Global Information Assurance Certification Paper

InfoSec in the real world: A pragmatic approach to implementing an effective security policy

Abstract:

At last, the whole subject matter of Information Security ("InfoSec") is receiving greater attention and more companies are beginning to take seriously the threat that security breaches may have a serious impact on the well-being - or, indeed, the very existence - of their businesses. This awareness brings with it increasing pressure on InfoSec professionals - many of whom, especially in smaller organisations, may have reached their position as "the company security expert" by default or without the benefit of specialised technical knowledge or traditional management training. This situation creates pressure from both ends: the need to keep up to date with the latest technical trends and vulnerabilities, as well as a need to present highly complex technical issues to lay management in order to secure the necessary funding and/or actions. This paper examines some of the ground rules needed to ensure that relevant InfoSec information is gathered, presented and acted upon in an effective manner under typical business constraints, such that an effective Security Policy can be established in every organisation, regardless of its size and complexity.

Why is a security policy important?

A company's Security Policy is the central repository where intangibles such as corporate philosophy, mission statements, culture, attitude to risk and other "hard to define" parameters can finally be crystallised into enforceable, measurable, action statements, procedures and ways of working. By focusing on a company's Security Policy, the InfoSec professional can effectively have a meaningful impact on the actual fabric of everyday business activities within an Information Security context.

Who needs a security policy?

All organisations need a security policy. As well as including the obvious examples such as medium or large corporations, this statement also extends to include small "SOHO" type businesses as well as purely "home use" PC's which also need protection if they are ever to be connected to the hostile internet environment. The threats to the integrity and therefore dependability of any computer system are increasing daily from the increasing sophistication and proliferation of intruder attacks and "malware". Therefore no matter

what the mission or purpose of a system, it is essential that to avoid such capability being compromised an effective security policy must be in place. Clearly the sophistication and scope of s uch a policy will be influenced by the size and nature of the organisation itself, but the underlying need for a security policy is nevertheless irrefutable. However, for the purpose of this discussion, we will constrain ourselves to a few general principl es which will remain effective regardless of the size of the organisation into which they are applied.

In many smaller businesses, the responsibility for forming and, ultimately, implementing and maintaining a security policy will fall to an IT technician or small IT-centric team. Often, this team's prior knowledge and understanding of security issues may only have come about as a by-product of their more general association with IT activities. Traditionally, and all too frequently, security has been tacked on to the general duties of whoever is responsible for system or network administration. It is only recently that the issue of security policy itself has raised it's profile to the extent that it is now receiving the attention it deserves, often involvin g a multidisciplinary team, or at least incorporating at least one team member having formal training in specialist security matters.

A security policy should reflect the philosophy and culture of the organisation itself - in many ways the security policy is the formal embodiment of the "ways of working" and informal culture which would otherwise remain qualitative as opposed to quantitative. Defining a security policy is an opportunity for an organisation to simultaneously **de**fine and **re**fine its collective attitude to both its internal operations and external relationships, and, as such, embraces all aspects of the organisation's operations, not just those directly impinged by "IT". In the extreme, some have used this mechanism to actually enforce a company 's otherwise implicit security policy by coding such rules into (for example) a perimeter firewall, thereby enforcing hitherto "unspoken" (and probably, therefore, unenforced) policy.

How should we start the security policy process?

One of the early step s in defining a security policy is to undertake a "state of the nation" review, in which the company's current approach to security-related matters needs to be examined. In a small company (e.g. a SOHO company), existing arrangements might comprise solely of the use of an antivirus package, or, increasingly, the use of personal firewalls on individual hosts, such as Zonealarm or Tiny Personal firewall. Larger, more "internet -

active" companies with "always on" Internet access (increasingly, ADSL or cable modem connected systems) might well already have a firewall in place at the Internet threshold providing some limited intrusion detection and prevention via simple packet filtering. A company whose business implicitly involves public Internet access (for example, a bank, or B2C trader) might already have more sophisticated trading protection protocols in place (e.g. SSL or SET), as well as a secure architecture deploying DMZ's and physically separate network segments. Nevertheless such organisations remain vulnerable to "back door" intrusion via unprotected PC modems or malware introduced into the company environment by other mechanisms such as buffer overflows or other exploitable security holes.
Or a company with an already established security policy may still need to consider system-wide upgrades, such as the need for centralised logging of distributed host-based intrusion detection systems to minimise time spent analysing and correlating logs from many different systems. Security Policy is a continuous process of evaluation and monitoring and what may have been sufficient or appropriate yesterday may well be inadequate and unprepared today. Whatever the size of an organisation, and whatever its current state of information security policy, there is always scope for a useful review of current policies and procedures. Just as security itself is not a product but a process, so it is necessary to constantly ensure that an organisation's security policy continues to meet the changing and evolving needs of the underlying business. A security policy is just a snapshot in an ever-evolving movie.

Structuring a security policy

In larger organisations, an overall security policy may comprise several sub-policies, such as a program policy, issue-specific policies, and perhaps system-specific policies. The program policy describes who is responsible and how compliance is to be monitored and ensured. It may also refer to external standards with which the policy is intended to comply, such as BS 7799 [2], part I (ISO17799) or ITIL (IT Infrastructure Library) [3]. Additionally, it will make reference to any issue-specific or system-specific policies to which authority has been subsumed.

Examples of issue-specific policies include those dealing with password standards and change procedures, acceptable Internet usage, anti-virus precautions and backup polices. System-specific policies may be invoked on individual systems requiring special measures, for example the need to place a root Certificate Authority's LDAP server in a secure, caged physical environment.

Every security policy, at whatever level, should at least address the following issues: -

- Specify the purpose of, and reason for, the policy
- Refer to related documents or policies providing additional guidance or detail
- Specify what is "in scope" and "out of scope"
- Mention any previous policies which are updated or cancelled by this policy
- Clearly state what actions should be taken, by whom and how often.

It is also important to ensure that the right people provide input into the formulation of the security policy and that it is eventually signed off at the right level and by all interested parties. As well as the operational departments themselves, input may be required from areas such as HR and Legal & Compliance, to ensure conformity with employment rules, civil laws and any industry - specific regulations (for example in banking, insurance or securities).

Depending on the size and complexity of the organisation, there may be a need to specify policies to apply to different c orporate levels, such as having an enterprise policy, divisional policies, and local policies. It should be clear whether lower level policies implicitly inherit the properties of a higher level policy or whether it is permissible for lower policies to be allowed to depart from general principles for the sake of local expediency or special circumstances. All policies, however, at every level should be: -

- Consistent, prudent and expedient
- Clear, concise and realistic
- Forward looking
- Readily available to all interested or affected parties
- Capable of being monitored for compliance or breach by use of effective metrics
- Possess inherent mechanisms for regular review and update

It is also important to differentiate between policies and procedures: essentially, p olicies deal with the "who", "why" and "what", whereas procedures focus on the "how", "where" and "when". The use of checklists is to be encouraged in carrying out procedures, particularly where the procedure may need to carried out under conditions of stress or duress (for example during a live security breach).

Who should gather information for the policy?

Too often, the task of information security is "tacked on" to an existing role or to the responsibilities of existing staff, frequently a system or network admin. functionary. This can have the effect, in priority terms, of downgrading the vital task of Information Security to a "when you have time" or "while you're looking at the network, look at this too" kind of activity. Such practice is increasingly dangerous and every organisation should take a step back to assess the real needs and level of importance of its InfoSec policy. And there is no hard rule which says that the Information Security Office should be part of the IT function. InfoSec spans every aspect of a businesses' operations and while much interaction between the IT function and the InfoSec office will be necessary, it is by no means a corollary that the InfoSec office will report through the IT function. The role of Chief InfoSec Officer should be carefully thought out, together with the scope of duties, responsibilities and reporting lineage. The fundamental support and co-operation of every corporate department is a prerequisite.
A key attribute of an InfoSec officer (as well as having appropriate technical knowledge and relevant, current experience) is an ability to communicate at all levels of the company. For InfoSec is not a "stand alone" activity but one which depends heavily on the commitment, co-operation and understanding of everyone within the organisation, from the chief executive through to the office cleaner. The InfoSec initiative must be sponsored and approved at the top level of management and its objectives and procedures effectively communicated through every level of the organisation. Too often, many company members view the consequences of an effective security policy as being restrictive or preventing them from doing their job as a result of outside "unnecessary" interference. Some individuals may even react negatively to any restriction by deploying their own intuitive "rules were made to be broken" principle. If it is to be effective, everyone in the organisation will at some point be touched by a properly enforced security policy and it is therefore essential to its continued effectiveness that any such contact should be viewed in a constructive, rather than restrictive sense. Even the best security policy can be compromised by non or reluctant compliance by a company's employees and any more extreme response on the part of internal personnel can be potentially more dangerous than deliberately vindictive external attacks. So communication, training, regular briefings, and involvement are all crucial factors in ensuring that a company's security policy remains effective.

Presenting your case

Another key skill in the InfoSec officer's armoury is the ability to gather and present information in an effective and constructive manner. For example, a key step in the security policy process is to conduct a risk assessment o r threat analysis. A good place to start this process is by examining the traditional threat vectors and assessing their relevance, vulnerability and impact on your particular business. This information must then be presented to an internal decision -making body in such a way as to make the risks and consequences very clear, as well as presenting a portfolio of options and actions available. Remember that decisions on InfoSec policy, while being of the utmost importance and relevance to the InfoSec officer h imself, are only one of the many (often conflicting) areas of activity competing for the attention and spending power of the manager responsible. It is therefore crucial that the InfoSec officer is able to compose a clear and comprehensive view of the situation for presentation.

No matter what stage your company's InfoSec policy has reached, there is always scope for improvement and refinement. Before embarking on any research, training course, demonstration, presentation or report, it is important to know where such a step lies in the overall context of improving the company's security infrastructure. Every activity should have an ultimate objective, whether it is to "upgrade our packet filtering firewall to an application gateway proxy server" or to "impl ement a configuration change management policy to monitor software upgrades, patches and tripwire-protected binaries and system files". Be aware, however, that, generally speaking, an objective such as "showing how many new TLA's* I can use to simultaneous ly impress and confuse my audience" should be avoided.
*(Note: *TLA stands for Three Letter Acronym, and their excessive use by over enthusiastic IT specialists is a common complaint amongst overburdened lay management).*

Any basic report or presentation s hould cover at least the following, in clear, understandable language, with all purely technical terms included only as of necessity :

- The current situation
- The threats faced, together with an assessment of vulnerability
- The likelihood or probability of these risks occurring in the foreseeable future (remember: risk = threat x vulnerability)
- The impact, in terms of cost or business impact, if any of these risks occurred

- How these risks may be reduced, mitigated, transferred or eliminated
- Why action needs to be taken
- What actions are available and the consequences & cost/benefits of each

You should focus initially on items which have a high probability of occurrence combined with high impact. These are the items which could literally bring your business to its knees and are the ones for which you are likely to receive initial agreement and funding in order to secure the company's immediate situation. Go for some "easy wins" – some initial milestones which will set the path for the continuing development and researching of your enterprise-wide security policy structure.

While it is always dangerous to assume the outcome of any meeting or presentation, it is always worth having a number of solutions or action plans available. It is not unknown for suitably dynamic management to listen to a concise, comprehensive and informative presentation and then say "OK, we now understand the dangers we face. Now tell us what should we do about it." At this point, it is essential to be able to offer several options, ranging from "let's make a more detailed study" through to "I happen to have here a comprehensive 2 year plan detailing every step of a new InfoSec policy which addresses every one of the issues just raised. Please sign here."

The right response will depend on the current state of readiness of your particular organisation, the budget available and the predisposition of management to take appropriate and speedy decisions. At the very least, you must be in a position to capitalise on the interest which your risk assessment and security policy fact-finding work has raised and to transform this into agreed and confirmed actions. Remember, your aim is always to continue to move the company's security policy one step closer to its objective - an objective which itself is a moving target as technology and the increased sophistication and scope of potential security threats continues to expand. The trick is to move closer to the objective faster than it is moving away from you. Remember also that you are competing for management time, attention and spending power along with several other departments or functions, all of whom see their own pet project as being the most important. Only you know that ensuring good information security is the determining factor as to whether they, or, indeed, the company as a whole will still be around to be able to make such decisions in a couple of years time!

Above all, remember that implementing a security policy is a never - ending process involving constant review and revision, as well a s constant vigilance to ensure that you always stay one step ahead of "your enemy". The term "information warfare" has been coined to depict this situation, and warfare is indeed an apt description of the subject matter. Except that these days "information terrorism" may be even more appropriate, since, like its counterpart in the physical world, the difference between warfare and terrorism is that, at least with conventional warfare, your enemy is readily identifiable - whereas the terrorist uses stealth a nd deception and exists in loose groups and associations which frustrate any co -ordinated action along traditional lines – just like Infosec's crackers and malware distributors. And, as in all forms of warfare, beware the enemy within…..

It's quite a cha llenge – and that's what makes it so interesting!

Further reading: -

Links: -

1. SANS Model Security Policies:
   http://www.sans.org/newlook/resources/policies/policies.htm
2. BS 7799 portal leading to several informatory sites
   http://www.yourgateway.to/bs7799/
3. UK ITIL site
   http://www.itil.co.uk/about_itil/concept.htm
4. SANS Reading Room – Papers on Security Policy Issues:
   http://rr.sans.org/policy/policy_list.php
5. RFC 2196: Site Security Handbook
   http://www.iet f.org/rfc/rfc2196.txt?number=2196
6. RFC 2504: User's Security Handbook
   http://www.ietf.org/rfc/rfc2504.txt?number=2504
7. Information Security Officer's Manual - the ISO Manual.
   http://www.eon -commerce.com/rusecure
   (commercial site but sample policies available for download)
8. Security testing methodologies: http://www.ideahamster.org

9. Concerns and issue s of "those on the frontline" www.securityfocus.com (29 specialist mailists available for free subscription)

10. Common mistakes leading to security breaches: www.sans .org/mistakes.htm

11. The open source security testing methodology manual v. 1.5
http://uk.osstmm.org/osstmm.htm

12. Worldcom white paper:
http://www1.worldcom.com/us/resources/library/reports/security/true_security.pdf

Books:-

1. Securing Windows NT/2000 servers for the Internet -Security checklists for system administrators.
O'Reilly ISBN 1 -56592-768-0

2. E-commerce system s architecture & applications, Wasim E. Rajput, ISBN 9781580530859

3. Essential System Administration, Aeleen Frisch, ISBN 9781565921276

4. Secrets and Lies, Bruce Schneier
Wiley ISBN 0 -471-25311-1

5. Database Nation: The Death of Privacy in the 21st Century.
Garfinkel, S. O'Reilly ISBN 1 -56592-653-6.

6. Hacking Exposed, 2nd Edition Joel Scambray, Stuart McClure, George Kurtz
McGraw-Hill Professional Publishing; ISBN: 0072127481

7. Building Internet Firewalls (2nd Edition) Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman
O'Reilly & Associates; ISBN: 1565928717

Last Updated: July 24th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor