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.

# Selling Security To Management

One of the biggest complaints heard from security professionals is related to the fact that they feel that management does not understanding or properly appreciate the problems related to ensuring the security and privacy of their systems. As with all problems of this nature, this problem is the result of a failure to communicate with management. While I realize this is not your typical topic for a SANS discussion, it is important to our credibility as professionals because, if we cannot effectively communicate with th...

Copyright SANS Institute
Author Retains Full Rights

AD

**Selling Security To Management**
**Jeff Hall**
**GSEC Certification Practical Version 1.2e**

One of the biggest complaints heard from security professionals is related to the fact that they feel that management does not understanding or properly appreciate the problems related to ensuring the security and privacy of their systems. As with all problems of this nature, this problem is the result of a failure to communicate with management.

While I realize this is not your typical topic for a SANS discussion, it is important to our credibility as professionals because, if we cannot effectively communicate with those who control our success, then we will continue to be relegated to our present role in the organization. The better we are able to communicate our issues to management, the more likely it will be that management will respond positively to our issues.

This document will help you understand how to create presentations that will engage management and will discuss the common presentation pitfalls that befall technology people.

## Creating Great Presentations

Great presentations do not just occur; they are the culmination of a significant amount of work. If you do not plan, then your presentation will not deliver the message that you are trying to communicate.

### Planning

Planning of a presentation requires you to develop a topic to be presented. Barbara Minto wrote a seminal work on writing, thinking and problem solving logic in the mid-1980s entitled The Pyramid Principle. As a management consultant with one of the "Big 5", this book and a related, internally developed training class was required for anyone in a management position within the Firm. Unfortunately, Ms. Minto's book is no longer in print, but if you ever get a chance to obtain a copy, I would highly recommend that you take the opportunity to add it to your bookshelf.

Ms. Minto argues in her book that effective communication of ideas is constructed like a pyramid. At the tip of the pyramid is the message or theme to be communicated. Underneath the tip of pyramid are the details in support of the theme that create the foundation of the message being delivered. The further you go down from the tip, the more detail that is offered.

The Pyramid Principle goes on to discuss that the construct of a presentation can flow from top to bottom (summary of findings and recommendations and then a discussion of the details that support those findings and recommendations) or from bottom to top depending on the needs of the audience. For senior management presentations, the top to bottom approach is usually the best way to organize your document because it effectively provides an executive summary of your findings and recommendations and then allows for selective discussion regarding the details


© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

that support your findings and recommendations. A bottom to top approach is typically used in the development of tutorials or training materials where ideas or concepts build on one another.

The result of this process is a definition of your message or theme and an outline of the material you wish to present and the strategy you will use to present it.

Research and Analysis

Now that you have an outline, you need to give it substance by researching your subject and developing sound conclusions and recommendations.

The problem most people face with this process is that there is typically an over abundance of information, but you only have so much time in which to present. However, now is not the time to worry about quantity, now is the time to get all of the quality facts that you can find. Focusing all of this information is done in the next step when we will edit it based on the needs of your audience.

Using your outline from the previous step, gather together as much information related to your various points as possible. Make sure you gather information that may be contrary to your position, as you will need it for your analysis later in this step. The SANS GIAC practical assignment does an excellent job of describing the research effort.

Once you have gathered all of your information, perform your analysis for the development of conclusions and recommendations. Do not be surprised if you find that some of your preconceptions regarding the topic to be misguided.

Audience

The next step in the process is remembering to focus on WHO is your audience. During this step, we will determine how to "filter" all of the information you've gathered to this point.

A security professional's audience is typically going to be a group of business executives with titles such as Chief Executive Officer (CEO), President, Chief Financial Officer (CFO), Chief Operating Officer (COO), Chief Information Officer (CIO), Chief Marketing Officer (CMO) and the like. To help you understand your audience, the following provides a brief description of each position's responsibilities and potential influence on your presentation.

> CEO/President/General Manager – These people are responsible for the overall management of the company, division, subsidiary, etc. These people will have a varied background, but they typically come from the operations or finance areas and have shown a broad base of knowledge regarding the industry and the organization. Their focus will be on the big picture and they will rely on the other executives to provide their own perspective based on their area of expertise. Their interest will be in determining if the definition of the problem is appropriate, the analysis of the possible solutions are well thought out, and the recommendations make sense based on the analysis presented.


© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

CFO/VP of Finance/Division Controller – These people are responsible for the financial well being of the organization. To dispel a popular myth, they are not always just "bean counters" concerned with every last expenditure. These people are also responsible for ensuring that the controls of the systems (manual and automated) are adequate. As such, you should make sure that your presentation provides information regarding how your recommendations improve the control environment.

COO/VP Operations/VP Manufacturing/VP Distribution – These people are responsible for delivering the goods and services that your organization provides its customers and clients. Their primary focus is ensuring that the processes and procedures related to delivering goods and services are as efficient and effective as possible within the control environment. If you are recommending changes in policies and procedures, you will need to provide details on how those changes will either not impact operations or will improve other aspects of the operations of the organization.

CMO/VP Marketing/VP Sales – These types of people are responsible for selling the goods and services of your organization. Their focus will be on making sure that your recommendations are not going to adversely affect sales. If your recommendations affect only non-sales users, these people will likely go along with your recommendations. However, if your recommendations affect customers or the sales force (a secure VPN for example), then these people will want to minimize the impact or possibly will argue that your recommendations are too onerous and should not be implemented. You need to remember the impact your solutions may have on customers and remote users.

CIO/VP IS/Director IS – You should already have a good idea of this person's role in the organization and this person should be your champion during the presentation. It is important that this person review and comment on your presentation prior to the actual meeting. This person can add insight into the internal politics between the previously mentioned players and can help you adjust your language so that it plays better to the audience.

Mr. Lenny Laskowski has produced short document on how to focus this analysis. He has broken down the word audience as a memory aid.

A nalysis – Who are they? How many will there be?
U nderstanding – What is their knowledge of the subject?
D emographics – What is their age, sex, educational background?
I nterest – Why are they there? Who asked them to be there?
E nvironment – Where will I stand? Can they all see and hear me?
N eeds – What are their needs? What are your needs as the speaker?
C ustomized – What specific needs do you need to address?
E xpectations – What do they expect to learn or hear from you?

If you can answer these questions, you should have a good understanding of your audience and what they will expect from your presentation and how to filter your information to meet their expectations.


© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Create A Draft

At this point we now have identified and filtered the information that we want to use, but we still have not really created the presentation. Now is the time to put your thoughts together in PowerPoint, Word or whatever you use for your presentations. Using your outline, the information you have gathered and the information filters you have identified, you now need to actually develop the presentation. Forget about the amount of time you have to present, just get your thoughts on paper. We will edit the content after the draft is completed and has been reviewed.

If your organization has a standard presentation template, USE IT! Nothing helps you fit in than making your presentation look and feel like all other presentations created by your organization. If your organization does not have a standard template, Ms. Ann Agee of George Mason University has developed a set of rules for formatting a presentation.

- You should have no more than six to eight words per line.
- No more than six to eight lines or 50 words per slide.
- Use only two fonts throughout your presentation. Ms. Agee suggests a serif font like Times Roman for page titles and a san serif font like Ariel for the body of your presentation.
- Fonts should be no smaller than 24 point to ensure your slides are legible when projected.
- Use graphics to make a point or enhance your analysis, but be careful to balance your graphics on the page.
- Avoid special effects such as screen wipes and sounds. They will give the appearance that your presentation is more show than go.
- ALWAYS spell check your presentation. Not once, but every time you make changes – make sure you spell check it prior to finishing your PowerPoint session. In this day and age, there is no excuse for poor spell and grammar.

Edit For Time

Now that you have your draft created you can now edit it for the amount of time you have to present. A good rule of thumb is each slide takes one to two minutes to present. Also plan for questions either throughout your presentation or at the end of the presentation. Another good rule of thumb is 10 minutes of questions for every hour of presentation.

In the beginning, you will probably find this part of the process the hardest to deal with. After all, you have all of this good information, but you cannot share it all with your audience. If you find that you are having difficulty with the editing, save your presentation and walk away from it for a while. When you come back you will be amazed at how well you will be able to trim it down.

A Second Set Of Eyes


© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Another key to a great presentation is to get a second set of eyes to review your presentation. Your second set of eyes should not be your buddy in the cubicle next to you; you should get your mentor or their mentor to review your presentation. They can provide you further input regarding further clarification that may be required, further editing for time and the all-important editing for political correctness.

Practice

Now that you have a presentation, you need to get comfortable with it. It does not matter how you practice, but you need to practice. If you are not comfortable with public speaking, then you will want to have a lot of practice. The key is to practice until you are fully comfortable with the flow of the presentation and the information you are presenting.

## Technology Presentation Pitfalls

The following is a list of presentation pitfalls and potential solutions that I have accumulated over my 25+ years of management consulting. This is not a complete list, but I believe that it covers a significant number of the presentation sins that I personally have committed or have seen committed over the years.

1. Techno-babble and Acronyms

   There is nothing more uncomfortable to any audience than unfamiliar terms used in documents and presentations. The next most uncomfortable thing to an audience is a speaker who assumes that they should know the terminology. The key to avoiding this pitfall is to remember WHO your audience is and WHAT their comfort level is with the topic being discussed. If you are not sure about the audience's level of understanding, then take some time to explain the technology and the terminology. If necessary, include a Glossary Of Terms as an appendix to your presentation as a future reference.

2. Expert Myopia

   All subject matter experts suffer from "expert myopia". This is not a bad thing, but it is something that every person needs to be aware. Every person has some area of knowledge where they are the perceived experts and as that expert, they tend to be very focused on that topic and assume some level of understanding of their expertise from others. However, where things go awry is that we, the experts, typically assume a greater level of understanding because of questions or discussions with our audience. When answering questions in your area of expertise, take a step back and politely probe the audience's comfort level with the topic so that you can appropriately discuss the topic with the correct level of detail and background.

3. Failure To Practice


© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Very few people can just get up in front of a group and speak off the cuff. However, speaking extemporaneously is not what a professional does. A professional practices their speech over and over. These practice sessions can range from just repeatedly going over the presentation in their head to practicing their presentation in front of a mirror. The key to addressing this area is to find a method of practicing your discussion so that you are comfortable with your delivery and your gestures. The more comfortable you are, the more comfortable your audience will be during your presentation.

4. Forgetting Your Audience's "Hot Buttons"

There are reasons or "hot buttons" that has prompted management to request your presentation to them. As the expert, it is your job to make sure that you find out those reasons. Everyone has or should have a mentor that is higher up in the organization. Go to your mentor and find out the reasons for your presentation. If your mentor does not know the reasons, prompt them to go to their mentor for the reasons. Once you have the reasons for your presentation, take those reasons and incorporate them into your presentation. When giving your presentation, focus on those "hot buttons" by consistently tying your discussions to the "hot buttons".

5. Humor

Humor is a tough subject. Some people are good at telling a joke and some people are not. If you are one of those that cannot tell a joke well, then a presentation is not the place to inject humor. And it is definitely not the place for using humor if this is one of your first presentations. If you are going to use humor, make sure it is relevant to your topic and presentation, the humor is not off color and the humor does not embarrass the audience. Remember that like a stand up comic, sometimes the room is just tough and your humor may not solicit a laugh from your audience.

Hopefully this document has given you some ideas on how to improve your presentation skills and get your ideas across.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

**Bibliography**

Creating A Great Presentation, Anne Agee, September 1998,
http://www.irc.gmu.edu/scampbel/aagee/aagee.html

A.U.D.I.E.N.C.E. Analysis - It's Your Key To Success, Lenny Laskowski, 1996,
http://www.ljlseminars.com/audience.htm

Gathering Information & Materials, Lenny Laskowski, 1997,
http://www.ljlseminars.com/gather.htm

Speech Preparation As A Process, Lenny Laskowski, 1997,
http://www.ljlseminars.com/gather.htm

Elements Of An Effective Speech, Lenny Laskowski, 1997,
http://www.ljlseminars.com/elements.htm

Overcoming Speaking Anxiety In Meetings And Presentations, Lenny Laskowski, 1996,
http://www.ljlseminars.com/anxiety.htm

The Minto Pyramid Principle: Logic In Writing, Thinking and Problem Solving, Barbara Minto,
ISBN: 0960191046, May 1996

© SANS Institute 2001, Author retains full rights



© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 26th, 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** |