Interested in learning more about security?

SANS Institute
InfoSec Reading Room

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

The social approaches to enforcing information security

Business security is becoming more strategically important everyday for sustainability, economic growth and future health. This report's focus is on enforcing information security using social approaches in the business environment. Most businesses have, or should have policies in place for various standards, procedures and guidelines. Although policy is a great tool to have in a business, a policy is only as good as its compliance from management and staff. This paper will focus on ways to improve policy compliance us...

Copyright SANS Institute
Author Retains Full Rights

AD

The social approaches to enforcing information security

Roger Gilhooly
December 11, 2002
Version 1.4b

Abstract

Business security is becoming more strategically important everyday for sustainability, economic growth and future health. Although security in business is a very broad topic, for this report, the focus is on enforcing information security using social approaches in the business environment.

Most businesses have, or should have policies in place for various standards, procedures and guidelines. Although policy is a great tool to have in a business, a policy is only as good as its compliance from management and staff. This paper will focus on ways to improve policy compliance using a social approach in the business hierarchy from employees to the CEO of a company. Many companies focus a great deal of time and money on new technologies for example, physical and logical barriers such as IDS systems, security guards and data protection mechanisms.[1] Although these methods work very well, intruders of your systems will always find ways around these technologies using other methods of attacks such as social engineering or internal threats.[2] In fact, numerous studies show that at least 65 percent of all company threats are internal.[3] The best approach to tackle this type of attack is to be close with employees and management utilizing more social approaches as opposed to technology focuses to achieve policy enforcement.

Introduction to Social Approaches to Policy Enforcement

Every company treats and looks at policies differently because every company is unique. Depending on how the company as a whole acts to policy will greatly impact the business at all levels of operations and productivity through standards, procedures and guidelines. The timely manner in which policies are created has an impact on policy compliance because it may become more difficult to keep track of all of the policies, or some policies that that were meant to be created were not. An example is if a company creates or changes policies throughout a company on an almost daily basis. Employees may lose track of current procedures, standards or guidelines or simply stop caring about the policy altogether since the policies appear to be changing everyday. How

---

[1] http://www.entrepreneur.com/Your_Business/YB_SegArticle/0,4621,298386,00.html
Article called : Security threats from within
[2] http://security.vt.edu/gotoclass/IT%20FDI-Summer-2002.ppt
Article called: Information Technology security at virginia tech
[3] http://www.expressitpeople.com/20021118/cover.shtml
Information security through awareness and education

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

management behaves in regards to policy is an important issue to look at as well, because management should respect company policy the same way employees are expected to. If company policy is not followed at all levels of a company then employees or other management may decide to follow suit and not follow the policy either thus, creating a security breach. Employees and management should receive the proper security awareness training of potential threats to company business and infrastructure. Training gets everyone in the company involved in security as well as teaches them how to recognize the importance of security in their company. Internal threats are a company's greatest weakness and can be the hardest threats to recognize. Lastly, proper business ethics in the business place should be outlined and signed by all employees upon employment with the company. Enforcement of employee ethics should be further enforced through group discussions. An ethical outline helps define to employees what is considered correct business etiquette to use while in the business place. Although using social approaches to defend against these threats will not make your company completely secure, it is a piece to the security puzzle and can be the difference between a secure company and an insecure company.

Policy Creation Timelines

Companies, particularly new growing ones, run into new policy related issues on an almost daily basis, which may result in the need for a new policy. This is due to issues constantly arising as the company proceeds along its growth curve. The larger a company grows the more policy will have to change with that growth because of employee numbers, economical capabilities and the time invested into the company.

It is up to security management and department managers to decide how often policies should be updated to conform to the changing demands. Items to address when creating or updating policy are money, time, and critical risk. Creating new policies costs money through the time and manpower it takes to generate them. Policy creation can take up a lot of business time through meetings, research and publishing of new policies, which can impact other business functions. Depending on how critical the policy is will greatly impact the amount of effort that will be put into the new policy. Exploring each of these considerations in depth while formulating new policy can be very beneficial to the company and can save time, money and losses of assets.

When an issue arises that may require a policy to be generated, often companies will change the existing policy and send out the policy to staff. The problem with this is that sometimes not all employees will receive the new policy due to an employee absence. A solution to prevent this frequent occurrence is to update policies or add new policies on a predetermined timeline. The timeline can vary depending on the company size, budget, and manpower. When an issue arises in between timelines that may require an immediate policy, instead of creating a

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

new immediate policy a simple email pertaining to the issue may be a more efficient approach. An email will allow you to send out a warning to all employees and management of the situation and will save money by not having to go through the entire policy creation process. This can also help prevent from a policy being rushed thus, causing a sloppy or incomplete policy. It may be necessary to send out a follow-up email after the initial email (1 to 2 months) to further ensure everyone is in compliance.

When the time comes for a new policy guide to be issued, the policy outline should be used to its full capability. The main sections of a policy are as follows:

- Background
- Policy
- Definitions
- Scope
- Responsibilities
- Sanctions
- Reviews
- Coordinator

Although some portions of the existing policy may not change it is important to always review each section when updating it. This ensures no changes are overlooked and ensures that the policy is completely accurate. Once company policies are updated the policy needs to be signed by the CEO and should be signed by all section heads affected by the policy, thus ensuring that everyone acknowledges and understands the policy.

Management and Security Policy

A major issue, with enforcing security policy is how some management can fail to adhere to company policy. A good security manager should explain to the CEO and upper management why it is important to follow the same guidelines as everybody else. Management not following guidelines sets a very bad example for the rest of the company and is a security risk whenever anybody doesn't follow guidelines. The policies are in place for everyone in the company to follow and abide by unless otherwise specified. When management follows the policy and guidelines they set an example for the rest of the company. Management not following policy may also lead to resentment or a low moral from company employees. For example, if parking spaces were assigned and a manager started parking wherever she/he pleased, other managers or employees would be more likely to park in choice spaces as well. The policy had been designed and implemented to prevent against burglary in the parking lot and now, because no one is parking in their assigned spots, the policy is being broken. All of the time, money and manpower put into creating the policy have been wasted due to managers using their superiority to their advantage.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

To help in persuading management to follow policy, good arguments to promote policy compliance are:

- Can you afford not to?
- Employees pay attention to what you do
- You helped create the policy you should abide by them the same way
- CEO and management pledge to follow policy

The question of "Can you afford not to?" can be a very powerful one for a CEO. If an issue does arise the CEO wants to be sure to evaluate the business risks.

No one wants to be forced to follow guidelines especially if everyone involved is not following the policies that are in place. Another good strategy to policy enforcement is to lead by example.[4] Employees and management alike will feel more obliged to follow the policy if everyone in the company follows it. It is important for the leaders of a company too not only lead by rules and consequences, but by example as well. If the leadership of a company cannot follow the policies in place then how can they expect anyone else to? They cannot because they broke their own responsibilities to the business.

Getting management involved in the policy creation process can help to enforce that same management to follow the policy. "You helped create the policy therefore you should abide by it", means that they would be contradicting their own rules. No one (especially a manager or CEO) wants to break the rules they helped create because it would make them look bad not only to the staff but also the people in charge of them.

The most insurance a security practitioner can receive from management are for management to pledge to follow the policy guidelines in place. It is important that when a manager agrees to pledge to the policy guidelines, to have them sign a document, dated, with a witness to ensure compliance and understanding of the agreement.

Awareness through Education

A major step to enforcing policy in any company is through education.[5] Employees cannot be expected to recognize a threat if they don't know what a threat is. An employee's ignorance will always be more expensive then education in the long run. Most corporations now have access to security awareness programs for employees and managers. Security awareness training helps give staff a better understanding of information security and best practices.[6] Although,

---

[4] http://www.achrnews.com/CDA/ArticleInformation/features/BNP__Features__Item/0,1338,19520,00.html
Best Suggestion for Owners: Lead by Example
[5] http://www.expressitpeople.com/20021118/cover.shtml
Information security through awareness and education
[6] http://www.redsiren.com/infosecu.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

these awareness programs may be expensive, they are not as expensive as an employee accidentally giving away trade secrets or other company sensitive information. A quote from Colin Rose, product manager with the network security company Iomart, “Staff are the biggest threat if they don’t have any education”.[7]

There are various security-training organizations through out North America and internationally. The key for your company is to find the training that meets your company needs and budget. The following survey acts as a guide to help determine the specific needs, timeframe to meet these needs, and the importance of each need to a specific company.

Number of employees in need of training:
Do the employees have any prior security background? ❑ None ❑ Basic (Basic security awareness) ❑ Intermediate (Familiar with IDS devices, possesses networking skills, etc.) ❑ Advanced (Information Systems Security Administrator or equivalence)
When do the employees need to be trained by: ❑ Less then 1 week ❑ Within 1 month ❑ Within 1 year ❑ After 1 year
How early can employees begin training? _____
How should the training be laid out: ❑ Part time training (nights) ❑ Part time training (days) ❑ Full time training (days)
Are there specific dates when employees cannot be in training? ❑ No ❑ Yes

Red siren education training

[7] Pg.21 Honeypots, intrusion and education. SC Magazine

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

If yes, please specify which dates are unacceptable: _____ _____
Please specify where employees can be trained: ❑ At the workplace ❑ At a separate facility provided by the training company ❑ At a separate facility sponsored by your company ❑ Employees can work from home Other, please specify: _____

In what areas do your employees need training? ❑ Data Security ❑ Passwords and Encryption ❑ Data Disposal ❑ Proper internet use ❑ Handling of computer evidence ❑ Property protection ❑ Computer viruses ❑ Hackers ❑ Desktop protection ❑ Best practises	❑ Disaster Planning ❑ Ethics ❑ Tempest ❑ Computer abuse ❑ Email ❑ Incident handling ❑ Firewalls ❑ Intrusion detection ❑ VPN Security ❑ Other Other, please specify: _____

Please specify your top 3 most important areas for training: 1. _____ 2. _____ 3. _____

Utilizing the survey, important data has been gathered such as the areas required for training, the timeframe in which to meet these areas and the importance of each area. The company should now have a good idea on the areas to focus on in its search for the appropriate security awareness training. The training company itself should also be accredited with experience and success. It is recommended to ask such questions to the security training company as:

- Are your instructors certified?
- What will our employees get out of the training?
- When and for how long will the courses take place?

© SANS Institute 2003, Author retains full rights

- Where do you provide your training?
- Why should we receive our training from you instead of someone else?

These questions are of significant importance to you because they can give you information on who, what, when, where and why. The who are the instructors, as to whether they are certified or not. The instructors should be qualified to teach security. What the instructors will teach to the employees is important because you want to be sure that your company will receive the proper training specified from the Specific Company Needs Survey. It is important to find out when and for how long the courses will take place. If your company needs the employees and/or management trained within a year it is important to determine whether the training company can reach this objective. Where the training is going to take place is necessary because your company may not want to send its employees away. Depending on where the training is, it may be easier for you to only send five employees at a time for training. The training company may teach the courses at your company headquarters but it is often better to teach at a facility away from the distractions of normal office routine. The security awareness company should be able to tell you why their services are of value to your company. Find out what your employees will get out of their training that their competitors cannot provide. If they cannot explain to you why they are suitable to train you better then anyone else, then they are not the right training company for you.

There are many possible training schools available. Just go to your favourite search page and type in security training, at least a hundred different schools will appear. As far as training goes security and network personnel should take more advanced courses then other employees. Below is a list of the recommended training companies for each type of employee.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

IT Staff/Security:	Everyone else (Employees, Managers):
Sans Institute http://www.sans.org	Information Systems Services http://www.leeds.ac.uk/iss/training/
CERT http://www.cert.org	Pro-ware Computing http://www.prowarecomputing.com
Internet Security Systems (ISS) http://www.iss.net/education/certification/	Interpactinc Security Awareness http://www.interpactinc.com/

The appropriate security awareness training company will depend on your specific company needs. Although companies can customize to your needs a company who readily trains employees for your specific needs is a wiser solution. This is because the company will have experience in teaching for your direct needs. A company that customizes the training for you may mean they have never trained anyone for your needs. Rather then take the chance of not meeting your criteria for your employees it is suggested to call companies of interests until you find one with the knowledge, experience and expertise to meet your company's needs.

Ethics and Security

When discussing social security approaches nothing is more important then the role ethics plays. Ethics should be enforced on employees from the minute they are hired to the minute they leave the company. When an employee is first hired, the original agreement contract between employee and company should discuss the importance of ethics not only to protect the company but to protect the employee as well. This ensures that all parties are in understanding and agreement of what is expected in the relationship.

Methods in which to induce and monitor ethics in the workplace can be done using a company code of ethics. A company code of ethics defines the basic ground rules for companies day-to-day operations. The reasons for introducing a company code of ethics are:[8]

[8] http://www.ethicsweb.ca/codes/coe2.htm

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- To define accepted/acceptable behaviours
- To promote high standards of practice
- To provide a benchmark for members to use for self evaluation
- To establish a framework for professional behaviour and responsibilities
- To use as a vehicle for occupational identity
- To use as a mark of occupational maturity[9]

By employees signing off on the code of ethics, they acknowledge having read and understood proper business conduct for example, the submission of corporate information to the public or the competition, acceptable employee behaviour, and employee safety.

The ethical agreement reached by employee and company is usually reached at the beginning of an employee's position with the company. The ethical agreement is often read and signed off by the employee at the same time as all of the other beginning paperwork such as tax forms, insurance applications and employee handbooks possibly polluting the dialogue and importance of the ethical agreements.[10] Although it is important for the new employee to sign a company code of ethics, ethics should be communicated to company employees throughout the relationship of employment. Methods of future ethical updates and reminders are:

- A company newsletter with a section devoted to ethics to which employees can send in real or hypothetical ethical dilemmas. Experienced personnel can respond with solutions.
- Client presentations in which clients are invited to discuss current project sites and goals, providing employees with an opportunity to appreciate the tangible value of their work.
- Brown bag lunches that can serve as informal sessions led by any staff member to discuss current corporate ethics issues in the news. How have corporations handled problems? What would employees suggest?[11]

Everyone has different ethical beliefs although some ethics may be agreed upon unanimously some ethics can have a fine line between what is right, and what is wrong. It is for this reason that ethics should be taught and discussed as a group, and not as an individual assignment. Ideas for stemming growth in this area are monthly meetings and group discussions regarding issues relating to policies. Group discussions will allow employees to get varying opinions of ethical issues instead of only relying on their own.

Ethics in the business place do change with time and growth of a company (although some principals will always stay). It is important to have proper ethical

[9] http://www.ethicsweb.ca/codes/coe2.htm Quoted from Why Have a Code of Ethics?
[10] http://www.stl-inc.com/WhyChooseSTL/ethics.pdf
[11] http://www.stl-inc.com/WhyChooseSTL/ethics.pdf Quoted from pg. 5

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

conduct outlined and signed by employees from the initial employment and along the employees' maturity within the company. Ethics should be discussed as groups to ensure agreement upon proper business etiquette as well as allowing employees to voice their own views and opinions. Defining ethics in a business provides a justification and guideline of what is right, and what is wrong in the business place.

Conclusion

New technologies are coming out all of the time and these technologies will be used to monitor your network, or enforce policy-using software, etc. These methods will be eventually subverted, whether it is through social engineering or the development of technologies that break the current ones. A prime example of this is a radar detector the police use to monitor vehicles speeding. To break this, people came up with a radar detector detector helping speeding drivers discover where police were using these devices. The connection is that technology is subverted and we don't know when it will be subverted or where. It is up to people to use proper judgement in determining a potential threat and the way to do this is through using more social approaches to enforcing information security.

Social approaches to enforcing security policy are through following policy creation timelines, dealing with management and security policy, educating employees and ethics. This report defined these issues and provided examples and solutions for each of these approaches.

Social approaches to security need to be used because they fill in any of the gaps that technology may have missed. Since security threats are changing all of the time and since the top 10 exploits are technology based, employees are always a target to trigger exploits in your companies security. As technologies grow, so will the lack employees put towards security and this is why more social approaches to security are necessary.

References

Vogon International Limited. "Vogon IT Security and Forensic Training". 2002 URL: http://www.vogon-computer-evidence.com/ Sub directories: investigation_services-00.htm, evidential_systems-00.htm, awareness_training-02.htm, awareness_training-10.htm. (2002-11-25).

Berg, Al. Canadian Initiative on Workplace Violence. "Making & Enforcing Corporate Policy". http://www.workplaceviolence.ca/corporate/corp-intro.html. (2002-11-25).

Sati*Star. "Policy Deployment". 1999-11-20. http://www.satistar.com/policy.htm. (2002-11-12).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

O'Farrell Neal. "Employees: Your best defence, or your greatest vulnerability". Executive Security Briefing. 2001-06-28. http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci751955,00.html. (2002-11-12 - 2002-11-25).

Kensington Technology Group. "Employee Education Tools". I.T.Tools. 2002. http://www.microsaver.com/tools/too_1003.html. (2002-11-20).

Granger, Sarah. "Social Engineering Fundamentals, Part I: Hacker Tactics". 2001-12-18. http://online.securityfocus.com/cgi-bin/sfonline/infocus.pl?id=1527. (2002-11-12).

Bruck, Michael. "Security Threats From Within". 2002-04-01. http://www.entrepreneur.com/Your_Business/YB_SegArticle/0,4621,298386,00.html. (2002-11-25).

Marchany, Randy. Donald, Wayne. "Why User Education". Information Technology Security at Virginia Tech. 2002. http://security.vt.edu/gotoclass/IT%20FDI-Summer-2002.ppt. (2002-11-20).

Delhi, New. Jasrotia, Punita. "Information security through awareness and education". 2000. http://www.expressitpeople.com/20021118/cover.shtml. (2002-11-12)

King, Ruth. "Best Suggestion For Owners: Lead by Example". 2001-01-29. http://www.achrnews.com/CDA/ArticleInformation/features/BNP__Features__Item/0,1338,19520,00.html. (2002-11-25)

Redsiren. "Educational Services". Preventive Solutions. 2002. http://www.redsiren.com/infosecu.html. (2002-11-25)

MacDonald, Chris. “Why have a code of Ethics?”. Creating a Code of Ethics for Your Organization. http://www.ethicsweb.ca/codes/coe2.htm. (2003-01-23)

Loring A, Deborah. Smoren, Bonnie. “Where Do Company Ethics Programs Fall Short”. http://www.stl-inc.com/WhyChooseSTL/ethics.pdf. (2003-01-23)

Condon, Ron. Tullett, Jon. Parkhouse, Jayne. “Honeypots, intrusion and education”. SC Magazine. December 2002. pg 21. (2003-01-05)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced