Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

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

Information Security: Starting Out

Going from technical guru to Information Security Manager can be a bigger step than you might think. Taking on the role of IT Security Officer in an enterprise that treats information security as an IT problem can offer many challenges and many opportunities to learn. Each organisation is unique and identifying those approaches that do not work is an important step forward in the journey to an effective information security program.
This paper is focused on delivering some broad guidance to the newly appointed info...

Copyright SANS Institute
Author Retains Full Rights

AD

Information Security: Starting Out

GIAC (GSLC) Gold Certification

Author: Stewart James, stewart@stootles.com

Advisor: Tim Proffitt

Accepted: June 18th 2009

Abstract

Going from technical guru to Information Security Manager can be a bigger step than you might think. Taking on the role of IT Security Officer in an enterprise that treats information security as an IT problem can offer many challenges and many opportunities to learn. Each organisation is unique and identifying those approaches that do not work is an important step forward in the journey to an effective information security program.

This paper is focused on delivering some broad guidance to the newly appointed information security professional. A direct reflection of the author's experiences, it targets administrative areas that are often over looked by those with a strong technical only background.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

1. Introduction

You have been the de facto IT security officer and have been offered the official role of the IT Security Officer within the IT Department, the first formal information security role at the organisation. It genuinely feels like the hard work has paid off. Your knowledge of technical matters is well rounded and you feel the new job title will make your wisdom readily accepted. Now is not the time to be complacent. There is a probability that your technical knowledge and your ability to communicate with business leaders will be put to the test.

Making the transition from a technical role into an information security professional can be a challenging exercise. Doing this in an organisation not affected by regulations such as Sarbanes Oxley or the Gramm Leech Bliley acts can be both a blessing and a curse. Making sure you take advantage of the blessings will help make you a well-rounded information security professional. Your real world experience may just be the edge needed in your future.

Taking time to evaluate and document where you are and where you are going is important to a successful transition. Recognising where your company could improve is important. It will help you avoid getting side-tracked by matters which feel more interesting. Striving to continually review and improve the work you have accomplished is as important as the first attempt.

Developing an understanding of best practice is fundamental to understanding information security. It can also be a false sense of right. Best practice methodology does not mean a company will readily accept it. It may not even be suitable for your company.

Of all matters that can be hardest to accept when trying to change culture, the need for failure can be the most difficult. Failure should be considered a requirement for success. Even instigating or participating in matters that you feel will fail can be of significant benefit to an organisation. We all learn from our mistakes and sometimes even organisations need to go through that process of failure before they can move onto their next victory. (Ulmer, Sellnow, & Seeger, 2006)

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Perhaps your reporting line is within the infrastructure group. This will prove to be a strength and weakness, though ultimately provide the ideal situation for an up-and-comer in the information security field.

As part of the IT Department some frustrations are to be expected. Not considered senior enough for the business leaders to be too concerned about matters you raise, after all security is just an IT function. On the other hand, your direct exposure to the business is limited and this provides an excellent buffer while you work on any skills you may need to cultivate.

Outside of the financial and resource constraints, one of the significant challenges is people, both technical and non-technical. By not effectively communicating with people, they will be the common blocker to your initiatives.

Technical people will respond well to technical discussions and you will still need to cultivate and manage your relationships carefully. If the network engineers condemn your proposed network changes because they feel they were not fully consulted or heard, arguing to move ahead anyway will be difficult. Even if you feel your solution is simple, best, effective or mandatory, you will need to ensure that appropriate time has been spent with those technical folk who have to ultimately implement your solution.

Business focused people probably don't want to hear the precise details of how this technology can detect an attack through fingerprinting ICMP packets. They do want to know how it is a better fit for the organisation and carries a significant savings over the existing approach. Employees want to know how things will help them do their job and will not be eager when they see something as an obstacle to their work. Learning to identify the information the business needs to hear and in a manner devoid of technical terminology is pivotal to improving your organisations information security tone.

Developing strong people skills should not be underestimated. Your ultimate success will stem from your ability to create and manage positive relations. While working within the confines of the IT Department, you will need to create a strong sphere of influence (Nader, 2002). Convince people that your idea is a good idea because they

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

trust you and trust that your interpretation of your idea as being good is true, not because you hold senior authority over them.

There are many courses available to help improve your skills. This paper is intended to help point someone starting out in the right direction. It is a direct reflection of the author's experiences and would readily send to his younger self.

2. Starting Out

2.1. Information Security sans Regulations

The US has delivered several regulations over the last decade which has made information security the personal responsibility of a company's senior officers. Regulations such as Sarbanes Oxley or the Gramm Leech Bliley acts are two such examples. Not all countries have equivalent laws and not all companies will be accountable to those laws. Information security is still practiced at such companies. Without the assignment of information security accountabilities to the executive officers through regulations, the approach may be a little different.

There is a significant amount of information security material now available as a result of the effort the US has made to improve information security. Some information is partly reliant on the senior officers having a legislated requirement to perform due diligence and due care. For those of us not in the US we may not be able to cite any regulations that will get senior management's immediate attention.

The more traditional approach will be the primary method that you will use to gain favour for a project or process improvement. Return on investment and cost benefit analysis that show a positive return will be needed. There may be no personal liability for a company's senior officers to do the right thing. They need to see how it will benefit them or their company.

US based information security professionals need to do this too, however, the reduced legal liabilities lowers the costs per incident therefore reducing the total spend available to protect against that incident.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

You will also want to practice your elevator pitch. An elevator pitch can be a short spiel about your project that you can put to senior managers when opportunity knocks. (Nader, 2002) If you are able to get minds thinking about your project you are more likely to be invited to give more information.

Experience in delivering a strong business case without the aid of regulations will likely be a powerful skill as your career progresses. Even if you eventually work in an organisation where information security is mandated by regulation, your skill will be of benefit to the company and yourself. Your recommendations for security expenditure will be based on benefiting the company and not just security.

2.2. Focus on the journey

Security is a process (Schneier, 2000), a journey and not a destination. Focus on the way you will perpetually work to improve the security posture of your organisation. Setting goals and milestones along the way is important. However, you are unlikely to reach a point where you can say "I have arrived and have nothing else to do".

Create a vision of where you want to be going as this vision will help you measure your progress when prioritising your work. You will find as you accomplish one task, another will need to be added. Without a documented plan, it will be easy to become side-tracked with something that feels a little more exciting.

Gartner has excellent papers to help any Security Officer in establishing goals for a long term strategy. (Scholtz, Byrnes, & Heiser, Establish an Effective Information Security Program, Part 1: Structure and Content, 2005) See section "2.5 Develop a long term vision" below for a brief overview of what a vision document may contain.

2.3. Process improvement

Something which is known and accepted is the idea of constant process improvement. (Cazemier, Overbeck, & Peters, 1999) Implementing a process that would be seen as best practice is the goal and it does not need to be the first process that an organisation experiences. Permit what may be considered flawed processes to be delivered to the organisation, allowing subsequent review cycles to improve that process.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

The SANS 27000 implementation and management course demonstrates a clear example of administrators reviewing system logs. While the goal may be to strive for the best possible solution, trying to leap to best practice may be too far to travel in one step.

- Level 1
  - Administrators regularly review server logs
  - Periodically review logs from desktops in the domain
- Level 2
  - Centralised log aggregation
  - Administrators review logs from all systems periodically
  - System generates automatic reports
- Level 3
  - Commercial log analysis tool is in place
  - Logs from all systems analysed hourly
  - Analysis software performs event correlation with near real time alerts for anomalies.

(SANS, SANS 27000 Implementation & Management, 2009)

Allowing a process to mature with the organisation can be more effective. Once the organisation has formed a simple habit, it is easier to improve that habit in small ways over time. This is often more beneficial trying to get the organisation to develop a more in depth process up front. (Burns)

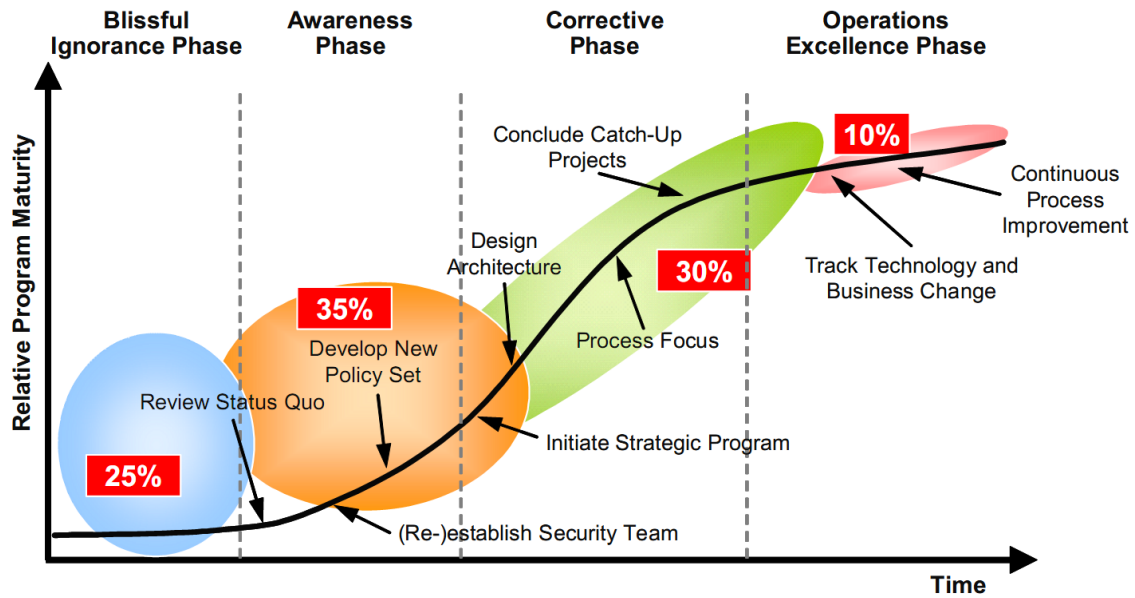
2.4. Identify where your journey is starting from

Take time to understand your current environment. Knowing the organisations current circumstances, strengths and weaknesses will help you in identifying what you should focus on and what should be in your long term vision.

While subjective in assessment, try and evaluate the organisations information security program maturity. (Byrnes & Scoltz, 2005) This will help you understand just what the organisation may need of you. If the organisation is already in the operations excellence phase, your need to lead the organisation is now a matter of review and

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

improve the existing processes. You should ensure you have a very good understanding of why the existing processes exist.



Note: Population distributions represent typical, large G2000-type organizations.

Source: (Byrnes & Scholtz, 2005)

If you have been elevated from a technical role into a new position of security officer, the organisation is more likely to be somewhere between "blissful ignorance" and "awareness" (Byrnes & Scholtz, 2005).

While working in an organisation that is operating in the blissful ignorance or even awareness band may be frustrating at times, the uncertainty of the organisation can be a significant benefit. It may mean that their definition of success is possibly limited and the business may be shielded from your early efforts. A failure in your attempt to implement a methodology, framework or process may not even be known by the organisations business leaders and you get to experience what doesn't work for the organisation or at least doesn't work right now.

Once the organisation starts to move on information security in a more serious manner, your buffer will quickly vanish. Be mindful of an increasing volume of pre-decision questions about a new product or service or requests from senior people for

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

advice on an upcoming policy that may not be technology focused. These will be indicators that information security is being considered in a more serious manner.

2.5. Develop a long term vision

The creation of a long term vision document will help you in assessing matters that require attention and in explaining to your superiors where you feel information security may be improved. "Establish an Effective Security Program, Part 1: Structure and Content" (Scholtz, Byrnes, & Heiser, 2005) is an excellent overview of what you might include in such documentation. This paper breaks a program into two streams: "strategic projects" and "controls and infrastructure projects".

Strategic projects:

- Information security architecture development
- Establishment of an awareness program
- Data/asset classifications
- Security policy redesign

Controls and infrastructure projects:

- Vulnerability management
- Patch management
- Identity infrastructure
- Secure remote access

The possibilities are almost endless. Each organisations culture will guide where energy may be best expended. On top of the small sample from Gartner above, you may also want to look for quick wins, centrally managed anti-virus for desktops or requiring all new hosts go through a vulnerability assessment. Be sure to include process improvement goals in this vision.

It is possible that a well laid out 5 year plan could take 10 years due to the organisation grappling with what it wants from information security. This can be an area of disappointment as another year rolls by and the security vision needs to be adjusted as only some things were completed.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

If you are constantly facing this problem, perhaps it is time to re-evaluate the methods you are using to deliver your message. This is one of the advantages of starting your career in an organisation that is not yet sure about information security. You are able to try different delivery methods and find what works with what sort of people (Shouse, 2007). This is not an indication of a failure on any individual's part; it is simply a learning process for you and the organisation.

2.6. Process improvement: Ninja style.

Your IT Department is possibly looking at something like the Information Technology Infrastructure Library (ITIL) framework to help align it to the organisational business needs. This type of program can have some fantastic advantages for you.

Change management and release management are excellent catalysts for improving the organisational security posture. They are also process development projects that don't need to come from the security officer. Once the IT department is heading down this road, leverage their needs to your advantage. A good example of this is the documentation surrounding a new system or service being released. Look at what the release management team requires and just add the information you are missing to do your job. (Kim, Love, & Spafford, 2008)

2.7. Best practice is not enough.

Immersion in understanding best practice is one of the first steps to understanding where an organisation may require improvement. This knowledge is extremely important for the new security officer as well as for knowing where to focus their energy. The number of frameworks and standards is vast: ITIL and COBIT (Service delivery framework), ISO27000 (Information Security Framework), COSO (Risk management framework).

This knowledge may give you the belief that your advice must be acted on, seeing as the basis of your advice is from a reputable source. Before the business is likely to act on your advice, they will probably want to know "How will that help achieve our

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

mission?" If you are unable to demonstrate clear benefits, the organisation is likely to ignore your advice.

The best way to deliver these standards and practices to a company, department or individual is to understand the business leaders (Covey, 1989). This will empower you to deliver the message in a format they understand, in a language they understand, and give concrete examples on what it really means to them. If you try to deliver a message in a format you find best for you, it will likely fail. (Shouse, 2007) Speak in a manner that the recipient prefers.

Be aware that best practice is only a guide. Some best practice may not be suitable at your organisation. You should be aiming to partner with the business to discover its needs and deliver a security program suitable to the company. Always be mindful that security needs must be measured against the needs of the company and sometimes a security practice is not suitable. Allow the business leaders to make the decisions about what is best for the company.

2.8. Accept Imperfection

Trying to deliver best practice in an area that the organisation has no practice (SANS, SANS 27000 Implementation & Management, 2009) can feel like an insurmountable challenge. The amount of effort it would take for the organisation to go from no practice to best practice is significant. If you attempt to deliver material that is demanding of best practice or nothing at all, people will fall on the side of "nothing at all".

Simplifying your requirements is probably one of the better approaches. If you require documented system architecture for the purpose of a security sign off, you may want to allow the documentation to be as simple as possible. It may miss important information and it may not suit your total needs.

By allowing the organisation to deliver simple documentation, you permit it to form a habit. If you require one page of documentation instead of ten, you are more likely

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

to get people to deliver that one page. After a year of developing this documentation you could add to it.

The importance here is to allow the process to mature as the organisation matures. Trying to force a group into what you consider a mature process will likely yield a high level of resistance. (SANS, SANS 27000 Implementation & Management, 2009) It may also put a negative value on your relationships with others in the organisation. By starting out with small requirements you are going to have a positive effect on those same relationships. They will more readily understand why that small requirement is important. It may even give you the chance to highlight why the requirement is important to their work.

While you have immersed yourself in information security, others have not. They may not have the time to focus on just the concepts of information security for a week. Your delivery of small requirements and then, small improvements can be considered a long term education program. Remember to use existing processes such as change, release and project management where possible.

2.9. Learning from failure

A foreign concept for many technical people is the idea of allowing failure. Although it can feel like a bad thing, it is a very important tool in some situations. Just like allowing a child to have small accidents to experience why something is not a good idea, you sometimes have to allow an adult or indeed a company do the same.

An organisation is full of people. Sometimes you need to allow people to experiment with their own ideas to see what works. Allowing people to experience failure can help them to understand why that approach is not suitable for the organisation. These experiences will help you in the long run as people remember past attempts and what didn't work.

You will need to permit all types of people to experiment with different options. As confident as you may feel that your information is correct, many people need to learn from experience. You also need to allow your theories to be examined. Your best

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

intentions may not be suitable for your company. Allow for this learning and reviewing in your estimation on how long to deliver a new process or product.

A brief example of permitting failure would be the way intrusion detection systems (IDS) may require more than one attempt to get right. It is not uncommon to win over management of why one is needed. Only to find the number of staff to manage the system is left at an effective zero and no additional resources in the operational staff pool to investigate relevant information from the IDS administrator. Never the less, moving forward with the IDS implementation may be the only way that you can prove that without human resources to manage the service and investigate alerts, the service will not be very effective. The benefit in the second round of attempting to implement an IDS is the business has seen for itself that an IDS without staff is not very effective.

2.10. Measuring your success

Managing your outcomes and your perceived workload is important. Others may see the wire framework you have in place as success and assume you can move onto other items. Your own measurement of success may need to be clearly communicated. A leveraged example of a successful Intrusion Detection System (IDS) is not when the solution is deployed into a production environment but when the information being generated by the system is being acted upon. Be sure to clearly communicate these requirements for success.

Documenting your idea of success up front is the ideal situation. Consider each area you are trying to improve as a micro project with documented milestones and progress reports as per your company's project management framework. Your supervisor should already be familiar with these progress reports and be able to identify when a project has been successful or not.

2.11. People, the new challenge

All the technical knowledge means very little if you are unable to communicate with different types of people in a manner that they understand. (Shouse, 2007) This is the biggest challenge a technical person can face in the shift from back room technical

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

guru to frontline business engagement. While you need to understand the technical detail of certain technologies, many non-technical people quickly lose interest with such detail.

These may not be exciting topics at first, immersing yourself in books on communication, business strategies and self-help books will be fundamental in building your communication skills. Understanding people will be the key to getting your message across (Shouse, 2007).

People can seem illogical. Books that document people in a more technical nature may be a worthwhile starting point. "How to spot a liar" discusses the human mind, its different thought processes and how the human body responds to stress. (Hartley, 2005) Other best sellers on the topic of self help books are well worth the read.

One of the better approaches that someone can use comes from the book "7 habits of highly effective people" (Covey, 1989). "First, seek to understand", people are more likely to listen to what you are saying when they feel you understand them and their issues. This can seem like the long road to success. You believe what you are trying to do is the best thing to do, why listen to someone? By listening to them you are taking their needs into account and they will know it. If you don't take this time you run the risk of people feeling you are just trying to make them do something that will not help them.

By developing good people management skills you will open more ears to your overall goals. People will be more likely to take what you say on board if you are able to make them feel that you are there for them. (Shouse, 2007) As a security officer you should be there for them, if the business stops so does your place in the organisation.

2.12. Governance without technology

An initial difficulty can be around the creation of policy that the IT operational group dislike. The issue is often around the "Security Guy" making up things without consideration of their needs. Delivering good principle based decisions can cause some staff to feel they are not trusted.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Rather than scuffle with operational staff, setup a governance structure that will allow principle based decisions to be made. A great resource in for this can be found in AS13335/ISO13335 (Australia, 2003)

Two forums should be created. One is a business focused, principle based policy group (SANS, SANS 27000 Implementation & Management, 2009). They will be focused on high level matters such as username standards, separation of duties and mandating the use of resources such as the centre for internet security. (CIS) This forum is an excellent opportunity for you to practice avoiding technical discussions. Initial members should be senior managers within the IT Department.

One of the biggest challenges for a technical group is to not talk about technology. This forum will need to avoid technical debate as the focus should be on the concepts. Where they need to understand the impact of a decision on technology they should refer it to the technical forum, which will be discussed shortly.

Try and identify someone senior within the IT department that is not technology focused. Even if they will not be a long term member, ask them to chair the meetings. They can identify when discussions are too technical and bring the conversation back to a non-technical focal point. It is possible that many members will need to practice not talking about the technical issues of a policy decision.

The goal of this forum is to allow IT managers to take ownership of policy. If they have had a chance to participate in the decision process they are more likely to enforce the policies (SANS, SANS 27000 Implementation & Management, 2009).

Once the forum is working, which may take some time and several revisions, you can consider inviting business leaders to sit in. By demonstrating a working forum you are more likely to get some interest from them. A track record of issues being discussed and decided on will help them find interest. You may even discover some people asking about participating when they see the forum working and having an impact on their area.

The second forum is a technical forum (Australia, 2003). This should be charged with deciding technical issues and policies (SANS, SANS 27000 Implementation & Management, 2009). It may include such things as whether internal only hosts should be

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

given private IP addresses, be protected by a firewall, or how security patches should be implemented. They may also be required to give information to the business forum. Some examples would be: what is a good minimum password complexity or what is the impact of enforcing existing password requriements.

Finding a good chair for this forum is also important. The chair should have enough understanding of technology to know if the discussion has gone off topic and also be able to withhold their personal opinion as to remain impartial. Expect many strong debates from this group as they strive to understand that what they have always done is no longer considered acceptable.

2.13. Increasing your organisational authority

As your abilities as a business leader develop you may be faced with some frustration. Your position and duties may be seen by others as just being an infrastructure or IT problem. Hopefully you have been using this to your advantage, focusing on building your skills in information security and people management.

Once you feel that your contribution to the organisation is held back by your organisational status and you are ready to take on more responsibility, it is time to put your case forward to be aligned to a more senior manager.

This can be a difficult proposition if your manager does not agree with your view. In this case, you will need to work with them to try and understand why they don't agree and see if you can get some level of mutual understanding. You will likely have to keep a working relationship with your manager after your realignment with the organisation. It will serve you little benefit to upset that relationship.

There are many options for where the information security role should reside. You may desire to leverage sources considered authoritative, the Gartner paper "Role Definition and Organizational Structure" (Scholtz, Role Definition and Organizational Structure: Security, 2006) is an excellent resource for understanding the different effect organisational positioning can have on information security.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Step lightly as you navigate this matter. Office politics exist, no matter how hard you try to ignore them they will be ever present. While you need to operate with the highest integrity at all times, you must be aware of them (Nader, 2002). If you are operating in the infrastructure branch of the IT department, consider trying to elevate to a position where you report directly to the IT Director, then the CIO with a final shift into the risk management area of your corporation.

The goal of this move is not to increase your pay. The reason for this shift is to improve the value you are able to give the organisation.

Altering your reporting line is a matter of demonstrating how your role in the organisation can better serve the organisation if reporting to a different area. This can simply be through the perception of others. While reporting to the infrastructure manager the development team may not see your role as concerning them. By reporting to the IT Director you can be seen a resource for both groups. Perhaps you already report to the IT Director which may have you labelled as an IT problem. Reporting to a CIO or into the risk management branch will help convey the message that information security is not just an IT problem.

Along the way you may identify a role you are in as being invaluable to the organisation. The additional challenge here is that you need to put a case forward for the current role to remain and a new role to be created.

If you are lucky your efforts along the way are noticed and your position is elevated by others above you. Perhaps the IT Director or Chief Information Officer has noticed your work and reorganises your role to report to them. If you are faced with this and don't feel you are ready, sit down and discuss what will be expected of you. There is every possibility you are under rating your abilities. There is a reason why a senior member has identified you as ready to have more organisational authority.

As you embark on your journey up the corporate ladder, keep in mind the higher you are the more your actions are exposed. A failure while reporting to the infrastructure manager is less visible than when reporting to the IT Director. Look out for those projects that are of high visibility and pay extra attention to them. You do not want to overlook a

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

minor matter that the CEO has an interest in. They could just be sizing you up for bigger things.

2.14. Your First Audit

Many people see auditors as people who will just find problems, regardless of what improvements you have made. They are often light on praise, which can leave you wondering if what you have been working on was worth your time. Even if they find issue with what you have been working on, as long as you have been making positives steps in the right direction, it has been worth your time.

Allow the auditors to carry out their role; their reports will often be given to senior executives. Use their findings to help fine tune your long term vision, depending on the frequency of audits and the size of the findings, try to resolve these matters before the next audit. They are a third party expert that can aid in identifying where security can be improved (SANS, SANS 27000 Implementation & Management, 2009).

If you have been working on improving organisational security by building small repetitive improvements, you are probably aware of the issues they raise. If they raise something you are not aware of, be thankful. For whatever reasons they have stated, they have identified a new issue. Add it to your knowledge and get on with resolving it.

Welcome an auditor as you would a penetration tester you have hired. By guiding them to areas you have concerns about they are able to take an independent view of the situation. If they feel there is a problem, their report to management may be just what you need to get some focus on that matter. Take time to mentor them on technology where required, not all auditors have a focus on technology. Helping them to understand your companies technologies can aide them in delivering relevant material in their reports.

Auditors have a thankless job. Their mission is to help organisations by finding areas of improvement. Too many people see them as a negative group that always seem to find problems and many think the same way about information security people.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

3. Conclusion

Through establishing definitive long term goals you are able to measure your eventual success on those initial ideals. It is rare that you will be able to deliver a framework that follows best practice, international standards and/or legal requirements on day one that will be followed by the organisation.

By focusing your energies on small iterative process improvements and avoiding single significant change approaches, you will find it easier to alter the corporate culture. This offers significant benefit in allowing you to improve your relationship skills while strengthening your understanding of the organisation's political landscape.

The benefits of not yet being considered an executive officer are substantial. The experiences you have in shaping your organisation's information security posture will assist you in the future. A luxury someone thrust into a position such as CSO is unlikely to have experienced.

By permitting failure as an acceptable temporary position in the journey to success, you will have gathered an understanding as to just what an organisation can deal with dependant on its maturity in regards to information security management. Your experiences will not guarantee zero failures with your next employer, they should be reduced.

4. About the Author

Stewart James has worked at a major educational institute for over 10 years, currently the network houses over 8000 desktops, 12 campuses and an endless parade of students. His career started off in a computer lab support role, through the ranks of Systems Programmers (unofficial security officer), Networks Group Security Officer and is currently the IT Security Officer.

Mistakes were made, lessons were learnt. These lessons have been put into this paper to try and help those who follow him. Technical guru to IT Management is a hard

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

road. People can be so unpredictable and difficult to understand that at times he was left wondering if perhaps managing a company's servers would be a simpler job.

This institute has enabled him to develop strong technical skills, but, also better people skills. He firmly believes people are the biggest hurdle to information security; especially in a tertiary education context where obvious improvements may not be possible when challenged with the concept of academic freedom.

His own challenges to raise information security awareness are ongoing, just like many other Security Officers.

5. References

Australia, S. (2003). *AS 13335.2 Information Technology - Guidelines for the management of IT Security part 2.* Standards Australis.

Burns, S. (n.d.). *Installing a new habit and breaking an old one*. Retrieved July 13, 2009, from Stephanie Burns: http://www.stephanieburns.com/articles/article06_habit.asp

Byrnes, C., & Scholtz, T. (2005). *Use Information Security Program maturity Timeline as an Analysis Tool.* Gartner.

Cazemier, J., Overbeck, P., & Peters, L. (1999). *Best Practice for Security Management (ITIL)*. The Stationary Office.

CIS. (n.d.). *Centre for Internet Security*. Retrieved from Centre for Internet Security: http://www.cisecurity.org

Covey, S. (1989). *The 7 habits of highly effective people.* FreePress.

Hartley, G. (2005). *How to Spot a Liar: Why People Don't Tell the Truth… And How You Can Catch Them.* Career Press.

Kim, G., Love, P., & Spafford, G. (2008). *Visible Ops Security*. IT Process Insititute.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Nader, J. C. (2002). *How to lose friends and infuriate your boss : take control of your career.* Plutonium.

SANS. (2009). SANS 27000 Implementation & Management. *SANS 27000 Implementation & Management : MGT411.* OnDemand: SANS.

SANS. (2003, April 1). *System Security Plan*. Retrieved 07 13, 2009, from SANS: http://www.sans.org/projects/systemsecurity.php

Scholtz, T. (2006). *Role Definition and Organizational Structure: Security.* Gartner.

Scholtz, T., Byrnes, C., & Heiser, J. (2005). *Establish an Effective Information Security Program, Part 1: Structure and Content.* Gartner.

Shouse, D. *Communicating like a Pro.*

Ulmer, R. R., Sellnow, T. L., & Seeger, M. W. (2006). *Effective Crisis Communication: Moving from Crisis to Opportunity.* Sage Publications, Inc.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

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

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