

Rebuilding the Human Firewall

Michael E. Whitman
Kennesaw State University
1000 Chastain Rd, MS 1101
Kennesaw, GA 30144
770-423-6005

mwhitman@kennesaw.edu

Philippa Fendler
Kennesaw State University
1000 Chastain Rd, MS 1101
Kennesaw, GA 30144
770-423-6005

pfendler@students.kennesaw.edu

John Caylor
Kennesaw State University
1000 Chastain Rd, MS 1101
Kennesaw, GA 30144
770-423-6005

jmc4189@students.kennesaw.edu

Danny Baker
Kennesaw State University
1000 Chastain Rd, MS 1101
Kennesaw, GA 30144
770-423-6005

dmb3237@students.kennesaw.edu

ABSTRACT

In 2000, a consortium of industry, government and academic representatives formed the Human Firewall Council, established on the premise that information security is a people problem, a managerial problem that does have some technical solutions. In 2004 the HFO changed hands, from the original commercial sponsoring organization to the ISSA. With this change came a need to revise and update the organization's Web site, and the Security Management Index, an online survey that allowed respondents to benchmark their organizations with their peers, based on the ISO 17799 standard. This paper overviews the efforts of a faculty and student development team in rebuilding the Human Firewall.

Categories and Subject Descriptors

C.2.0 [Computer Communications Networks]: General – Security and protection

K.3.2 [Computers And Education] - Computer and Information Science Education – Curriculum, Information systems education.

K.4.1, .2 & .4 [Computers And Society] - .1 Public Policy Issues - Abuse and crime involving computers, Computer-related health issues, Ethics, Intellectual property rights, Privacy. .2 - Social Issues - Abuse and crime involving computers. .4 Electronic Commerce - Security

K.6.5 [Management Of Computing And Information Systems] - Security and Protection – Authentication, Invasive software, Unauthorized access.

General Terms

Management, Security, Human Factors, Standardization, Legal Aspects.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Information Security Curriculum Development (InfoSecCD) Conference '05, September 23-24, 2005, Kennesaw, GA, USA. Copyright 2005 ACM 1-59593-261-5/05/0009...\$5.00.

Keywords

Information Security, Information Assurance, Information Security Awareness, Information Security Regulatory Compliance, Information Security International Standards

1. INTRODUCTION

Information security, from its humble beginnings as computer security, has often been misrepresented as a technological problem with technological solutions. Modern thought on information security has revealed an approach more aligned with strategic business management. Information Security is about managing information risk. Managing information risk is about identifying and assessing threats to the information assets in the organization, and taking specific steps to counter those threats. In 2000, a consortium of industry, government and academic representatives formed the Human Firewall Council, established on the premise that information security is a people problem, a managerial problem that does have some technical solutions. This consortium founded a virtual society, the Human Firewall Organization. The HFO was open to anyone who agreed with its Manifesto:

As a business leader and member of my organization's information security team, I realize that information security is not just a technology concern confined to the IT department. I recognize the need to give equal attention to human management and worker behavior security issues, and will strive to build better information security awareness throughout my organization based on the principles described here in the Human Firewall Manifesto.

In 2004, the commercial organization that sponsored the Human Firewall Organization, and its virtual home, was acquired by another security organization. After a short while, the demands on the original founders in their new roles in the acquiring organization required that they seek sponsorship for the HFO elsewhere. At the time, members of the Human Firewall Council, as the advisory committee for the Human Firewall Organization were also members of one of the most widely recognized

professional associations in information security, the Information Systems Security Association (ISSA). The leadership of the ISSA agreed to accept sponsorship of the HFO, and in early 2005, the organization shifted its virtual residence.

2. THE SECURITY MANAGEMENT INDEX

At the time control was transferred to the ISSA, the HFO had been offering the Security Management Index (SMI), from its website for over three years. The SMI was a benchmarking service, offered free of charge, designed to compare a respondents' survey to the most widely recognized international information security standard, ISO 17799. ISO 17799 originated as British Standard BS 7799 – and was formalized by the ISO in 2000. "ISO17799 is actually "a comprehensive set of controls comprising best practices in information security". It is essentially, in part (extended), an internationally recognized generic information security standard. The ISO 17799 standard comprises ten prime sections:

- Security Policy
- System Access Control
- Computer & Operations Management
- System Development and Maintenance
- Physical and Environmental Security
- Compliance
- Personnel Security
- Security Organization
- Asset Classification and Control
- Business Continuity Management (BCM)"[1]

The SMI asked approximately 130 over the 10 domains. Upon completion of the survey, the respondent would receive their score, rated as a percentage, and the scores of their peers a) by industry, and b) by organizational size (e.g. under 500 employees).

It was the recognized value of this instrument that motivated the ISSA to sponsor the HFO.

3. KENNESAW STATE UNIVERSITY AND THE SMI

In 2003, one of the faculty members at Kennesaw State University, who had served on the Human Firewall Council while employed in industry, engaged the principal author of this paper to join the Human Firewall Council, as the author's published works clearly reflected the same vision and orientation as the HFC. Both faculty members were members of the ISSA. During the transition between the corporate sponsor and the ISSA, the two KSU faculty members volunteered to increase their level of involvement in the administration and governance of the HFC and the SMI. In late 2004, the principal author completed a revision of the SMI, more closely aligning it with the ISO standard, and removing any marketing-oriented references. The KSU faculty also began an analysis of the survey responses over the entire life of the SMI. In doing so, certain implementation issues arose that prompted the team to recommend a complete overhaul of the SMI, and eventually the HFO Web site as well. During the summer of 2005, a team of graduate students, lead by the principal author began this overhaul.

3.1 Objectives of the Project

The SMI project had three principal goals:

1. Improve the ability of the administrators to extract the finalized survey responses for statistical analyses. At the current time the dynamic nature of the SMI allowed the easy addition of questions, but made it difficult to extract the responses. The survey responses of some 2400 respondents resulted in over 120,000 entries in the survey database.

2. Update the SMI questions to reflect the changes recommended by the KSU faculty team the previous year. The SMI questions, while technically accurate required additional modification for statistical validity. Some categories had an equal number of questions as the standard had sub-categories, while others differed. It was determined that the two documents needed to be more closely aligned.

3. Update the application infrastructure supporting the SMI and the HFO Web site to facilitate future updates, and to bring the site into standard practice. The older VB framework needed to be updated to VB.Net, allowing easier maintenance and functionality.

3.2 Goals Supporting the Objectives

The goals of the project assigned to the student development team based on the objectives are:

- Either create a new Security Management Index (SMI) survey or repair the existing one and insure its functionality.
- Update links so that they were site relative.
- Update database code such that it was site relative.
- Debug pages and get them functional with the primary focus on the SMI.
- Create a data extraction utility that would build a CSV file from the database table.
- Update dynamic questions in the database.
- Update information on several pages.
- Update colors to enhance look and feel of the site.
- Test the availability and reliability for the site to ensure that links actually work and that the functionality of the dynamic code performs as expected.

3.3 Analysis of Initial System State

Initially the site had several issues that required resolution before the SMI could be addressed. These included:

- Numerous pages and directories which were no longer in use
- System files that did not function.
- Links were not document relative.
- Database code relied on hard coded location that was not relative to the location of web files.
- Numerous errors on each page that disrupted functionality.
- Dynamically loaded questions in the database were outdated.
- Data in the access database files was difficult to extract and utilize within a reasonable amount of time.
- While working on the functionality of the survey, the

look and feel could be updated to make the site more attractive and user friendly.

3.4 Work of the Project Team

Over the course of the assigned project, the team managed to complete most of the overall goals of the project. The team:

- Created a data extraction utility that took the row based answers and converted them into a comma delimited query file, listed by participant.
- Repair of all database code to make it site relative.
- Repair of numerous asp VBScript errors to make asp pages functional including all SMI related pages.
- Updated numerous links to be document relative.
- Building of the SA Survey and Register pages in .NET. The pages are functional yet not accessed by the current site as the ADO.NET pages are not included.
- Numerous HTML fixes to update page information and complete simple HTML coding.
- For user friendliness, “Back to Top” links have been added for easy navigation within long pages.
- The existing yet not applied style sheet was updated and linked to make design changes easier.
- Documentation for future references has been created. For the database table documentation, please see below.
- Due to the new use of colors, new “Page Headlines” were created using Macromedia Fireworks.

These updates met the criteria laid out for the project team.

3.4 Future Enhancements

Although these changes have greatly increased the usefulness of the Security Management Index, and the HFO Web site, the following additional changes are planned:

- Update the member list to reflect active members.
- Include credits for completed enhancements.
- Review and if necessary update the copyright statement to reflect all copyrights holdings.
- Make the navigation a separate file that is included within the pages, so that future changes will only have to be done once.
- Change and update pictures to refresh the look from time to time.
- Update news articles to give this section meaning, otherwise it is better to be left off.
- Update and replace links on the resources page to make it meaningful.

In addition to revisions planned for the remainder of the Web site, the site also contains another survey, the Security Awareness

Index, a 30 question instrument designed to allow the respondent to benchmark their information security awareness efforts with their peers and industry. This survey requires the same attention afforded the SMI. The overall site will continue to undergo revisions as the Human Firewall Council itself evolves.

In July 2005, a new version of the ISO 17799 standard was published. The next major project will be to compare the two standards to determine what if any changes will need to be made to the SMI.

4. LESSONS LEARNED AND CONCLUSIONS

From academic and information security standpoints, the project provide a number of learning opportunities, for the students performing the revision, the faculty members managing the project, and the HFC/ISSA program leadership. These include the following:

The conversion of a published standard to an interactive questionnaire is a project best handled by a panel of experts knowledgeable on the subject. The use of such a team made the process much more accurate than if a single individual had attempted to do so.

The inclusion of student team members dramatically reinforces their learning experiences, combining diverse skills from Web services, Web site development, database organization and query and information security standards content. Each student came away from the project far more knowledgeable on the breadth of the project than they were prior to its initiation.

The value of the sponsor of the organization will prove to be far more valuable than originally estimated. With the established membership of the ISSA, the HFO will be able to combine its fellowships with that of the ISSA and reach far more individuals and organization than previously possible. With the reconstitution of the HFO Website and the Council itself, the program will elevate the value of its projects to support the national needs in protecting cyberspace, and meeting the need for increased information security program development and awareness in all sectors, public and private.

5. ACKNOWLEDGMENTS

Our thanks to the ISSA for their support in the use of the HFO content in this paper.

6. REFERENCES

- [1] Anonymous. “The ISO 17799 Directory” WWW Document viewed 5/15/2004 from <http://www.iso-17799.com>.