirement so complex?'. To this end, we must develop the understanding that passwords are easy to guess and there are specific tools like LC3 that can break a password and display it to the cracker to utilize a user's account unauthorized. In running these tools within an organization, we can exhibit a sample of the number of accounts that were broken at a specific point in time (visual impact bears depth). However, we must be careful about displaying the actual user id and password that was broken since it can lead to unwarranted disputes concerning the intent of the exercise.

Data or Asset Classification

Any security standards or best practices we propose to implement should include data or asset classification. Defining an owner and ultimate responsibility for a piece or group of data is crucial to the success of an information security program within any organization. From the data classification, we determine required controls commensurate with the sensitivity of the data as classified by the owner. This portion of the program and ongoing training may take longer than other components to sink in to the audience and may have to be separated from the other training.

Viruses

Viruses are probably the most recognizable aspect of user error from lack of security awareness. Viruses are propagated rapidly from one user action, thus should get considerable focus in any security training, newsletters, and holistic awareness program. The method for the spreading of most viruses is through email system and usage, so the risk of opening email attachments must be conveyed and understood by all user audiences.

Software and Desktop Policy

Software piracy is a continual problem for the manufacturers and the consumers of software products. With this, liability can arise on an organization from the result of illegal copying and distribution of licensed software. The user base must all be using licensed software of some means, even if it falls into the classification of an evaluation license. A specific example of a software risk to a company network is that which can arise from third-party users with vulnerable versions of IIS on their laptops. Hence, third-party users must be made to understand that they must turn off all unnecessary services

© SANS Institute 2000 - 2002, Author retains full rights.

while connecting to the company network. A clear desk and clear screen policy should also be considered and communicated as part of the awareness program. Any such policy should be tightly aligned with Data or Asset Classification Policy.

Data Backups

Data backups are often an overlooked component of data security. Most industry consortium-based standards cover the recovery of critical production system files, but the key files of end users are often omitted from an information security program. Letting users know about the significance of backing up crucial files on their laptop/desktop PC is a significant component of issues such as recovery and incident response. The security team should take a proactive stance for end-user data backups by providing an easy method for users backing up their own data (e.g. a batch file on their Windows desktop).

Incident Reporting

Due care must be taken to break this down to a level understandable to all. Although any awareness program cannot be one size fits all, this area necessitates simplification. All companies should have an incident response program, because at the minimum every one will face threats to confidential data. Incident examples—including a social engineering scheme, unsolicited emails asking for company contacts, and a rapidly of a virus spreading—will serve as the best educator. Convey the critical steps for one of the above-mentioned incident types such as contacts, escalation, and readiness to assist in the investigation and handling of the particular incident should it occur.

Inclusion in systems analysis & design

Security inclusion in the design phase of solution and systems build has a major impact on the measurable success of information security within an organization. This aspect would not be included in many practitioners idea of security awareness training; however, it is crucial due to the related operations impact, which is a matter many of us lose sight of during our daily activities.

Users must understand this factor because of the potential cost impact to the organization. If those involved in designing and building company-enhancing solutions do not factor security into the design process, it will prove costly in the long run as the company must "retrofit" security mechanisms. It produces a situation where the old cliché 'pay me now or pay me later' will reign accurate.

Physical Security

Last in this list, but certainly not least-- the first barrier of defense, physical security. If an organization wants to look at defense in depth, physical security awareness shall be the first line and most important line of defense. We must express not to leave doors propped open, identification mechanisms such as badges must be worn at all times, and not to let others walk behind us into our facilities without the proper access control mechanism being used (i.e. card, key, or biometric).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Audience Component

Once we identify the key information security topics to include in the awareness program, we must align our thoughts with the variety of audience we will encounter with the program. As witnessed, many organizations do not include members other than employees as participants in their program. For large organizations, it is fully recognized that this may be difficult. However, large and small organizations similarly have many third parties who deal with their critical data, including consultants and contractors who are involved in long-term projects. A breakdown of the audience and relative experiences of the author are expressed below.

As Shelly Nuessle suggests in the April 2002 version of PASSWORD the ISSA Magazine, once we know the ideas we want to emphasize, the message needs to be developed and should be based on the respective audience. Common components to the message prior to its needed modification per audience may address the following:

- What to do?
- Where to go?
- WIIFM (What's in it for me?)
- Who is responsible?
- How do I change?[1]

An additional question not included in the above list but nevertheless commonly asked by users would be:

- What does this mean?

The question above is obviously related to WIIFM, but at the same time carries different characteristics and an ambiance of 'how can I learn more' or 'teach me more about this'. Thus, the topic could be a branch of security learning that triggers more interest in the overall awareness program and empowers further knowledge gain.

Employees

The employee audience will serve as the most difficult to extend the message to and for them to implement in their daily functions. Some reasons for the challenge and importance of this group are that they are the widest audience both in numbers and geographically; they handle the majority of the company and confidential data; they are the most imperative and influential audience since they drive business; they talk to customers directly; they have the ability to access the most resources; some are less technical; and they know operations and will recognize irregularities.

[1] Nuessle, p. 5-6

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The aforementioned items are only some of the challenge characteristics from the employee audience. As a direct result of the list, we must employ tactical messaging to them in order to:

- Avoid social engineering or other crude attacks;
- Stress the importance of client and partner data (at the least for liability's sake);
- Achieve a common understanding of approved behavior;
- Understand where they are coming from
    - Our users often perceive our passion for information security as 'the sky is falling on us' paranoia. As a good friend has pointed out on several occasions, they are worried about making the bits flow;
- Get a proactive sense of the organization-specific threats.

Management

As specified in ISO 17799, management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.[2]

In order for management to set the direction, we must enable them through positive security awareness training. The message to management should incorporate:

- Risks and associated impact to business;
- Intrusion war stories;
- Legal issues- company and personal liability
    - Executives need to be sensitive to the fact that emails are discoverable evidence and can be interpreted out of context by outsiders. A good technique to teach management when they are scribing sensitive emails is to ask themselves, "How may this email sound if read on the witness stand?" and act accordingly;
- Permitted and disallowed behaviors on company resources;
- Knowing how to talk about security
    - The executive management of the organization needs to learn that they must be careful to avoid making overstated/exaggerated claims that would pose a challenge to hackers
    - Case in point- Oracle's Larry Ellison boldly claimed that Oracle 9i's security is unbreakable. However, security monitor CERT reported at least thirty-seven vulnerabilities in mid-March 2002.[3]

Management understanding is essential in order to achieve support for the program, the associated budget, and the circumstances that dictate us needing them to talk to employees to get a complete, enforced message across on an ad-hoc basis.

Third Parties

[2] ISO 17799, p. 1
[3] Middleton

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The most neglected users in terms of security awareness training within organizations are third parties. The majority of this group is composed of contractors and consultants. The sporadic in-and-out behavior of some of these users, as well as their cost, makes it difficult to get some of their time. Other members of this audience may be on project for months upon months such as in an outsourced business unit. Regardless of a third party individual's stay, it is best to require all third parties participate in awareness training as soon as they arrive and prior to granting them network access. Also, other members of this group may include business partners who are competitors of an organization as business trends have evolved. Other than these members signing non-disclosure agreements, part of the awareness program could be an evaluation of their security program.

Selected reasons not to neglect training third parties include:

- They may handle focused company financial information;
- They develop key revenue-generating/company-enhancing solutions and programs;
- They often hold proprietary source code;
- They handle key networking data.

ISSUES ENCOUNTERED

After developing key topics and identifying key audience groups, we will be training the various groups with access to company data. While training frequently occurs, human obstacles will stand in the security educator's path at times. They may come in bunches, trends may develop, and certain parties may continually make the same type of mistakes. Figure 1 displays the goal of creating a human firewall and corresponding issues that companies face from people problems on the right side of the diagram. Meanwhile, the author subsequently provides detailed lists of people problems encountered in his specific experience.

© SANS Institute 2000 - 2002, Author retains full rights.

Figure 1: Creating a Human Firewall[4]

Passwords

1. Users giving passwords out rather easily when Social Engineering conducted on them.
2. Company password policies not followed on all systems.
3. Shared user accounts.
4. Posted on laptops with yellow sticky notes.
5. Written down at user's desks.
6. Weak or no passwords on Home PCs and DSL connecting to company networks.

Data or Asset Classification

1. Over-classifying data by utilizing Confidential as a default.
2. Not classifying data at all.
3. Many systems unknowingly brought in, which cannot be tracked by the program.
4. Passing confidential network data in the clear (user ids, passwords, IP addresses, key port numbers).
5. Leaving confidential printed data out in the open in company areas where non-employees have access.
6. Owners not understanding their responsibility and assuming security responsible for classification.
7. Such a wide distribution of company information because of the latest element of partnership, mergers, acquisitions.

[4] humanfirewall.org

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

8. As a consultant, one may hook up to a vulnerable network and have other client data accessed or compromised or can also be the cause of vulnerability via an insecure laptop with unnecessary services running on it (e.g. IIS or Gopher).
9. Voice transmission do not receive attention from users as word-of-mouth is overlooked as a security issue.

Viruses

1. Non-company email accounts often carry them in.
    a. Slip by an email gateway in this case. They use http.
    b. IM chats also use http, which is permitted traffic on TCP port 80.
        i. IM and IRC vulnerabilities being exploited frequently.
2. Curiosity drives too many users.
3. We all are susceptible, even when trying to investigate a virus.
    a. Recent forged message from Cisco Product Security Incident Response Team (psirt) received by author believed to be from a known source, which it was not.
4. They have more noticeable impact to everyone than any other security problems.
5. Users do not frequently run scans and retrieve live updates on their own.

Physical Security

1. Piggybacking is not that difficult.
2. Be aware of the access-control lists (ACLs) to all areas of the company's facility.
3. Theft- cable locks are not that effective.
4. The same fear (in a different manner) that motivates can cause users not to question unfamiliar faces—in this case fear of conflict.
5. Very hard to track variety of people in and out of the company's facility, even with front desk manned, etc.
6. Key areas with third parties not escorted.
7. Power trip-ups occur, failover needs to be stable.

Physical Security Problems 101

In the November 2001 INFOSECURITY Opinion article written by Jon-Louis Heimerl, he summed up physical security weakness in one story. In a single trip to a client, he broke into every key area that should have had barriers. The article can be found at the following URL:

http://www.infosecnews.com/opinion/2001/11/28_03.htm

Or can be summed up by his statement, "In maybe an hour and a half, I had completely compromised their telephone switch room, server room, lab, loading dock, and the office of the vice president of MIS."[5]

[5] Heimerl

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

LESSONS LEARNED AND THE PATH FORWARD

The advancement of security awareness in many organizations will remain a continual, uphill battle. With new issues we face as security professionals popping up as fast as we can blink our eyes, we must remain persistent.

Some of the latest troubling examples have been published in recent articles regarding firewalls and IDS. A summary in Security Wire Digest by Cheryl Balian about a recent CERT study concluded that six major attack trends have emerged. The points Balian summarizes are as follows:

- the automation and speed in which malware races through operating systems;
- the ability of attack tools to cover their tracks and re-configure themselves for deeper intrusions;
- an increasing permeability of firewalls;
- a faster discovery rate of breaches;
- infrastructure assaults that affect communication platforms;
- and attackers' ability to exploit the interdependent nature of the Internet structure.[6]

Additionally, the April 2002 Network Fusion News article on IDS by Ellen Messmer puts IDS signatures as passable. Tests performed by NSS Group found common vulnerabilities in leading commercial IDS systems from a polymorphic buffer overflow. She also specifies that some IDSes, which depend on mirroring traffic, drop packets when traffic flows increase.[7]

Therefore, while recognizing technology tries to catch up to its flaws, we must educate our non-security peers continually when simultaneously deriving strategies for technology usage. We are all susceptible to both the technology and the human errors that can occur. A November 2000 ComputerWorld piece recommends that forty cents of a security dollar should be spent on awareness from security budget and an additional twenty cents should be spent on technology.[8] In this facet, the author has found that transparent works best for technology such as personal firewalls, email attachments, and even email encryption where products can encrypt email without the user even knowing the outbound email is encrypted. Rather than relying on them retrieving updates, pushing anti-virus signatures to end-users can also prove to be a solid practice. With this transparency, we can offload selected scope of the awareness training.

The following sentiments have also ensued from the author's experience in awareness training.

Missed or ignored messages- We use the analogy for users to think of their password as their ATM pin, but it and other comparisons are never absorbed by many of them.

---

[6] Balian
[7] Messmer
[8] McBride

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Whether it is the password makeup/randomness requirements or the fact that they do not have a physical (ATM) card in-hand is debatable.

A belief in the latter of these two can actually be achieved and measured in the form of two-factor authentication smart cards. If an organization cannot deploy token-based authentication, we must continue to push the message to end-users. As previously mentioned, we should be using key techniques in the awareness training where we can exhibit a sample number of vulnerable accounts or sticky notes with passwords on them found at a user's desk. As mentioned earlier, visual impact bears depth on a person being keen to key issues. Why else would physical security issues be the most identifiable and easy to express to management?

Non-compliance via negligence- Our users tend to act in a negligent manner in many security-related aspects of their daily behavior, although it may not be of malicious intention. For instance, they leave confidential documents on printers or lying around at their work areas. If we do not stress to them that they must protect our data, they will neglect to do so. If we do not employ a data classification program, the information will not have proper handling requirements. Some users may even overlook the painfully obvious by leaving a laptop on their desk in an open area overnight rather than taking them home or locking them in a secured area. We must emphasize the value of the data on the laptop, rather than the hardware itself. When encountering the certificate error message on a web site, users will click "Yes" to proceed rather than viewing the contents of a certificate hypothetically about 99% of the time. Some users also send emails with sensitive data such as IP addresses in clear text email over un-trusted networks such as the Internet. The author has found the majority of this occurs from third parties who do not abide by policy, whether the disobedience of policy is due to not attending mandatory security awareness or disregarding the Data Classification Policy. We must enforce all users to participate in awareness training prior to granting them access to our networks.

Laptop theft on the rise- A growing number of distributed user audiences who possess portable PCs exists. Consequently, laptops are a frequent source of theft as is discussed in a recent USA Today article. Safeware reports that 591,000 notebooks were stolen in 2001, which is a 53% rise over the previous year. Also, the annual CSI/FBI survey found an average loss of $89,000 per respondent.[9] We must then relate this physical security issue and compound it to the many other physical security issues we face as noted in the Heimerl discovery referred to earlier to comprehend the risk level.

Lessons over discipline- Awareness will be better accepted by the audience in the face of lessons learned versus enforcement. For example, if a user(s) falls victim to a social engineering attack, explain the attack and not to do it again rather than suspending accounts or berating users. Furthermore, when scanning an internal network with tools like ISS Internet Scanner, leave the message on that User A is probing User B's computer and measure the reaction.

[9] Baig

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Reaching the audience- Establishing fear, as Nuessle also points out, is a temporary motivator,[10] although it carries substantial strength. No matter the duration, fear carries impact and opens up people's ears. For many audience members of the awareness program, the subjects being discussed and overall content is boring, to put it mildly. Some security professionals suggest flavoring the training up with prizes or related rewards, which can be beneficial, but fear is a human instinct that we can twist on and results in the arousal of one's attention. We can make use of a presentation technique such as FUD (Fear, Uncertainty, Doubt) to "scare" the audience to get their undivided attention and focus.

The FBI/CSI survey is often employed to establish the fear. The 2002 Computer Crime and Security Survey results have been published for public use. The continued upswing in incidents establishes that we are all susceptible to security breaches. The 223 respondents who reported $455,848,000 in financial losses show the abundant agony on companies who quantify the losses and these numbers should be stressed to management, employees and third parties alike. The number of respondents (74%) cited their Internet connection as a frequent point of attack.[11] These types of stats remain alarming and companies without verifiably appropriate security controls are open to liability lawsuits, as cyber crime and security have shifted to the courtroom.

Breaking things down to a personal level and providing a 'common ground' such as that which has personal effect on them poses another method of user awareness communication. Home networks and high-speed "always-on" Internet connection security concerns are just a few items to discuss with end users. Additionally, although it should not be recommended, users may use home PCs to access company resources such as web-based email. The security of these environments may eventually impact the organization's security posture.

Helping users understand what they sign serves as a third relationship-developing activity. While recognizing this may seem a trivial task, it establishes a rapport with them in the case where they have signed acceptable use policy, confidentiality agreement, non-competitive agreements or the like. Additionally, experience has proven to the author that making users initial each paragraph of an agreement and provide signature at the end of the agreement causes them to actually read the agreement more often than merely providing signature at the end of a document.

The three techniques mentioned here should be very helpful, because we must remember that we are the ones who may be saying 'no' to them quite often thereafter.

Once we have developed the program there comes time where we must re-evaluate the program. As Neussle discusses in PASSWORD, awareness leaders need to gather information about what worked and items that are subject to improvement.[12] Industry site humanfirewall.org provides an easy-to-use, beneficial tool to assist evaluating security

[10] Nuessle, p. 5.
[11] CSI/FBI, 2002.
[12] Nuessle, p. 7.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

awareness in an organization. Although we may meet resistance at varying points in our path, we must persevere and drive toward enhancement.

CONCLUSIONS

It is well established that there is a need for security awareness program, but the content of the training and the message to convey may be of similar debate to that of security policy. Nonetheless, we must maintain the focus on developing and strengthening the program around the issues and obstacles we face daily. A good metric to use is ISO 17799's Critical Success Factors for Information Security, which is noted as follows:

a) Security policy, objectives, and activities (e.g. Security Awareness) that reflect business objectives;
b) An approach to implementing security that is consistent with the organizational culture;
c) Visible support and commitment from management
d) A good understanding of the security requirements, risk assessment and risk management;
e) Effective marketing of security to all managers and employees;
f) Distribution of guidance on information security policy and standards to all employees and contractors;
g) Providing APPROPRIATE TRAINING and EDUCATION;
h) A comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement.[13]

Key audience groups have been discussed throughout, but a very pivotal faction not yet discussed is the awareness trainers and leaders. We need to strive for continued learning for security staff members, which we can then pass on to others in awareness programs. We cannot keep up with all of the issues only by newsletters, so we must push management to enable us with dedicated training away from day-to-day activities, which will fuel our learning.

The saga we face continues, but let us remember…. BE AWARE!

ACKNOWLEDGEMENTS

The author wishes to acknowledge Jeff Lowder and Paul Stamp who proofread an earlier version of the practical and offered valuable suggestions for improvement.

[13] ISO 17799, p. x-xi.

© SANS Institute 2000 - 2002, Author retains full rights.

Bibliography

References

Baig, Edward C. "Unlock the secrets of security for your laptop." 09 Apr 2002. <http://www.usatoday.com/life/cyber/ccarch/2002/04/10/baig.htm> (Apr 2002).

Balian, Cheryl. "Report: Internet Attack Trends More Malicious Than Ever." 15 Apr 2002. <http://www.infosecuritymag.com/2002/apr/digest15.shtml> (Apr 2002).

"Creating a Human Firewall."
< http://www.humanfirewall.org/images/blueprint_small2.jpg> (Apr 2002).

"Cyber crime bleeds U.S. corporations, survey shows: financial losses from attacks climb for third year in a row." 07 Apr 2002.
<http://www.gocsi.com/press/20020407.html> (Apr 2002).

"FBI Survey finds computer attacks up." 08 Apr 2002.
<http://www.usatoday.com/life/cyber/tech/2002/04/08/fbi-survey.htm> (Apr 2002).

Heimerl, Jon-Louis. "The 'Other' Side of Information Security." 28 Nov 2001.
<http://www.infosecnews.com/opinion/2001/11/28_03.htm> (Jan 2002).

< http://www.dictionary.com/search?q=awareness> (Apr 2002).

< http://www.dictionary.com/search?q=knowledge> (Apr 2002).

ISO/IEC 17799 Information Technology Code of Practice for Information Security Management, ed. December 2000: x-xi, 1.

McBride, Patrick. ComputerWorld. "How to Spend a Dollar on Security." 09 Nov 2000.
<http://www.computerworld.com/cwi/story/0,1199,NAV47_STO53651,00.html> (Apr 2002).

Messmer, Ellen. "Put to the Test: New threats force intrusion detection vendors to rearm." 15 Apr 2002.
<http://www.nwfusion.com/news/2002/0415idsevad.html> (Apr 2002).

Middleton, James. "Security flaws leave Oracle users exposed." 18 Mar 2002.
<http://www.vnunet.com/News/1130185> (Apr 2002).

Nuessle, Shelly. "Invest Your Security Dollar for Maximum Return."
PASSWORD the ISSA Magazine April 2002: 5-7.

© SANS Institute 2000 - 2002, Author retains full rights.