How to make
The “Perfect” P.B. & J.

Finding your Company’s Perfect Security

Charles W. Fullerton
CEH,OPST,CISSP,CSS1,CCNP,CCDA,CNA,A+
CEO, CISO, Lead Security Consultant
Fullerton Infosec, Inc.
www.fullertoninfosec.com

How to Build the "Perfect" P.B.&J.

Introduction

In today's post 9/11 world, cyber-security is taking on a new light. Companies and even Government agencies need to be compliant with new regulations, yet still ensure that their company is secure in the way it handles information. Each company will implement their security differently. With that in mind, how does each company implement their security differently yet still maintain compliance with the needed regulations? The answer to this question is that each company must find its "Perfect Security" standard.

Perfect Security is a customized standard that is a perfect fit for the company and the way it does business. Your company's current Security can then be tested against this Perfect Security standard to determine where the company's actual security posture stands compared to it. Numbers can be crunched within this process and a numerical level of your company's security can be computed.

A good example of this comes from the Open Source Security Testing Methodology Manual or OSSTMM. Its use of Risk Assessment Values, or RAV's, is an important part of the OSSTMM Security Test. You may review the latest version of the OSSTMM at www.isecom.org/osstmm.

The OSSTMM can also provide guidance, ensuring that you secure all aspects of your business. It not only covers IT security, but other areas, such as, communications, wireless, process security (or Social Engineering testing), information, and physical security as well.

Step One: Gather the Ingredients for Perfect Security… Mix Well

As you may have surmised, there are three main ingredients to this plan. The first, "P", stands for Policies. If you don't have a Security Policy that is well defined and in place, it is vital that one be established. It is your Policies that will protect you if, by chance, you become a litigant in a court case. Chances are you already have a number of policies that would be integral parts of your Security Policy in-place, thereby enabling you to create or modify a corporate Security Policy as a start.

The next ingredient, "B", stands for Best Practices. There are a number of Best Practice Methodologies and standards that can be utilized. Standards, like ISO 17799, which may meet the needs of some companies, can have portions that fulfill some of your requirements. Feel free to implement these portions into your Security Policy. If you are uncertain about which standard best suites your individual corporate needs, many

references are available on the Internet. You could also contact your local chapter of ISSA to request answers to questions you may have. Be sure to take the time to research what is best for your organization.

The final ingredient, "J", stands for Justifications, which is made up of three parts: Legal, Industry and Business.

Legal Justifications are the first part and **must** be adhered to. These are minimum standards that every business must comply with. Examples of Legal Justifications include HIPAA, GLBA, SOX, COPPA, GISRA, and many others. Your company's legal counsel should be consulted to see which justifications are required for your organization. One point to remember, compliance does not ensure effective corporate informational security.

Industry Justifications are the second part and while not legally mandated, are highly recommended. These are most commonly found in unregulated industries where many companies have adopted justifications in order to stem the tide of Government regulation. The pharmaceutical industry is a good example of this. While companies won't get fined if they choose not to follow the Industry Justifications, implementing them could minimize the impact of future regulations that may be imposed on the industry and it may boost the level of your security within the organization.

The final part is our Business Justifications. These are the items that must be in place in order to do business. Examples of this include having a local web server to allow the company to engage in e-commerce as well as an email server to help the company communicate within and with the outside world. Any implementation of this type of justification must comply with the Legal Justifications, and should comply with the Industry Justifications.

Once we have collected all of this information, we need to determine what is the Security goal for your organization and implement it into our dedicated security policy. As this can be rather tedious, it can help to import this information into your policy as you receive it. When this task has been completed you now have your first version of your organization's Perfect Security Policy.

Step Two: Taste Test it.

Now that we have defined your security policy based on your "Perfect Security", it's time to see how the rest of your business compares to your standard. As you begin the actual implementation of your new policy you will, almost assuredly, find faults within your infrastructure, and that is to be expected. By testing it, you can identify what needs to be brought into compliance to meet these new standards.

There are many different ways to test your business against your standard. The OSSTMM is an excellent guide to utilize to ensure a thorough testing of all aspects of security within your organization. Many companies outsource these types of security testing as they are rather in-depth and they may not have the employees certified or competent to conduct them.

Consultants can help by providing experts in each area of an OSSTMM test as well as tailoring the individual tasks of the test to fit the individual business, regardless of size. Some consultants will even work with people on your staff to do the testing when a certification of the OSSTMM test isn't required such as in the case we are describing.

Smaller businesses can benefit from a knowledgeable consultant that can take the OSSTMM and scale it for use at a smaller business.

The largest of companies should take no more than 90 days from start to report-in-hand for this type of testing, and smaller companies should be able to have their reports delivered in just a few short weeks.

The OSSTMM requires a reporting workshop that identifies each area in need of improvement to resolve vulnerabilities. Each of these items should be reviewed and fixed as quickly as time and budget allow. As each section of items in the report is repaired it should be spot tested to verify that it is compliant with your "Perfect Security Standard".

Step Three: Kick it up a notch.

Another benefit of an OSSTMM test is that it will point out areas of improvement for the efficient running of your company. This will assist you in realizing changes that could save the company money by economizing and streamlining your processes. This type of testing also may identify other areas that could be run more efficiently, and if deemed necessary, will give you the ability to go back to the policy and make changes to run your business effectively.

In addition to updating your Security Policy, you can also use this opportunity to have your technical personnel update the guidelines and procedures within each area of the Security Policy. This is an important part of the process as this assures your employees fully understand what your Policy dictates and know what steps to take to follow it.

Conclusion

Now that the framework is in place, you can now go back and perform your Security Audit for compliance purposes. An OSSTMM Certified Security test is a great example of this. If you used the OSSTMM as your assessment test then you now know what's involved so there will be no surprises. The OSSTMM is quickly becoming the de-facto world standard for compliance audits. It is known throughout the world and over 150 security professionals review and submit updates to the OSSTMM on a regular basis. The OSSTMM is compliant with a number of laws and best practices from many different countries. It truly is a global document.

Finding your company's Perfect Security is not a once and done thing. Your Perfect Security Policy is a living document and must be reviewed and updated on a regular basis. Performing this along with regular testing of your security posture will prove that you are performing your due diligence and due care.

About the Author

Charles "Chuck" Fullerton has worked in the IT and Security fields for over 15 years. After serving in South Korea with the U.S. Army, Chuck has worked with many different industries such as, manufacturing, education, finance, healthcare, law enforcement and telecommunications. His philosophy on security is that "everyone has a responsibility to maintain a level of security for themselves on the Internet. People must learn how to secure the equipment under their control." Chuck started the Charles W. Fullerton Institute of Analysis to do just that. CIA was then acquired by Fullerton Infosec, Inc. in July of 2004. Chuck also teaches Intense School's Professional Hacking course which prepares security professionals for the Certified Ethical Hacker Examination.

Fullerton Infosec's motto is "We Care about Your Security." We are committed to providing ethical, objective, vendor neutral security testing to our customers. We also provide Security Policy generation and updating, Security Awareness training and will open are Honeynet Project to clients starting towards the beginning of 2005. Chuck can be reached via email at cfullerton@fullertoninfosec.com.

Document Search Keywords

Security Policy, Security Architecture, Security Testing, Perfect Security, OSSTMM, ISECOM, Chuck Fullerton, Fullerton Infosec