WEB SITE SECURITY DISCLOSURE POLICIES OF ONLINE SECURITIES FIRMS: ARE THEY SATISFACTORY?

Donald R. Moscato, Iona College, dmoscato@iona.edu
Eric D. Moscato, Iona College, emoscato@iona.edu

ABSTRACT

This paper is the latest component of a research project conducted by the authors over a four-year period. The first phase emphasized the privacy policies of global banks and other businesses engaged in E-commerce [7, 8, 9, 10, 11, 12]. Over 800 individualized web-sites were visited and evaluated. This, the third phase of the research project, focuses on the security policies in place for retail online securities institutions. The purpose of this research study is to review, compare and summarize the security policies of online securities firms as they are expressed on their web sites. As part of this study, we ask the important question "Are the existing web site policies inadequate, acceptable or laudable"? The study was conducted during the month of June, 2006. On of the authors conducted the review of each of the sites evaluated. This paper reports on the results of 59 major, high profile online securities organizations.

Keywords: Security, online securities firms, encryption, firewalls, web sites

INTRODUCTION

As more and more global business is conducted via an E-commerce modality, it is imperative that a level of trust is achieved whether it is business-to-business (B –B) or business-to-consumer (B-C). The consumer must be confident that a business establishment has taken the proper precautions to secure its site and data from either deliberate or accidental disclosure, modification or destruction (4). This trust is especially necessary while conducting any type of financial securities' transactions. "According to an FCC study, nearly 10 million consumers were victimized by some form of identity theft in 2004 alone- That equals 19,178 people per day, 799 per hour and 13.3 per minute" [14]. It is

easy to understand why companies are rushing to stem the tide of potential bad publicity that could be disastrous for their reputations. According to a Wall Street Journal article identity-software sales are on the rise [3, 7].

The element of trust in any business relationship is a necessary condition. One might say that e-commerce is dependent on the mutual trust of both sides of the relationship. In security transactions, the consumer is engaging in financial transactions via cyberspace and the firms involved must create an infrastructure that not only provides security to its customers but also communicates its security policies to its clientele in an effective manner. This infrastructure might include one or more of the following components: firewalls, encryption, event logging, passwords for authentication of users, monitoring software and biometric devices. But the nomenclature of security can be obtuse and difficult to comprehend by the typical customer. On the other hand, if a securities firm does not provide enough information on security to its customers, then the relationship is based solely on blind trust. Our objective in this paper is to visit the web sites of online securities firms, perform both a quantitative and qualitative assessment of explicitly stated security features and to provide an interpretation of the results obtained.

For this research project, the authors surveyed the web sites of over 59 online securities firms and focused on the security information communicated by these firms to its customers. A questionnaire was developed to capture the relevant data from each site.

COMPONENTS INCLUDED IN THE QUESTIONNAIRE

A multi-part questionnaire created by the authors based on either the presence or absence of a given security feature response was completed for each web site reviewed. These security features were selected based on information contained in FFIEC research documents as well as items identified in the financial securities industry as being timely and relevant to customer transaction security [4].

The following list of security features were used in the study:

- Encryption in the transmission of data
- Encryption in the storage of data
- The strength of the encryption employed
- The existence of firewalls
- The use of event logging, auditing and monitoring
- The use of a user login and password
- The use of a glossary of security terms
- The use of a system timeout feature and
- The existence of a formal statement on identity theft.

As further background statistics, the authors also determined the length in pages of any security statements, whether there was a link to the security statement on the firm's home page and qualitative assessments on the level of detail contained in the security statement and whether or not the security policy statement was easy to read and understand.

The next section of the paper presents the results of the site visits in tabular form along with a brief interpretation of them followed up by any implications that can be deduced from the findings.

RESULTS

Table 1 presents the data on how many pages were used by each securities institution to communicate its security policy. By far either one or two pages were used for expressing the security statements.

TABLE 1
Number of Pages Devoted to Security Policy

PAGES	Number	Percentage
0	4	7%
1	32	54%
2	14	24%
3	2	3%
4	1	2%
5	2	3%
6+	4	7%

Table 2 depicts the characterization of the level of detail in the various firms' security policies. The three categories are as follows: very detailed (includes technical terms), not technical (uses only narratives without technical terms) and skimpy (very little description of security). It is interesting that there was almost an equal distribution across all three categories.

TABLE 2
How Detailed is the Security Policy?

Level of Detail?	Number	Percentage
Very Detailed	19	32%
Not Technical	21	36%
Skimpy	19	32%

Table 3 shows that the vast amount of companies do have a link to the security statement on their home page.

TABLE 3
Is There a Link to the Security Statement on the Home Page?

Is There a Link?	Number	Percentage
Yes	42	71%
No	17	29%

Table 4 illustrates very clearly that retail securities firms were overwhelmingly more explicit in their policy statements that they encrypted their customers' data during transmission. A "No" response does not mean that the companies do not encrypt, only that they do not explicitly state that they do. Our focus is on how and what they communicate on their web pages.

TABLE 4
Policy Statement on Encryption of Data During Transmission

Transmission Encryption of Data?	Number	Percentage
Yes	37	63%
No	22	27%

Table 5 shows that only about one third of the firms were explicit in their security statement on data encryption during storage. Compare these results with Table 4 and encryption during transmission.

TABLE 5
Policy Statement on Encryption of Data During Storage

Storage Encryption of Data?	Number	Percentage
Yes	21	36%
No	38	64%

Table 6 shows rather surprisingly that more than half of the securities firms do not explicitly state to the consumer who will have access to their data. This revelation is alarming. Encryption is an agreed upon mechanism for enhancing online security [18, 21].

TABLE 6
Does Security Policy Say Who Has Access to Data?

Access to Data Statement?	Number	Percentage
Yes	26	44%
No	33	56%

Table 7 shows that over two thirds of the retail securities firms are not likely to explicitly state that firewalls are employed as an integral part of their network security policy.

TABLE 7
Is There a Statement on Firewalls in Network Security?

Firewall Statement?	Number	Percentage
Yes	18	31%
No	41	69%

Table 8 illustrates very emphatically that online retail securities institutions do not share information on logging, auditing or monitoring policies that might be in place.

TABLE 8
Is There a Statement on Logging, Auditing or Monitoring?

Logging, Auditing, Monitoring?	Number	Percentage
Yes	15	25%
No	44	75%

Both **t**ables 9 and 10 show that the online retail securities firms were overwhelmingly more likely to state that passwords and user logins were required to use the sites. In point of fact, the responses were identical in both tables.

TABLE 9
Is a Password Required to Use the Company's Site?

Is Password Required?	Number	Percentage
Yes	53	90%
No	6	10%

TABLE 10
Is a User Login Required to Use the Site?

Is User Login Required?	Number	Percentage
Yes	53	90%
No	6	10%

TABLE 11 shows that the retail securities institutions were very evenly split in their policy of explicitly revealing whether or not SSL technology was being used on the site.

TABLE 11
Does the Site State it Employs SSL?

Use of SSL?	Number	Percentage
Yes	34	58%
No	25	42%

Table 12 shows that the vast majority of the online retail securities firms studied do not include a glossary of terms on their web sites. We expect this observation to be reversed in the near future as more companies attempt to inform their customers of the need for more security awareness.

TABLE 12
Is There a Glossary of Terms on the Web Site?

Is There a Glossary of Terms?	Number	Percentage
Yes	8	14%
No	51	86%

Table 13 illustrates that about two thirds of the retail securities firms still do not have statements

on identity theft on their web sites. This should also change in the near future as more and more incidents of identity theft are given more publicity in the media.

TABLE 13
Is There a Statement on Identity Theft?

Statement on Identity Theft?	Number	Percentage
Yes	20	34%
No	39	66%

Table 14 shows that most securities' firms, by a wide margin, do not state the existence of a timeout feature on their web sites. Once again, by explicitly making the consumer aware of this feature the company draws attention of the need to always be security conscious when dealing with financial transactions [15].

TABLE 14
Is There a Timeout Feature Stated on the Web Site?

Is There a Timeout Feature?	Number	Percentage
Yes	18	31%
No	41	69%

Table 15 shows that online retail securities institutions are much more inclined to have a section of their web sites devoted to security tips. The quality of this section varies dramatically across the various companies visited in this survey.

TABLE 15
Is There a Statement on Useful Security Tips on the Web Site?

Statement on Security Tips?	Number	Percentage
Yes	42	71%
No	17	29%

Table 16 summarizes quite effectively the fact that two thirds of the web sites surveyed appear to be easy to read and comprehend. Unfortunately, this characteristic when viewed in the light of the previously reported results does not imply that the consumer is receiving an adequate level of disclosure of security policies being employed by the different institutions.

TABLE 16
Is the Bank's Security Policy Statement Easy to Read and Understand?

Easy to Read & Understand?	Number	Percentage
Yes	40	68%
No	19	32%

SUMMARY AND CONCLUSIONS

The focus of this paper was on the content and scope of the security statements that the 59 surveyed online securities firms published on their web sites. The absence of explicit statements focusing on the numerous criteria contained in the questionnaire does not necessarily mean that the firms do not employ one or more of these security features. It only suggests that they did not choose to share that information with their consumers in a readily accessible manner. One cannot make any generalizations as to the reason or intent of these decisions. We can only comment on their presence or absence in the web pages. The authors selected the specific items to include in this study based on a review of important security criteria often cited in the literature. From the results reported in this paper it is quite clear that some of the security criteria are explicitly employed by some firms more than others. For example, statements on the timeout feature, identity theft, a glossary of terms, encrypting for storage, security hints and logging are not as universally adopted as some of the others. One could argue that as consumers get more sophisticated and, as e-commerce activity escalates, online securities institutions will be more inclined to add some of these criteria in order to build customer trust [19].

It is also interesting that these companies differed in the ease of understanding as well as the number of pages devoted to the security statements. As more consumers become aware of the risk exposure of their financial assets, it is likely that they will (along with the respective government regulators) get more involved in demanding greater security from the financial securities companies [1].

In 10 out of 13 items reported in this paper, the percentages were greater than or equal to 64% in one of the categories. This discovery represents a substantial difference in the reporting profile among institutions. We have tried to elaborate

within the paper on the implications for the industry emanating from this disparity. In three of the categories the percentages hovered around 50/50 which represents an even split among the firms' sites that were reviewed. Why is there such a disparity among the results? Clearly, some firms believe that it is important to share security policies with the consumer so as to build up trust in the organization. On the other hand, those that do not disclose more information might be doing so because they do not believe that it is either needed or important. Perhaps, some might not have given it sufficient attention out of ignorance. One can only hazard a guess.

Another interesting question that can be raised is to whether or not there should be more government regulation focused in this area. What with Sarbanes-Oxley and the recent FFIEC (the U.S. Federal Financial Institutions Examination Council) guidelines , one can reasonably ask if the Securities and Exchange Commission (SEC) should mandate all online securities firms to use a common template of security disclosure practices [6, 18]. FFIEC in recent pronouncements has been much more aggressive in their guidelines regarding authentication policies and identity theft [9, 20]. Although the focus of the guidelines was on two-level authentication factors, it might not be that unrealistic that they might address firewalls, logging, encryption and monitoring as standards for the industry as part of a greater risk management policy. If left to their own actions, will more retail securities firms voluntarily increase the disclosure of security standards on their web sites or will they be motivated by coercion from either the government or quasi-governmental agencies?

As with all meaningful situations there are going to be significant trade-offs. Unfortunately, as financial institutions pursue strategies that increase user friendliness they do so at the risk of unnecessarily greater exposure to security violations [2]. It is the authors' conclusion that, in the near future, there must be a convergence to a fuller disclosure of security policies on web sites or else consumers will be wary to engage on financial transactions with the recalcitrant institutions. Finally, it is the authors' contention that, from an overall assessment, the published securities' policies of the selected high profile online securities firms are inadequate to garner the level of trust that is essential to an informed customer. Especially, in light of the rapid rise of identity theft as published in the popular media.

REFERENCES

1. Bank, David and Christopher Conkey (2005) New Safeguards for Your Privacy, *Wall Street Journal*, March 24.
2. Bauerlein, Valerie (2006). Online Banking Strives for the Human Touch, *Wall Street Journal*, July 6, pp. D1, D2
3. Delaney, Kevin J. (2005). 'Evil Twins' and 'Pharming', *Wall Street Journal*, May 1, B1.
4. Federal Financial Institutions Examination Council (2005). *Guidance on Authentication in Internet Banking Environment.* http://www.ffiec.gov/press/pr101205.htm.
5. FTC Study (2000) Privacy Online: *Fair Information Practices in the Electronic Marketplace, A Report to Congress*, May.
6. Marlin, Steven (2005). Congress Responds to Data-Security Fears, *Information Week*, July, 26.
7. McWilliams, Gary (2005). Identity-Software Sales Are Soaring, *Wall Street Journal*, May12.
8. Moscato, Donald and Benjamin Robinson (2002) The Global Race to Compliance: Information Privacy in an Electronic Commerce Framework, *Comm. of the IIMA*, Vol. 2, 4, 111-120.9.
9. Moscato, Donald (2003) An Empirical Analysis of Web Site Privacy and Security By Industry, *Issues in Information Systems*, Vol. Iv, Issue 1, 264-270.
10. Moscato, Donald and Eric Moscato (2004) An Assessment of Privacy and Security Policies of Global Financial Institutions, *Proceedings of Third Int'l Business. And Economy. Conference.*
11. Moscato, Donald and Eric Moscato (2005) Explicitly Stated Security Policies of Web Sites of Global Banks of Europe, Australia, Asia and the U.S. *Communications of the IIMA*, Vol. 6, Issue 3.
12. Moscato, Donald and Eric Moscato (2006) Published Security Policies of Web Sites of Global Banks of Mexico, Central & South America, Canada and the U.S., *Issues inInformation Systems*, Vol. VII, No 2, 23-227.
13. Moscato, Donald and Eric Moscato (2007) Pursuing Trust in an Internet Banking Environment: The U.S. Experience, *Proceedings of the Sixth Annual Business and Economy Conference*, January, 2007.

14. Petouhoff, Natalie L. and Brian Johnson (2006) "How Much is Your Customer's Trust Worth," *Customer Inter@ction Solutions*, July, p. 52-53.
15. Robb, Drew (2005). Ciphering Out Security, *Computerworld*, September 19, 26-29.
16. Rompei, Adam. (2005). The World's Best Internet Banks, *Global Finance*, September, 31-35.
17. Roth, Daniel and Stephanie Mehta. (2005). The Great Data Heist, *Fortune*, May 16, 66-75.
18. Snyder, Joel. (2005). Tale of the Tape: Encrypt Data Now, *Network World*, July 4, 13.
19. Strom, David (2007). Fraud Busters, *Information Security*, January, 24-31.
20. Vance,Jeff (2006).Guide to Two-Factor Authentication, *Network World*,June,36-38
21. Vijayan, Jaikumar (2003) New Privacy Rules Could Mean Headaches for Financial Services IT, *Computerworld*, August 11, 7.