Interested in learning more about security?

SANS Institute InfoSec Reading Room

Developing a Security Policy - Overcoming Those Hurdles

This paper describes the real-life experiences involved in developing a security policy and gaining its endorsement in a medium sized company. The major challenges, as with all companies, is the big cost factor and the acknowledged belief that security is not a real issue. After all, who'd want to attack us and what damage could they do? There is a real belief among companies that it won't happen to them and we can recover if it does. What many companies don't realize is that attacks can occur without warning and for n...

Developing a Security Policy — Overcoming Those Hurdles

Prepared by: Chris Wan

GSEC Practical Assignment Version 1.4b, Option 2

Date: 24 April 2003

Abstract

This paper describes the real-life experiences involved in developing a security policy and gaining its endorsement in a medium sized company. The major challenges, as with all companies, is the big cost factor and the acknowledged belief that security is not a real issue. After all, who'd want to attack us and what'd amage could they do? There is a real belief among companies that it won't happen to them and we can recover if it does. What many companies don't realize is that attacks can occur without warning and for no apparent reason. Attackers don't necessarily steal information. They can bring your servers or systems down in a denial of service attack or they can compromise the integrity of your systems. Attackers don't need reasons, only opportunities.

This paper hopes to describe how to bypass and manage some of these hurdles and gain the acceptance of executive management. Without executive management endorsement of the security policy, it won't be effective or taken seriously. This paper also hopes to give some guidance on the steps to developing a security policy and what to do after the security policy is endorsed. Hopefully this will give others some insight into the security policy process and help them face their hurdles.

We Need a Security Policy

I'm a consultant working in a medium-size consulting firm where the main emphasis is on billing and revenue generation. If you're not billing to a client, you're an overhead. That was the main reason why I was sent for security training. It was a useful skill that could be used for billable projects. Work associated with internal processes and administration is viewed as low priority often performed by overheads. Hence our IT department was recently cut in half to reduce costs. The company could not seem to grasp the significance of spending in IT, especially security. Surveys of large companies have shown that many organisations cannot effectively determine their return on investment (ROI) when it comes to security spending [6].

As a consequence, we currently have no helpdesk and absolutely bare minimum support. I also discovered we had little or no basic security controls such as enforced password rules, access controls and secure remote gateways just to name a few and no intrusion detection. Our systems were wide open to an attack and we wouldn't even know if we were under attack. It wasn't surprising to discover that we didn't have a security policy.

As a result of an IT infrastructure review conducted by an external auditor, it was recommended that our company establish a formal IT Steering Committee to deal with issues of a corporate IT nature and develop a security policy to address the security issues that were discovered during the review. The IT Steering Committee was quickly established for this purpose and I was asked to develop the policy and recommend options for its implementation.

What is Information Security?

Before I could even start, I had to understand what a security policy was and what information security was all about. As I discovered, the purpose of information security is to ensure business continuity and minimise damage to the business by preventing or minimising the impact of security incidents. Information security management enables information to be shared, whilst ensuring the protection of information and computing assets. It has three basic components:

- Confidentiality — Protecting sensitive information from unauthorised disclosure or intelligible interception.
- Integrity — Safeguarding the accuracy and completeness of information and computer software.
- Availability — Ensuring that information and vital services are available to users when required.

The corporate information security policy describes the principles upon which information security standards and operational guidelines are based. It does not attempt to provide specific implementation steps or instructions, but rather it provides guidance from which specific security measures and requirements are derived.

The Big Sell Job

Developing a corporate security policy document and setting individual policies requires the participation and support of stakeholders from across the organization, especially senior management and business unit managers. So often, the biggest obstacle in developing a security policy is convincing management that we actually need one and that it must be taken seriously. A security policy goes far beyond the simple idea of "keep the bad guys out"[1]. I was concerned that management just wanted me to develop the policy to meet the recommendations of the IT infrastructure review and not actually implement it. The arguments after all were, we don't have any intellectual property worth stealing, so why do we need to protect ourselves. I was determined to change this view. I was also concerned that we didn't have the equivalent of a Chief Security Officer (CSO) to champion the cause of security. CSO's are not commonplace even in industry [5]. In fact, we didn't even have a dedicated Chief Information Officer (CIO). This role was combined with the Chief Financial Officer (CFO). As you can see, internal IT was of very little importance to the overall running of the company. The IT Steering Committee did its best but some members were not from an IT background and many had conflicting views on how security should be managed. I knew for a fact that selling the need for information security was going to be difficult.

As a first step, I arranged a meeting with the IT Steering Committee where I presented the reasons for developing and implementing a security policy. My approach was to discuss the company's vulnerabilities against the four main

types of attacks namely, confidentiality, integrity, denial of availability and repudiation. The Steering Committee became extremely concerned after I listed various ways hackers could enter the corporate network as it is and the damage they could cause by compromising the confidentiality and integrity of information, sabotaging critical systems and even completely removing critical applications. At the conclusion of this meeting, I managed to secure the IT Steering Committee's support to develop a corporate security policy and map out an implementation plan including options, recommendations and costs.

I learned that the best way to sell security is to emphasise the financial implications or risks if systems were attacked. The value of information and processes should be known, the risks in the current environment analysed, so that an appropriate set of countermeasures can be implemented [2] .

I interviewed individual stakeholders and members of the IT Steering Committee and asked questions like:

- What are we trying to protect? Client Information?, Competition analysis?, Financial Information?
- What attacks do you think are likely?
- Where do you think we are vulnerable, if at all?
- What would be the impact if confidential information was compromised or stolen and released?
- What would be the impact if systems such as email and accounting were brought down for 1, 2 or 5 days or even indefinitely?
- How well could we recover from such scenarios?
- What do you think is a reasonable cost for security?

This is to determine what they think about security, the possibility of attack and what the impacts are to the business if attacks occurred. I ran through various scenarios involving all the company's systems and information. The answers I received generally reflected the fact that a denial of service attack could seriously cripple the company especially if key email and accounting systems were brought down. In addition to this, I learnt that we hadn't tested a full recovery of all our systems, only our accounting systems, due to a lack of servers. If we had to rebuild all our systems, there was no guarantee it would be possible. Stakeholders were convinced the company's knowledge database contained no sensitive information that could be compromised if there was an attack. I was quite surprised by this view considering that nobody in the company could honestly say they knew every scrap of information stored in the knowledge database. I know from personal experience that, due to cost cutting in the IT department, the knowledge database was not regularly maintained and had, in fact, become a "black hole". If the confidentiality and integrity of the knowledge database was compromised, the potential impact could be significant especially if client confidential information became available.

In light of this, I decided to proceed with a top down approach of defining what needs to be protected, what are the threats and risks of an attack, what are the impacts and consequences and how can we protect ourselves.

Establishing the Company's Risk Profile

Security is typically based on some form of risk assessment. There are various methods of deriving risk, usually based on a combination of likelihood and consequence or impact information ie. How likely is a particular threat and what damage could be done if that threat was realised? Many organisations do not realise that risk assessment is a very important of the information security process. Too often, risk assessment is sacrificed as organisations try and quickly develop a corporate security policy to appease auditors and their shareholders. As many as a third of companies polled by PriceWaterHouseCoopers were found not to have conducted any risk analysis at all [4].

This is a difficult area with few objective methods of deriving a quantitative risk. What is essentially important is that management accept the chosen process and are prepared to support risk decisions based on that process, rather than being able to accurately predict probabilities and impacts. Traditional 'Risk Analysis' requires an assessment of both impact and probability for all the various threats and exposures that the company may be subject to. A major benefit of the application of Risk Analysis is that it brings a consistent and objective approach to all security reviews [3].

The approach I took is outlined below and was used to better understand the company's business requirements in terms of;

- the data that will be accessed
- the sensitivity of that data
- the environment the data will be accessed from

This information was then analysed to determine the appropriate security risk profile. A 'strawman' view was used to quickly establish broad requirements and further refined as more information became available.

Review of Data Sensitivity

Data sensitivity is based on the assessment of impact when there is a loss of data confidentiality, Integrity or non-repudiation. After determining the main types of company data, I interviewed the key stakeholders regarding their views of data sensitivity and summarised the findings in three separate tables according to the security criteria above. I found that each stakeholder had wide conflicting views of data sensitivity. For example, some stakeholders believed the loss of the knowledge database would have little or no impact on our earnings while others argued that the company's ability to be competitive in the market would be directly affected by the loss of the knowledge database. One thing that all stakeholders agreed on was the loss of the company's financial data would be a critical blow to the company.

The table format I used provided a qualitative measure of impact against the three security criteria above ie. an impact rating is assigned on a scale of 1 to 5 for a given item of data. In the following example, I interviewed the stakeholders regarding share-holding information for the company and the results were summarised in three tables corresponding to Confidentiality, Integrity and Non-Repudiation.

Table 1 below, provides an example of the results for loss of confidentiality.

Table 1: Impact if there is a loss of Confidentiality

	L		M		H		
	0	1	2	3	4	5	Score
Financial		✓					1
Legal / Regulatory		✓					1
Image / Reputation			✓				2
Competitive advantage			✓				2
Environment	✓						0
Human Safety	✓						0
					Highest Score		2=M

In the above example, the share-holding information scored an average 'Low' impact for confidentiality.

Once all the data types were rated, the information was categorised and summarised as per the example in Table 2 below and used to develop a risk profile for the company. The data item categories were C -Confidentiality, I-Integrity, NR - Non Repudiation.

Table 2: Data Sensitivity

Data Item	C	I	NR	Comments
Client Information				
Names	L	L	L	
Comment history	H	L	M	
Billing details	M	H	H	
Employee Information				
Payroll records	H	H	M	

Risk Profile

The risk profile for the company was developed using the data sensitivity analysis and assessing it against the levels of access such as physical, network, system, application and data. For example, if an area containing sensitive data is physically accessible from an unprotected location, it would

rank as a high risk environment. The table below shows an example of the risk profile that was developed for the company.

Table 3: Risk Profile

	Risk Characteristics by Access Layer					
	Physical	Network	System	Application	Function	Data
Significant and High Risk Env.	✓ (Data access terminal can be in any unprotected location)	✓ (Data is transmitted over open public networks using an insecure standard protocol)				✓ (Highly sensitive data accessible)
Moderate Risk Env.			✓ (Basic password authentication process only)	✓ (Basic password authentication process and application users defined)	✓ (Some restrictions on sensitive functions)	
Low Risk Env.						

In this example, the overall risk profile for the company was Medium/High. My company was expected to operate key information services containing highly sensitive data across insecure open networks. Only basic password based controls currently exist at the system and application levels to prevent unauthorised access.

By taking the time to properly develop the risk profile for the company and identify the potential serious security risks, I was now able to develop a security policy that would address the risks and exposures accordingly.

The Security Policy – Final Result

The corporate security policy was developed based on the risk characteristics of each access layer. So how did we go about developing the individual policies? The first issue revolves around the content and structure of the policies themselves: Are they complete? Are they fully up to date? Do they reflect your needs? This list of issues is extensive! [3]. As this was the first security policy for my company, I didn't have any templates to reference and form the policy structure, so I asked several colleagues who had previous experience in security policy development for templates and also searched my company's knowledge database, the Internet and the SANS library. I managed to receive sample security policy documents that were developed by my colleagues for their clients as well as a diverse selection of templates from the Internet and the SANS library. To ensure the security policy was of a high quality and adhered to standards, I reviewed a number of Government and Industry standards and guidelines as a potential base for the company's security policy. The key standards documents I referred to in the development of the corporate security policy were:

- Australian Standard for Information Security Management - AS/NZS 4444 (draft 99006),
- OGIT - Gatekeeper,
- Multimedia Victoria - IT Network and Application Security Best Practice Statements

The main topics that appeared in most of the templates were policy definition, objectives, owner and responsibility. As a result of this, I developed a suitable policy template that covered the key areas of:

- Policy definition,
- Objective of the policy,
- Potential benefits,
- Recommended actions and
- Policy owner.

An individual policy was developed for each risk/issue that was identified during the development of the company's risk profile and interviews with stakeholders. These individual policies were then structured and grouped according to the security access layer model as discussed above. For example, the policy for user access to the company's network was grouped under Network; and the policy for securing desktops and laptops on the premises was grouped under Physical. By grouping the policies this way, I found it most beneficial as it organised the policies according to the high level model of security within my organisation and also allowed me to logically reference the policies. One important fact I made very clear to all stakeholders was that the corporate security policy is a "living" document and as such individual policies are added and updated periodically according to a strict change control process.

In addition to the security policy document, I also developed a report detailing solutions and options to address the security risks and issues. This was a result of a request by the IT Steering Committee to better understand the security policy and its overall risks. I provided estimates for implementation and fully costed each solution and/or option in terms of capital costs, labour costs for implementation and ongoing maintenance costs. Some solutions were as simple as strengthening the password policy, while others were more complex and expensive such as a VPN which incorporated new hardware components and new software. The report was provided to stakeholders so that actions could be identified, prioritised and funded. I believed it was important to show some quick wins that could be achieved with little or no cost as well as the more expensive and strategic options.

The first draft of the security policy was reviewed by the IT Steering Committee and stakeholders in about 2 weeks. Most reviewers either had no comment to provide or provided minor changes but one or two tried to dilute the strength of individual policies by rewording them or simply trying to justify removing them altogether. I wasn't sure if this was because the security policy was covering areas they have jurisdiction over or it was possible they truly

believed the company had nothing to fear. I heavily argued against diluting any of the wording or removing specific policies unless the reasons were compelling, simply because this would jeopardise the meaning of the security policy and I was very serious about promoting the security policy throughout the company. I hoped most stakeholders got something useful out of the exercise and were now willing to support the new policy.

As mentioned previously, attached with the first draft of the security policy was a report that provided recommendations, options and estimated costs for addressing the security risks and issues. There seemed to be greater interest in this document than the security policy but that was to be expected as the company is driven purely by cost and revenue.

The one pleasing result was the IT Steering Committee was happy to recommend the endorsement of the security policy and recommended actions to the CEO and Board of Directors. The CEO and Board of Directors reviewed the security policy and endorsed it as a company-wide initiative. It was decided to initially implement all recommended solutions and actions that did not involve a substantial capital investment i.e under A$50K. Recommended solutions and actions involving capital and ongoing investment greater than A$50K would require a business case to be approved prior to commencement of work.

Overall, the result was very pleasing and more than I expected. The company saw the need for security and was willing to act. Part of this reason, I suspect is because of increasing focus on the company and its responsibility to shareholders. Whatever the reason, it also helped that executive management were able to review a high-level action plan and associated costs for implementation. It helped that they could plan for the implementation of security in stages and budget for it.

Conclusion

The road to completely securing a company's information is a long and difficult one. By far the most difficult step in this journey is convincing strong-willed executives that security is a big issue and not something to be taken lightly. As I pointed out time and again, information security may not directly determine if you make that big sale or your revenue targets will be met next year but it can protect you against revenue loss due to various attacks such as denial of service or confidentiality attack.

Developing the first security policy for your company can be daunting task. The corporate security policy sets the strategy for implementing individual security measures throughout the company ranging from new password access procedures and controls to setting up a PKI infrastructure or implementing new firewalls and intrusion detection software. Without the security policy in place and endorsed by the CEO and senior executives, the support of the organisation cannot be guaranteed and effective security measures cannot be put in place and maintained.

When developing a security policy, you must firstly identify and determine the company's risk profile. As I explained above, you cannot design an effective policy without knowing where your strengths and weaknesses lie. The risk profile should then determine how you develop individual policies and which areas to target. There is great source material on the Internet or in the SANS library on security policies and excellent templates can be found. I've found that it is better to design your own policy template rather than directly use a predefined one. This is simply because you can tailor it to suit your needs as I did. By researching a large cross-section of sample policies, you can obtain a good idea of what your security policy should look like and the type of content it should contain.

An excellent addition to the security policy is a report that details recommended solutions that will address the security issues and risks including a summary of the solution, how it will address the issues and the cost of implementing the solution. This will definitely help in the struggle to convince senior executives of the merits of a security policy and not just dismiss it as a piece of paper. Once the security policy has been endorsed, it's a good idea to start implementing security measures that require little or no cost and is not labour intensive. This ensures quick wins and visibility to executive management that the security policy is being implemented and followed. This is very important to ensure management backing and continue the momentum – "strike while the iron is hot" as they say.

In summary, it is relatively easy to develop a security policy. There are numerous case studies and policy templates available to assist with this. The tricky part is developing your company's risk profile and mapping the security policy to the risk profile. This has to be done correctly to achieve maximum benefit. It is also very useful to include a report detailing how you can implement the security policy and the costs associated with this. In this way, executive management can see a clear action plan for implementation and be able to plan and allocate funds as appropriate. This will hopefully assist you to win their confidence and backing. Without executive management endorsement, information security cannot be implemented effectively as you will have difficulty convincing others in the organisation to support you.

There are many hurdles to jump to reach your goal. Some are small and easily navigated while some are large and complex. Keep persevering and you will succeed. You need to remember the 3 key items to implement your security policy successfully:

- *Executive management endorsement* — Key to the whole process. Without this, you cannot move forward.
- *Stakeholder agreement and consultation* — Very important to involve all stakeholders and business units in order to develop an accurate risk profile of the company.
- *An effective action and implementation plan* — Important for others to know how security will be implemented and how it will affect them.

References

[1] Blacharski, Dan. "Emerging Technology: Create Order with a Strong Security Policy." September 2000.
URL: http://www.networkmagazine.com/article/NMG20000710S0015
[2] Boran Consulting. "IT Security Cookbook" October 2001.
URL: http://www.boran.com/security/
[3] Information Security Policy World. "The Benefits of: Security Risk Analysis". Copyright 1993-2002.
URL: http://www.information-security-policies-and-standards.com/benefits.htm
[4] Hulme, George V. "Security Policies: How Much is Enough?" September 3, 2001.
URL:http://www.informationweek.com/story/IWK20010830S002
[5] Hayes, Mary. "Impact Player." February 25, 2002.
URL:http://www.informationweek.com/story/IWK20020222S0002
[6] Hulme, George V. "Management Takes Notice." September 3, 2001.
URL:http://www.informationweek.com/story/IWK20010831S0014

Last Updated: October 2nd, 2013

Upcoming SANS Training

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

SANS Seattle 2013	Seattle, WAUS	Oct 07, 2013 - Oct 14, 2013	Live Event
SANS Baltimore 2013	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SEC760 Advanced Exploit Development for Penetration Testers	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SANS Bangalore 2013	Bangalore, IN	Oct 14, 2013 - Oct 26, 2013	Live Event
GridSecCon 2013	Jacksonville, FLUS	Oct 15, 2013 - Oct 17, 2013	Live Event
Healthcare Cyber Security Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 24, 2013	Live Event
Securing the Internet of Things Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 22, 2013	Live Event
SANS Tokyo Autumn 2013	Tokyo, JP	Oct 21, 2013 - Oct 26, 2013	Live Event
ICS410	Sterling, VAUS	Oct 21, 2013 - Oct 25, 2013	Live Event
October Singapore 2013	Singapore, SG	Oct 21, 2013 - Nov 02, 2013	Live Event
SANS Dubai 2013	Dubai, AE	Oct 26, 2013 - Nov 07, 2013	Live Event
FOR572 Advanced Network Forensics and Analysis	Washington, DCUS	Oct 28, 2013 - Nov 02, 2013	Live Event
SANS Chicago 2013	Chicago, ILUS	Oct 28, 2013 - Nov 02, 2013	Live Event
MGT415 at (ISC)2 SecureSoCal 2013	Manhattan Beach, CAUS	Oct 31, 2013 - Oct 31, 2013	Live Event
SANS South Florida 2013	Fort Lauderdale, FLUS	Nov 04, 2013 - Nov 09, 2013	Live Event
SANS DHS Continuous Diagnostics & Mitigation Award (CDM) Workshop	Washington, DCUS	Nov 06, 2013 - Nov 06, 2013	Live Event
MGT415 at (ISC)2 SecureDallas 2013	Dallas, TXUS	Nov 06, 2013 - Nov 06, 2013	Live Event
SANS Pen Test Hackfest Training Event and Summit	Washington, DCUS	Nov 07, 2013 - Nov 14, 2013	Live Event
SANS Sydney 2013	Sydney, AU	Nov 11, 2013 - Nov 23, 2013	Live Event
SANS Korea 2013	Seoul, KR	Nov 11, 2013 - Nov 23, 2013	Live Event
Cloud Security @ CLOUD Expo Asia	Singapore, SG	Nov 13, 2013 - Nov 15, 2013	Live Event
SANS London 2013	London, GB	Nov 16, 2013 - Nov 25, 2013	Live Event
SANS San Diego 2013	San Diego, CAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
FOR585 Adv Mobile Device Forensics	Vienna, VAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
Asia Pacific ICS Security Summit & Training	Singapore, SG	Dec 02, 2013 - Dec 08, 2013	Live Event
SANS San Antonio 2013	San Antonio, TXUS	Dec 03, 2013 - Dec 08, 2013	Live Event
SANS Cyber Defense Initiative 2013	Washington, DCUS	Dec 12, 2013 - Dec 19, 2013	Live Event
SANS Oman 2013	Muscat, OM	Dec 14, 2013 - Dec 19, 2013	Live Event
SANS Golden Gate 2013	San Francisco, CAUS	Dec 16, 2013 - Dec 21, 2013	Live Event
SANS Forensics Prague 2013	OnlineCZ	Oct 06, 2013 - Oct 13, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced