Global Information Assurance Certification Paper

The Role of the Security Administrator as a Security Advocate

Being a champion of security in a large organisation.

By
David Fosdike
GIAC Security Essentials Certificate Research Paper

September 23, 2004

Abstract

In a large organisation, security, particularly information security (IS), tends to have a low profile and an associated poor image. Most staff will only consider it cursorily when it impinges personally on them or on the work they do. The general feeling is that it is an expensive, intrusive but necessary evil. Senior management often see it as impost on the bottom line, users as a waste of time and something to be subverted. Even IT professionals see it as an afterthought when building, purchasing and managing systems.

The purpose of this paper is to outline some of the common problems in giving IS a positive reputation within an organisation. It will describe some of the reasoning as to why IS is necessary and some practical steps to help the Security Administrator (SA) to raise its profile. The paper will have a particular stress on the role of people in security management and show how the SA can address three general audiences within the organisation, Senior Management, IT Professionals and Computer Users[*].

'If it weren't for the users I could get my work done!'

The focus of this paper is on larger organisations where there are distinct groups and hierarchies of people with distinct jobs and where there may be geographical separation (e.g. a branch network). The dissemination of important information, regarding things like computer security, in such organisations is more complex than in a smaller organisation where everybody seems to know what is going on.

The IT equivalent of the old retail store adage, 'If it weren't for the customers I could my work done,' seems to fit well with many IT professionals who feel frustrated that people get in the way of the smooth running of their systems. This includes security professionals. We are brought back to reality, though, with the simple realisation that it is people we are working for. But as true as this is, the SA also requires the cooperation, and often the help, of other people in an organisation to get the job done.

This section could have been entitled 'Time for an attitude check.' SAs should remain positive about the people in an organisation and learn how to empower them to assist in the security solution. They also need to know how to persuade others, a sort of 'good social engineering', in order educate and coopt them into achieving their ends.

Kevin Mitnick has well summed up the human factor in security:

> Security is too often merely an illusion, an illusion sometimes made even worse when gullibility, naïveté, or ignorance come into play… In the end, social engineering attacks can succeed when people are stupid or, more commonly, simply ignorant about good security practices. With the same attitude as our security-conscious homeowner, many information technology (IT) professionals hold to the misconception that they've made

[*] Note: This paper is written in an Australian context but care has been taken to generalise the content to make it useful to security professionals everywhere.

> their companies largely immune to attack because they've deployed standard security products-firewalls, intrusion detection systems, or stronger authentication devices such as time-based tokens or biometric smart cards. Anyone who thinks that security products alone offer true security is settling for the illusion of security. It's a case of living in a world of fantasy: They will inevitably, later if not sooner, suffer a security incident.
> As noted security consultant Bruce Schneier puts it, "Security is not a product, it's a process." Moreover, security is not a technology problem- it's a people and management problem.
> As developers invent continually better security technologies, making it increasingly difficult to exploit technical vulnerabilities, attackers will turn more and more to exploiting the human element. Cracking the human firewall is often easy, requires no investment beyond the cost of a phone call, and involves minimal risk[1].

While people are a major problem in securing an organisation they are also often the key to getting the security job done.

Know Your Audience

Senior Management – includes the so-called CxOs:

- These people are *decision makers.* They are concerned with the organisation's mission and the policies and objectives needed to carry out that mission.
- They are concerned with *stakeholder outcome.* The stakeholders may vary from organisation to organisation. Whether they are shareholders (stockholders), government agencies or not-for-profit bodies it is still the bottom line that must end up in a favourable light. The senior management in this case need to see how security can enhance revenue or cut costs.
- Part of their role is to *minimise risk*. They are concerned with ensuring the longevity of the organisation and keeping it within proper regulatory and ethical standards.
- They have a responsibility to *maintain the public image of the organisation*. Failure to do this has been shown to negatively affect both profit and net worth.

IT Professionals

- Analysts and programmers are concerned taking raw information and presenting it to the organisation in understandable format.
- Administrators are concerned with maintaining the infrastructure on which information is collected, stored, transmitted and presented to the organisation in understandable format.
- Helpdesk staff help other staff in an organisation to use the systems.
- Support staff help the IT department to run smoothly by doing the administrative, clerical, training, and desktop support tasks among others.

Users.

- They are, by and large, *job focussed*. People who are satisfied with their work tend to focus on their role, their clients and the team of people they work with. The information they derive from the organisation's computer systems is merely a means to an end.
- They may be *not conscious of risk*. Computer systems are a tool to allow them to be productive; they need to know how to use a tool, not

necessarily how the tool works, but like any tool of trade they need to know to how to maintain it to best effect.

Senior Management

The problem:

Security costs money. Security infrastructure costs money to set up and maintain. For any organisation this can be great deal of money. The security shopping list can be lengthy: firewalls, intrusion detection systems (IDS), disaster recovery warm sites, anti-virus software, anti-spam software and public key infrastructure (PKI) and so on. For a large organisation the cost may well be multiplied as it may require redundant firewalls with multiple feeds from the Internet, multiple IDS with management software, warm recovery sites may be required to become hot recovery sites, anti-virus and anti-spam software may need extra management and PKI may have to be rolled out into many more scenarios. Senior management must know that money is necessarily and responsibly spent.

Spending on security must to be directed at actual requirements. The SA needs to help decision makers to know how much to spend. The CSI/FBI Computer Crime and Security Survey in the US or the Australian Computer Crime and Security Survey have various charts which may help to determine the amount of spending that may be expected to be available for security spending. Whether or not security will actually get the money may depend how well the SA communicate the requirements. As a guide the chart in Figure 1 on p. 4 shows that only 23% of (US) organisations spend more than 5 cents of every IT dollar on security and more than 50% spend 2 cents or less. Where does the organisation fit? Figure 2 on p. 5 will help to see where the organisation fits by industry type.

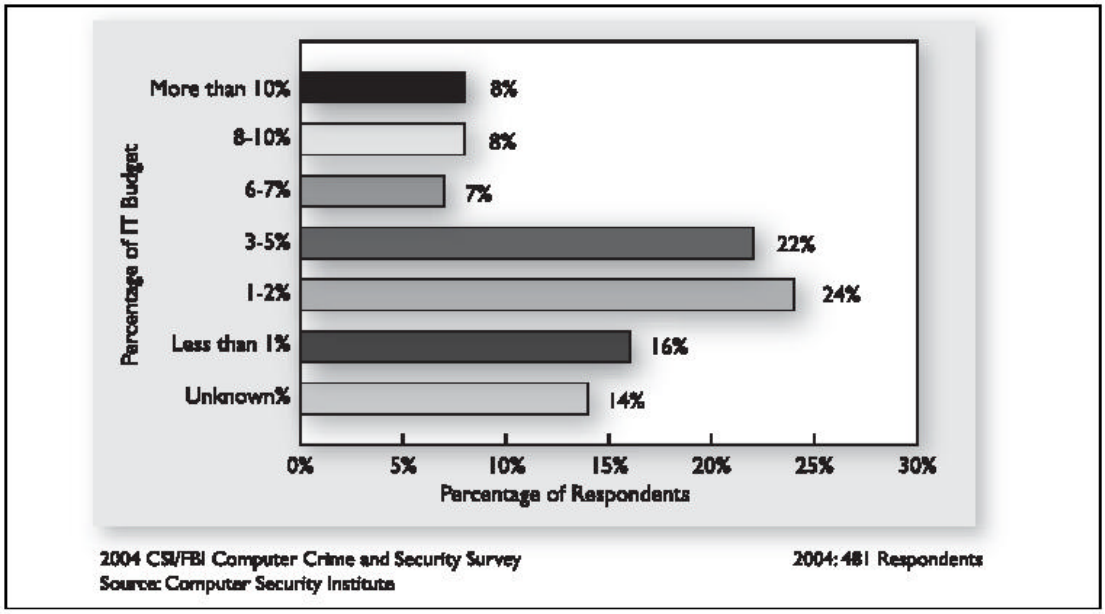

Figure 1.Percentage of IT Budget Spent on Security[2]

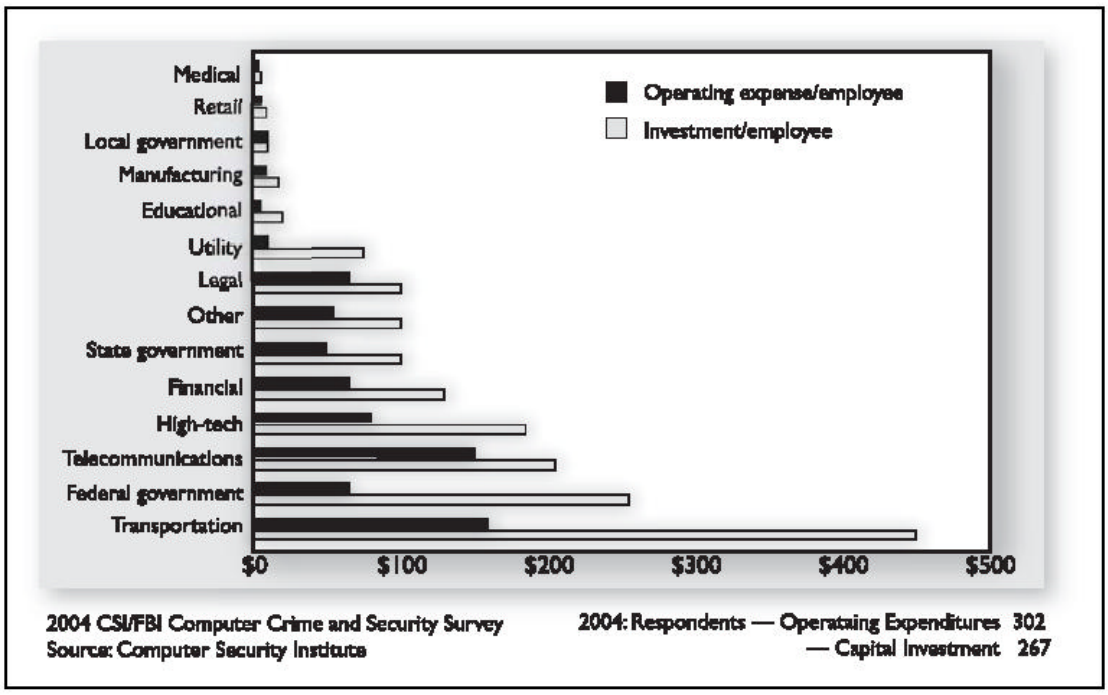

Figure 2. Relative expenditure on security per employee[3]

Senior management often perceive that *security has negative return on investment (ROI)*. One view is that security does not produce anything. Threats, generally, do not become reality with a frequency that brings alarm to company decision makers, and, not being on the frontline where the vulnerabilities are, they fail to see the continual attacks that, without the security procedures and infrastructure they have paid for, would become reality. The two things usually required to bring about a positive ROI, higher revenues and reducing costs, do not seem to apply to securing the organisational assets and wealth making ability. Senior management may also fail to grasp the internal risk. Sabotage, fraud and commercial espionage may all go unnoticed, affecting the fiscal outcome, if measures to detect them are not put in place. If measures are in place then such crimes are less likely to be perpetrated. Again there are hidden savings in the cost of security.

Why have security?

Risk Management. Any organisation must recognise the risks associated with carrying out its mission. The risks must be identified and analysed for likelihood, impact and cost. Controls, proportional to the risk need to be put in place. Risk management is not just about IT assets, (hardware, software, data, networks, etc.) but also about people. Protecting the physical, psychological and legal rights of personnel may have a direct effect on the overall morale of an organisation, which will in turn effect its performance.

Table 1 on p. 6 outlines some of the risks faced by an organisation connected to the Internet and their effects. Security administrators must determine the risks associated with their organisation and put forward proposals to deal with them.

Risk	Source	Technical Effect	Organisational Effect
Malware (Virus, worms, adware, spyware etc)	Usually external	Loss of usability of servers, computers and network. Possible loss of data.	Loss of ability to deal with clients. Downtime for clean-up.
Denial of Service attack	Usually external	Loss of connectivity. Loss of processing capability.	Loss of electronic connection with clients.
Fraud	Usually Internal – sometimes externally by former employees	Probably none.	Loss of funds, possibly leading to bad PR.
Espionage	Internal/External	Probably none although damage may be caused by a spy trying to cover their tracks.	Loss of Intellectual Property, code, trade secrets, client data etc. Loss of client privacy.
Sabotage/Vandalism	Internal	Loss of systems -computer or otherwise. Loss of data.	Loss of funds, loss of PR, personal injury or even fatality.
Spam (and other nuisance email)	External	Higher bandwidth required from Internet	Lost productivity from dealing with spam and its content.

Table 1. Risk Source and Effect.

The perception of the organisation may be diminished in the eyes of its stakeholders, clients, employees, law enforcement bodies and the general public by poor security practice. Having a website down or defaced can lead to this as can poor computer audit practices. Examples of defacement and bad public relations include the US Senate and FBI within days of each other[4], the Recording Industry Association of America[5] and even the Apache Software Foundation[6] who are generally acclaimed as being security conscious.

Cost due to breaches. There is a cost to repair damage due to poor security Will it be higher than the cost to protect against it?

Commercial espionage is a threat to an organisation's intellectual property. Intellectual property is at the core of many organisations today. If it is lost, stolen or tampered with, it may be the end of an organisation or in the case of Microsoft Corp. ,as reported recently, by the BBC, a big embarrassment:

> Microsoft has admitted that some of the source code for its widely used operating systems has been leaked on to the Internet. … Some of the core computer code for Microsoft's Windows NT 4 and Windows 2000 products has been found circulating online. The files are reportedly proving very popular on file-sharing networks such as Kazaa and chat nets such as IRC.
>
> …The leaked chunk contains library and text files, scripts, executable programs and raw computer code. …
>
> Why is this a problem for Microsoft?
>
> For several reasons.
>
> Firstly, it is yet another security lapse during a month that has seen the appearance of the fastest spreading virus ever as well as the discovery of yet another critical vulnerability in the Windows operating system.
>
> Secondly, Microsoft's growth has come about because of its tight control of its intellectual property - the source code of its products. This has helped it maintain a stranglehold on the desktop computer market. That hold has been demonstrably loosened now. Rivals could use it to get a better idea of how Windows works and help them compete against Microsoft.

> Thirdly, it might be the last straw for people tired of the security headaches that Windows creates.
> Fourthly, for Microsoft to have this code paraded in public is hugely embarrassing. Not least because the code is littered with profanity and might show that many Microsoft programmers do not do a very good job[7].

Business facilitation. Without internal networks and connection to the Internet it is difficult to remain in business today. Good security practice protects and promotes such connectivity.

Raising the profile

Have a policy. The SA needs to work out, with the business, a policy for information security for the organisation. The policy must to take into account the types of data used by the organisation, the type of business it conducts and how it interfaces with the rest of the world. It needs to consider the entire perimeter of the organisation – hosts, routers, modems, the Internet, physical borders and people. It has to consider how to deal with known threats and vulnerabilities. It must define valid access policies to data and hosts and punitive measures for breaching these policies. A good starting point for the policy is an IS policy standard such as ISO17799[*].

Have a plan. Nothing is harder to do than go to a senior decision maker in an organisation asking for money with no plan. A plan should include an objective of what is to be achieved, a cost-benefit analysis, implementation schedule and an accurate as possible costing.

Use language and methodologies understood by the audience. Avoid technical jargon by communicating in ordinary language, using examples and analogy where necessary. Telling a COO that the 'main DNS server is undergoing a DDoS attack which in turn means that other organisations cannot resolve the IP of our HTTP servers and therefore B2B traffic is not flowing,' does not help the much. What the COO wants to know is, 'that due to illegal activity on the Internet directed at our organisation we are unable to do business with our partners.' The COO may want further explanation and how the problem can be solved, but now does not feel intimidated. Use a technical glossary like the ones at http://www.microsoft.com/atwork/glossary.mspx and http://www.investorwords.com/ to help choose the right words.

One method that may be effective for a non-technical audience is the use of a diagram to get a point over. For example a 'Risk Analysis Matrix' may be useful. Perhaps a more useful way of expressing risk is to use a modified growth-risk matrix as in Figure 3 on page 8. This can be used to show a non-technical person the risk associated with a given threat or vulnerability and its likelihood of happening in comparison with known threats. Senior

[*] ISO17799 may be purchased from http://www.iso17799.net/ or the Australian/New Zealand equivalent AS/NZS 7799.2:2003 from http://www.standards.com.au/Catalogue/Script/Details.asp?DocN=AS956629867290

management may be aware of viruses, for instance, but not aware of threat to the mainframe via the 'backdoor'. Using a chart similar to this will help them to measure unknown threats in terms of existing ones. Extra emphasis can be added by using spots of different sizes to indicate effort required to fix the problem.

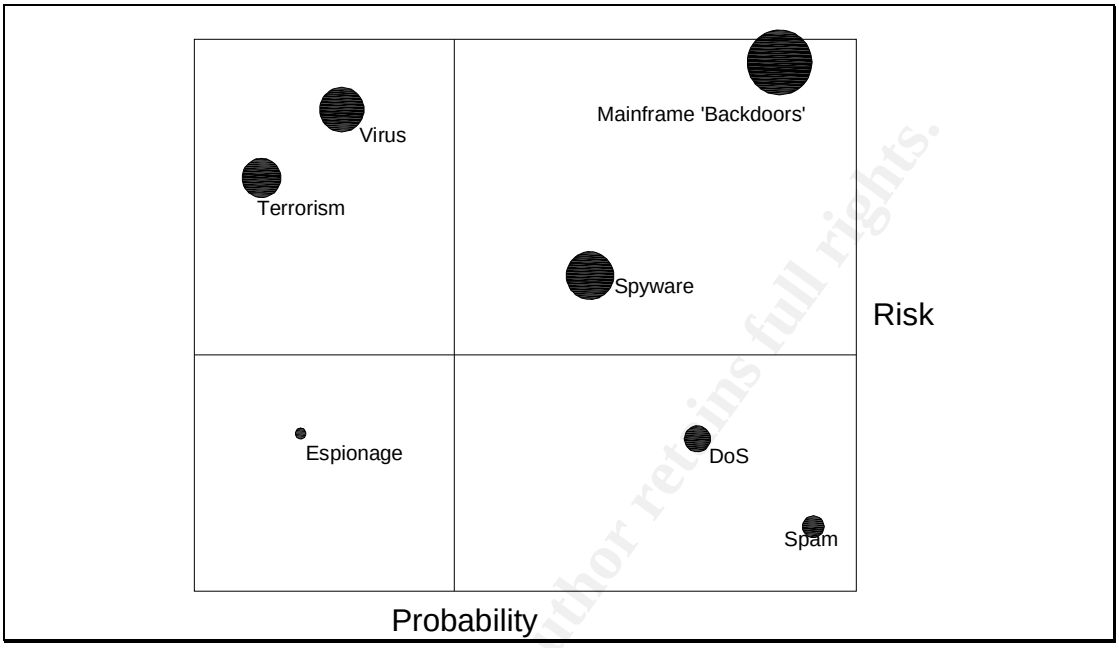

Figure 3. Probability-Risk Matrix

Using this will help a member of senior management see in familiar terms how risks in an organisation compare with one another. It can be used to go from a known risk, perhaps one an organisation has been through, for example a virus attack, and compare it to some other risk, which the SA needs resources to target. The matrix may be further modified by making the cost of risk mitigation proportional to the size of the 'risk spot' on the diagram.

Don't give up. If a request is dismissed, rework it, find an alternative or include it as a part of some other project. Often a good security idea rejected today will tomorrow become the pre-requisite of a project that comes out of some other part of the organisation. For example, it is evident that the firewall needs upgrading. It is getting difficult to manage and cannot handle the bandwidth the organisation uses for browsing and email. Senior management does not see this as critical and rejects the request for an upgrade. Two months later the purchasing department finds they can cut costs and get better discounts from suppliers by using the Internet for their ordering and invoicing. At this stage the SA modifies the proposal to include it as a requirement for the purchasing project. It is easily accepted.

Avoid FUD and don't 'fire from the hip'. FUD, short for fear, uncertainty and doubt, is a mechanism used, or perhaps abused, by vendors and consultants in selling security solutions. A rational, well thought out presentation of a risk and its solution, conservatively costed with a realistic implementation plan is more likely to be accepted by corporate decision makers than hurried, inappropriate or nebulous proposals. Even if a proposal is not accepted, the professional standing of a security administrator will be enhanced and will be more likely to be listened to again. See quote above on 'Managing Fear' by Daintry Duffy in CSO Magazine.

MANAGING FEAR

When all else fails to secure funding for security—and much of the time, all else does fail—it's not uncommon for the desperate to resort to spreading fear, uncertainty and doubt (FUD) about security threats in order to get your attention, and your budget dollars.

It is not done blatantly nor proudly, but it is done. One CSO admitted to walking into the boss's office and stealing a file, then locking the computer down with a password-protected screen saver so that the boss couldn't access his own system. The goal was to scare the boss into understanding the security risks he posed, and, to an extent, it worked.

In the long run, though, FUD does more damage than good. It creates a cry-wolf atmosphere and sets up a dysfunctional relationship between the security team and the other executives, who will grow to view the CSO suspiciously at best, and at worst, dismissively[8].

Follow correct procedures. There may also be formal requirements, such as a 'Capital Expense Request' in the organisation to get the money needed to achieve security objectives. Find what the procedures are and use them. In general senior management will frown on 'rogue' proposals. Following correct procedures shows professional integrity.

Use real-world examples. Find out what the organisation's peers or opposition are doing and make it known. Often the question then comes, 'What are we doing in that area?' This is now an opportunity to a vision for what could be done within the organisation. Use industry reports (available from consulting corporations like Gartner, Forrester, etc., most of the large audit companies and law enforcement bodies) indicating what others are spending on security and to keep up with industry trends.

Use a *professional approach*. This includes not only a knowledge of security but also knowledge of the organisation and what the implications are should threats against it be realised. Have an *integrated approach* – don't be isolated from the rest of the organisation.

BUSINESS INITIATIVES AND DEMAND

Maintaining a competitive market position in any industry depends upon an organization's ability to launch new business initiatives on a regular basis. These initiatives tend to focus on revenue-enhancing objectives such as increased customer satisfaction, greater workforce productivity, better supplier and partner integration, and more cost-effective back office operations. Launching these initiatives, however, requires a strong Internet-based infrastructure that extends the enterprise perimeter, allows many different classes of users to access the enterprise network, and places valuable enter- prise information assets at risk. Because launching these initiatives is a major business priority, developing the necessary IT infrastructure requires building up the appropriate security capabilities[9].

Use security as a facilitator. In the current Internet environment an organisation needs the infrastructure to allow the unrestrained but secure transfer of information with other organisations. It must allow for the confidentiality, integrity and availability of its own and its partners' data. Not enhancing a secure infrastructure and, for example, investing the amount that would have been spent on it, would have an opportunity cost[*] associated with it. Such a cost would be the sum of the losses incurred through poor security and the lost revenue or cost savings of further opportunities the infrastructure would have provided offset by the revenue derived from the investment. See comment above by the consultancy group PricewaterhouseCoopers on 'Business Initiatives and Demand'.

For example, the SA may propose that the organisation needs to spend $200,000 on security to last over five years. Management decides, instead, to spend the money on an advertising campaign. The campaign brings in extra sales with a net value of $450,000 (this includes the cost of the campaign). However, over the next five years the company:

- loses $150,000 in downtime due to a DoS attack,
- foregoes a discount of $135,000 by not being able to place orders and receive invoices electronically,
- is sued, successfully, by one of its employees who on the basis that they were morally outraged by images that appeared in spam and on colleagues web sessions: total cost $230,000
- has a client database stolen and published on the Internet which results in a net revenue loss to its competitors of $420,000.

	$150,000.00
	$135,000.00
	$230,000.00
	$420,000.00
	($450,000.00)
The opportunity cost in this case would be→	$485,000.00

An emerging opportunity to save costs is coming as more organisations become compliant with internationally recognised standards such as ISO17799. Such organisations may receive favourable treatment from insurers by having to pay lower premiums when covering their organisation

[*] Definition of 'opportunity cost':
The cost of passing up the next best choice when making a decision. For example, if an asset such as capital is used for one purpose, the opportunity cost is the value of the next best purpose the asset could have been used for. Opportunity cost analysis is an important part of a company's decision-making processes, but is not treated as an actual cost in any financial statement.
Source URL:http://www.investorwords.com/3470/opportunity_cost.html

against threats to information systems. Current trends in insuring against external threat are covered in the CSI/FBI Computer Crime and Security Survey[10]. There is the possibility, too, that third-party organisations offering services will do so at a discount when connecting to compliant entities. Compliant organisation will be able to do e-business more economically.

Make sure senior management is aware there are statutory requirements that they may need to adhere to. These will vary as to where the organisation is in the world but here are some as a starting point:

Requirement	Covers
Audit requirements	Independent review of processes, manual and IT as well as financial records etc.
Where to get help: Internal Auditors, External Auditors, Professional Audit bodies in your country, e.g.The Information Systems Audit and Control Association (ISACA) or The Institute of Internal Auditors (IIA) or in Australia, the Institute of Chartered Accountants in Australia (ICAA)	
HIPAA	Healthcare Privacy - US
Where to get help: http://aspe.hhs.gov/admnsimp/index.shtml	
Sarbanes-Oxley	Corporate governance regulations for the prevention and reporting of corporate fraud in the US or in US companies.
Where to get help: http://thomas.loc.gov/cgibin/cpquery/R?cp107:FLD010:@1(hr610 http://www.plainlanguage.gov/hotstuff/govtbriefs2002.htm	
Gramm-Leach-Bliley Act (GLBA)	Financial services client privacy US
Where to get help: http://www.ftc.gov/privacy/glbact/	
Privacy Regulations	Legal rights of clients and employees
HR and Legal departments. US: http://www.usdoj.gov/04foia/privstat.htm Australia: Privacy Act 1988 http://www.privacy.gov.au/act/	
Common law	Acts of theft, fraud, trespass and other criminal acts. In some jurisdictions also covers breach of contact and some other civil matters.
Where to get help: Legal departments, government agencies, Police, FBI etc.	
Employee Rights	Legal rights of employees, occupational health and safety issues.
Where to get help: HR and Legal departments – Government labour relations departments.	
Shareholder Rights	Legal rights of shareholders and other investors.
Legal Department. Stock or Share Exchanges. Govt. agencies: SEC in US, ASIC in Australia etc.	
Fiduciary Duty	Legal requirements of management committed with a trust on behalf the organisation. (E.g. Board members may have entrusted to them the final responsibility for IS. The SA acts under their authority.)
Legal Department. Govt. agencies: SEC in US, ASIC in Australia etc. Law enforcement bodies.	

The events of September 11, 2000 brought the whole area of *Disaster Recovery Planning* (DRP), sometimes referred to as *Business Recovery Planning* (BRP) to a head. Human nature means that a trigger like September 11 will have lesser effect as the event fades in people's minds. Part of the

duty of a security professional is to help keep DRP in the minds of an organisation's leaders in order to keep funding and planning for this aspect.

IT Professionals

The problem:

There is a belief that *security risk is overstated*. How many times have we heard "We already have a firewall! Isn't that enough?" Because security breaches that cause visible problems occur infrequently it is easy to say there is no problem. Those who look after systems, whether software or hardware, assume their systems are safe because they have never seen an attack.

There is a belief that *security takes unrewarded effort*. There are many tasks involved with implementing, testing and maintaining systems and security often takes a backseat. Deadlines imposed by project leaders or management may mean that important security implementation and testing will be put aside until a system is in production, or more likely never at all.

There is a belief that *security interferes with the final outcome*. Security imposes restrictions on any solution. How a solution is implemented in the 'back end' will impose requirements for secure coding (see comment below by Marcus Ranum), audit controls, backup and restore procedures, server hardening, etc. The thought can be, 'If the users can't see it, it doesn't really matter. They have their functionality. That's all that counts.' The 'front end', where the users will interface with the system, needs to be slick and easy to use. Security requirements such as entering or re-entering passwords may be seen as not user-friendly and therefore avoided by system implementers.

MARCUS J. RANUM, Senior Scientist at TruSecure wrote recently:

Failing Miserably

It doesn't seem that a day goes by without someone announcing a critical flaw in some crucial piece of software or other. Is software that bad? Are programmers so inept? What the heck is going on, and why is the problem getting worse instead of better?

One distressing aspect of software security is that we fundamentally don't seem to "get it." In the 15 years I've been working the security beat, I have lost track of the number of times I've seen (and taught) tutorials on "how to write secure code" or read books on that topic. It's clear to me that we're:

• Trying to teach programmers how to write more secure code

• Failing miserably at the task

We're stuck in an endless loop on the education concept. We've been trying to educate programmers about writing secure code for at least a decade and it flat-out hasn't worked. While I'm the first to agree that beating one's head against the wall shows dedication, I am starting to wonder if we've chosen the wrong wall. What's Plan B[11]?

IT professionals working in customer service roles sometimes have a conflict too in maintaining security. For example, while wanting to help users with lost or expired passwords it may be felt that procedures to verify the users identity are intrusive or insensitive.

Other support staff also need to know the importance of security within IT. While they may not be accessing or designing access to sensitive information, they may be used in social engineering exploits to get to others who have that access. Trainers need to make the effort to know and disseminate security related information to users.

Why have security?

What is at stake here is similar to that outlined in the Senior Management section (see p 5) but at level closer to the actual assets which security processes seek to protect. Among other aspects *asset protection* and *defence in depth* are key area for IT professionals to consider.

Asset protection includes protecting the privacy of clients and other staff, protecting the organisation's reputation, its financial assets and its intellectual property.

Defence in depth is a concept that needs to be in the minds of all IT professionals, not just the SA. Many barriers need to be placed in the way of data losing their confidentiality, integrity or availability. Firewalls, IDS and accessibility to data through to backup and recovery and DRP implementation are all responsibilities usually undertaken by IT professionals.

Raising the profile

Promote the idea that implementation of security is part of *professional integrity*. As IT professionals they need to recognise that they have the protection, as well as the dissemination, of an organisation's data as part of their core role. Your encouragement as a fellow professional will be invaluable.

Promote *security in the System Development Life Cycle* (SDLC). As a SA become involved with how systems (hardware, network or software) are designed, purchased, enhanced, configured, tested and maintained. Your interest in these steps will mean not only do you know about the SDLC but also that others have your input.

> **What's Plan B**? I think that Plan B is largely a matter of doing a lot more work on our compiler and runtime environments, with a focus on making them embed more support for code quality and error checking. We've got to put it "below the radar screen" of the programmer's awareness, just as we did with compiler optimization, the creation of object code, and linking. We've done a great job building programming environments that produce fast executables without a lot of hand-holding from the programmer. In fact, most programmers today take optimization completely for granted—why not software security analysis and runtime security, too? For that matter, why are we still treating security as a separate problem from code quality? Insecure code is just buggy code![12]
> Marcus J. Ranum.

Have programmers regularly check for security bugs in the languages they use – they may find other bugs which when fixed will help them produce better solutions. If you have

the resources do the job of checking yourself and keep a register of bugs along with the risks they impose. See Appendix A for a list of useful URLS for programmers regarding secure programming. Consider changing computer language implementations to enforce secure programming. Marcus Ranum (see above: 'What's Plan B') backs this up, along with some other ideas that improve the security of code.

Show *security as an asset* that, if built-in, will give the organisation a higher profile with clients. Clients of your organisation need to have confidence that their privacy, and possibly their assets, are protected by the organisation's systems. Breach of trust through poor security can lead to an organisation's loss of reputation leading even to failure. The fraudulent activity that led to the recent failures of some high-profile companies could well have been caught had appropriate audit procedures been built into and maintained in their computer systems. Emphasise good implementation and coding practices to ensure cheaper maintenance.

Build some simple live examples of how buffer overflows work or how unsanitised input data can be used to gain access to a database. Show how easy it is to take over a host that has not been locked down. See http://www.arcert.gov.ar/webs/textos/SecureSoftware-01-10-01-FINAL.pdf or similar URLs to find examples of this kind of exploit.

With administrators don't takes side in the 'which OS is best argument'. The SA's job is not to run down the job of another but simply to improve security across the board. Encourage the use of best practice on each OS in your network.

Help helpdesk and support staff to recognise social engineering attacks and help them to understand what is at stake. Knowing that they are part of the defence-in-depth strategy will help the SA coopt their help in other areas.

Use some of the security budget to purchase books, manuals etc. to inform IT professionals. Subscribe to magazines, mailing lists and newsgroups that promote IT security. The aim: Get the message out there!

Table 2 on p. 15 shows some of the areas that a SA will need motivate and assist other IT professionals in.

Programmers	Administrators	Helpdesk	Support
▪ Sanitising data input ▪ Valid port ranges ▪ Buffer overflow attacks ▪ CGI ▪ Memory cleansing ▪ Cryptographic techniques	▪ Server Hardening ▪ Patch Management ▪ Network Hardening ▪ Protecting high profile account ▪ Auditing ▪ Forensics ▪ BU ▪ DRP ▪ Incident response	▪ Social Engineering ▪ Guarding against 'rogue' software ▪ Incident response	▪ Social Engineering ▪ Asset tracking ▪ Security training

Table 2. Areas of security concern for IT professionals.

Some IT departments have regular work in progress meetings. Use these as a forum without being overbearing. Choose a topic that is current and make a short presentation on it – use real examples if possible.

Computer Users

The problem:

There is a *divide between technical and non-technical staff*. The quote (opposite) from Kim Girard in CIO Magazine, reflects the change in attitude which SAs (and other IT professionals) must have toward ordinary users if they are get rid of some of the bigger problems in IS.

In general, users think*, 'Security is not my problem*.' Each user within an organisation has a role to fill. Each role may have many facets and in general computer or network security is not felt to be one of them. The SA is responsible for the entire perimeter of the network, and the users are part of that perimeter. It is part of their role to encourage users to have a conscience about security and do something to protect themselves.

> **Users JOIN THE BATTLE.** To gain control of the biggest nuisances, IT departments need to stop viewing workers as the enemy—and start recruiting them to be part of the solution.
>
> CIOs who send out e-mail warnings or updates to workers are fooling themselves because employees "will think it's some techy thing that they don't have to worry about," says Chris Belthoff, a senior security analyst at Sophos, a corporate provider of antispam and antivirus solutions.
>
> Belthoff advises that companies create a hands-on training program with employees to educate them about the dangers of spam and viruses. He says it's critical to show workers what spam e-mail subject lines look like so that they recognize them in their inboxes. Programs to train IT workers to be end user teachers are available…[13]

How much users are part of the problem is evident from the 2004 Australian Computer Crime and Security Survey. Figure 4 on p.16 indicates that 'changing personnel (users) attitudes and behaviour regarding computer security practices' has been the number one problem for three years running.

Figure 4. Problem number one - changing user attitudes[14].

Security gets in the way of doing my job. How often has it been heard, 'But I need this software!' – some 'harmless' utility downloaded from somewhere (who knows?) on the Internet. Such rogue software:

- is often not licensed. This leaves the organisation open to legal action by the owner of the software.
- may lack certification or other such verification if downloaded from the Internet. It may look genuine but who knows?
- may have required modification to security settings on the user's machine. For example, allowing non-secure ActiveX.
- could be a front for some kind of exploit used to gain access to the user's machine and data, for example, Trojan, spyware, virus etc.

@#$%^ Passwords! The problem is how to keep the user's environment safe while at the same time not adding an irksome task to their already heavy workload. Users will do almost any thing to rid themselves of having to remember a six or eight character string that must be changed every 30 days. They will write it down, make it easily guessable, use a sequence where one

password is derived from the last etc. Then some interfering SA at head office puts policies in place to say they are not allowed to do that. What are they going to do? In most cases, unless there are measures in place to verify compliance, they will continue to do the same.

Why have security?

Auditability. Users need security to protect their access rights to a network. In the case of a fraud committed against the organisation, if a user has allowed their user name and password to be used either wittingly or unwittingly by a third party, then the user may be held liable wholly or partly for the fraud.

Job Protection. Apart from the auditibility aspect, users need to consider that if the organisation fails their job fails. It is their favour to protect the organisation from illegal activity.

Social Engineering. One the main exploits used to get information from organisations is through its employees. Social engineering is the use of psychological techniques to obtain information or access to information. One of the main security perimeter elements of an organisation is its employees.

Raising the profile

Make life easier for users – this is very important if you want them to help you. For example, make virus and spyware signature update automatic and put in auditing to ensure that the automated process is working.

Advertise what is current in threats, what is being done to counter them and any benefits that flow to the organisation's staff.

- Antivirus Solutions. Keep systems clean, leading to minimal downtime, which in turn enhances job satisfaction.
- Antispam Systems. Spam wastes time and can be offensive. Make sure users know how to use the systems effectively (some work on feedback mechanisms).
- Phishing attacks. Tell users how to deal with these – especially never to use the links provided and give a mechanism for the user to report these.
- HTTP filtering. Sometimes these systems can be either overzealous or not up-to-date. Provide feedback mechanisms to report both false positives and false negatives. Make known the danger of threats that can come in via browsing (spyware etc.) and regulations regarding offensive material in the workplace.
- Explain the rationale behind locking screens, strong passwords, password privacy etc.
- Remind them: The continuity of their employment depends on the continuity of the organisation. If it fails because of poor security practice, their jobs are in jeopardy.

Passwords – provide practical help. Show them:

- How they protect the user and the organisation.

- How to form a good one. See Appendix C.
- How to protect it. Don't write it down, don't share it etc.

Push for 3-factor authentication and single signon. These will make life easier and more secure for all.

THE TEN IMMUTABLE LAWS OF SECURITY

Law #1: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore

Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore

Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore

Law #4: If you allow a bad guy to upload programs to your website, it's not your website any more

Law #5: Weak passwords trump strong security

Law #6: A computer is only as secure as the administrator is trustworthy

Law #7: Encrypted data is only as secure as the decryption key

Law #8: An out of date virus scanner is only marginally better than no virus scanner at all

Law #9: Absolute anonymity isn't practical, in real life or on the Web

Law #10: Technology is not a panacea[15]

Explain the 'The Ten Immutable Laws of Security'. Make available some interesting material on security. Put together a package of material or a presentation based on the positive side of security. Don't run down your audience; show them what they can do and how it will benefit them. Use the fact that the majority of users will have a computer at home. Tailor a presentation (or a series) about what they can do to protect themselves in the home environment. Many of the principles will overflow into the work situation. Include topics such as:

- Preventing identity theft. Checking certificate validity etc.
- Antivirus, anti-spyware and antispam software configuration and maintenance.
- Personal firewall configuration.
- Browser configuration.
- Wireless network configuration.

Readers in your audience may enjoy books like 'The Art of Deception' by Kevin Mitnick or the 'The Cuckoo's Egg' by Cliff Stoll. Do a lunchtime screening of the film 'Sneakers' for anyone who is interested and point out what is realistic and what is not.

As with senior management, avoid being too technical in your presentations. Design an intranet page with security tips and up-to-date information for users.

Basically, use anything to get the message over.

Getting Help – know who your friends are

The SA is not alone in getting the security message over. Other departments within the organisation that can help are:

- *Legal*. The organisation's attorneys and lawyers can help keep the senior management up-to-date with regulatory requirements and can

help formulate policy as well as vet policy documents for accuracy from a legal point of view.

- *Human Resources (HR).* A thrust of this document is the human element in security. The organisation's HR department can help to disseminate information about security as well as promote training. Two other area where HR skills become important are the vetting of job applicants for security related attributes (police record etc.) and the counselling of staff in the case of breaches of policy.
- *Audit – Internal and External*. IT staff often see auditors as the enemy. On the contrary, a well conducted audit will reveal weaknesses and question countermeasures to bring to light how security can be strengthened, leaving the IT department with work to do. Once the work is done, IT will be seen in a more favourable light.

What the Security Professional needs to do.

Maintain a good knowledge of what is current in information security. Along with knowing the latest worms and viruses the SA should be reading books, whitepapers and magazines as well as participating in other forums, newsgroups and mailing lists in order to be aware of the changes and challenges for each of the groups addressed in this paper.

Be a conduit for best practice in your organisation. While SAs cannot be an expert in every field they need to know where to find security information and how to pass it on. Know what vendor offerings are available to solve problems.

10 Immutable Laws of Security Administration
Law #1: Nobody believes anything bad can happen to them, until it does
Law #2: Security only works if the secure way also happens to be the easy way
Law #3: If you don't keep up with security fixes, your network won't be yours for long
Law #4: It doesn't do much good to install security fixes on a computer that was never secured to begin with.
Law #5: Eternal vigilance is the price of security
Law #6: There really is someone out there trying to guess your passwords
Law #7: The most secure network is a well-administered one
Law #8: The difficulty of defending a network is directly proportional to its complexity
Law #9: Security isn't about risk avoidance; it's about risk management
Law #10: Technology is not a panacea[16]

Finally, *practice what you preach*.
Checklist:

- Become aware of the '10 Immutable Laws of Security Administration' by Scott Culp of Microsoft Corp. (see above).
- Lockout and Screensavers. Is your screen locked when you are away?
- Vulnerability assessment. Are you sure your firewall is safe?
- Do you have good password practice?
- Threat analysis. Do you know what is out there and how to protect against it?
- Laptop. Is it protected by passwords? Do you protect it physically?
- Backup. How long since you backed up critical scripts or other data?
- Coding practices. Is your code safe?

- Forensics. Are you ready to handle an incident?

Summary

The security administrator needs to bear in mind the many factors involved in the security process and the many parts of an organisations security perimeter. The SA must take an integrated approach looking at all tiers and groups of people in the organisation with SA at centre. Without such an approach the SA stands alone in the fight against threats from within and without. Getting the tools to do the job, the information to execute the security process effectively, and the cooperation of others to follow policy, will be an uphill battle unless everyone that can be involved is involved.

The security administrator in a large organisation must champion the cause of security or risk being unable to complete the task.

Appendix A

Useful URLs for Programmers regarding secure programming:
Java:
http://www.securingjava.com/toc.html
http://www-106.ibm.com/developerworks/java/library/j-javaevol/javaevol.html
http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/java.html
http://java.sun.com/security/
http://java.sun.com/security/seccodeguide.html
http://www.microsoft.com/mscorp/java/
C/C++
http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/c-cpp.html
http://msdn.microsoft.com/VISUALC/default.aspx?pull=/library/en-us/dv_vstechart/html/vctchcompilersecuritychecksindepth.asp
And this one poses an interesting question…
http://research.microsoft.com/projects/SWSecInstitute/challenge-pl.htm
Perl
http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/perl.html
http://www.perl.org/
http://www.cpan.org/
http://www.perl.com/pub/a/2000/01/10PerlMyths.html
http://www.w3.org/Security/Faq/

Appendix B

System hardening.
http://www.microsoft.com/technet/security/topics/hardsys/default.mspx
http://csrc.nist.gov/
http://www.linux-sec.net/Harden/harden.gwif.html
http://www.redhat.com/docs/manuals/enterprise/RHEL-3-Manual/pdf/rhel-sg-en.pdf
http://www.freebsd-howto.com/ (not much here – BSD info seems to be light on)

Appendix C

'Do's and Don'ts' of password formation. This may vary depending on the organisation's platform mix.

Do:

- Use a password that is memorable - that way you won't have to write it down.
- Use numerals or special symbols in place of letters in more common words and vice versa in numeric sequences. For example 0 for O, Z for 2, 1 for I, @ for A.
- Use common words backward and include and add special characters.
- If you have trouble remembering, do not write your password down, instead find a sentence you can remember and use the initial letters and add numerals or special characters. A variation on this is to take a book that is permanently on your bookshelf, open randomly at a page and use the first or last line on the page for the initial letters – you could also use the page number as the numeric portion of the password. Bookmark the page and place the book back on the shelf. Should you forget it is simply a matter of going to the page you have bookmarked.

- Use an unusual foreign word and add numerals or special characters.

Don't:

- Use a common name - yours, your child's, your wife's, your football team's etc.
- Use your account name.
- Use a Date – in any format.
- Use common passwords – like the organisation's name or 'password' .
- Use keyboard sequences – like QWERTY, ASDFGH or FREDFRED or PLOPLOP etc.
- Mix case if some of the platforms on your network cannot tell the difference.
- Use the internal account passwords (or account names for that matter) for logging into external services or even the organisation's DMZ.

Examples:

- DavidF – Bad, D@V1Df - Good, D@@5Vi1d15 – Better
- 2004-09-22 – Bad, 2@@#+o9+zz - Good, 23_2@@#+o9+zz – Better
- Australia – Bad, @ustralia – good, @u5tra1i@_42 - Better

Table of References

[1] Mitnick, Kevin D. and Simon, William L. The Art of Deception: Controlling the Human Element of Security. Indianapolis, Wiley Publishing, Inc., 2002. p. 4

[2]Gordon, Lawrence A. et al."2004 CSI/FBI Computer Crime and Security Survey." FBI2004.pdf URL:http://www.gocsi.com/.(15 Sep. 2004.) p. 4

[3] Gordon, Lawrence A. et al p. 5

[4] Festa, Paul."Senate, FBI sites down on hack attacks." CNET News. May 28, 1999. URL:http://news.com.com/Senate,+FBI+sites+down+on+hack+attacks/2100-1023_3-226493.html.(September 20, 2004)

[5] Lyman,Jay. "RIAA Web Site Defaced, Taken Offline." NewsFactor Network. August 28, 2002. URL:http://www.newsfactor.com/perl/story/19227.html (September 20, 2004)

[6] Shankland, Stephen." Apache site defaced in 'embarrassing' hacker attack." CNET News. May 5, 2000.URL:http://news.com.com/2100-1001-240174.html?legacy=cnet.(September 20, 2004)

[7] BBC News UK, "Q&A: Microsoft source code leaked." 13 February, 2004URL:http://news.bbc.co.uk/1/hi/technology/3485545.stm. (September 20, 2004)

[8] Duffy, Daintry."6 Ways to Fend Off FUD."CSO Magazine Sept. 2003.URL:http://www.csoonline.com/read/091803/pay.html (September 20, 2004

[9] PricewaterhouseCoopers Global Technology Centre.Information Security: A Strategic Guide for Business.San Jose, PricewaterhouseCoopers Global Technology Centre. November 2003. p.15

[10] Gordon, Lawrence A. et al p. 7

[11] Ranum, Marcus J. "Security: The root of the problem", ACM Queue.Security Vol. 2. No. 4 - June 2004, URL:http://www.acmqueue.org/modules.php?name=Content&pa=printer_friendly&pid=160&page=1 (September 22, 2004)

[12] Ranum, Marcus J.

[13] Girard, Kim.," I.T. Security Management / Why You SHOULD Sweat the Small Stuff."CIO Magazine.March 15, 2004.URL:http://www.cio.com/archive/031504/security.html.(September 22, 2004)

[14] The Australian High Tech Crime Centre et al. "2004 Australian Computer Crime and Security Survey."2004ACCSS.pdf. URL: http://www.auscert.org.au/crimesurvey (September 20, 2004)p. 21

[15]Microsoft Corporation. "10 Immutable Laws of Security." URL:http://www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.mspx, (September 21, 2004)

[16]Culp, Scott.,Microsoft Corporation. "10 Immutable Laws of Security Administration." URL: http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx, (September 22, 2004)