Explicitly Stated Security Policies of Web Sites of Global Banks of Europe, Australia, Asia and the U.S

Donald R. Moscato
Iona College

Eric D. Moscato
Iona College

Explicitly Stated Security Policies of
Web Sites of Global Banks of Europe, Australia, Asia and the U.S.

Donald R. Moscato
Iona College, Information Systems, New Rochelle, New York 10801
(914) 633-2555
dmoscato@iona.edu

Eric D. Moscato
Iona College, Finance, New Rochelle, New York 10801
emoscato@iona.edu

ABSTRACT

This paper is the latest component of a research project conducted by the authors over a three-year period. The first phase emphasized the privacy policies of global banks and other businesses engaged in E-commerce. Over 600 individualized web-sites were visited and evaluated. This, the second phase of the research project, focuses on the security policies in place for global financial institutions. The purpose of this research study is to review, compare and summarize the security policies of global banks as they are expressed on their web sites. A total of over 300 web sites of global banks were included in this phase of the study. The study was conducted during the month of June, 2005. This paper reports on the results of a total of 180 banks representing Europe (40), Australia (20), Asia (60) and the U.S. (60).

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 their sites and data from either deliberate or accidental disclosure, modification or destruction. This trust is especially necessary while conducting banking transactions.

In his book, Kevin Day (2005) presents eight security rules. They are as follows: (1) rule of least privilege, (2) rule of change, (3) rule of trust, (4) rule of weakest link, (5) rule of separation, (6) rule of three-fold process, (7) rule of preventive action and (8) rule of immediate and proper response. Any global bank would be wise to base their e-commerce security on a well-planned total security framework such as Day proposes.

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 banking, the consumer is engaging in financial transactions via cyberspace and the global banks 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. But the nomenclature of security can be obtuse and difficult to comprehend by the typical customer. On the other hand, if a bank does not provide enough information on security to its customers, then the relationship is based solely on blind trust.

For this research project, the authors surveyed the web sites of over 300 global banks and focused on the security information communicated by these banks to its customers. A questionnaire (see Appendix I) was developed to capture the relevant data from each site. One hundred and eighty banks are included representing Europe, Australia, Asia and the U.S.

The first section of the paper presents a discussion of security criteria that is widely considered important for organizations engaged in e-commerce and especially global banking institutions. In the second section, the authors present the tabulated comparisons among the four selected banking regions. They are presented along with a

discussion of the results. In the final section of the paper, the authors present a summary and conclusion along with a future research plan.

IMPORTANT SECURITY CRITERIA FOR BANKS

Encryption

Encryption is the coding of plain text information into unreadable/unbreakable data that will eventually be deciphered at the other end. A bank can utilize encryption in two ways. It can focus its efforts on encrypting the transmitted message so that if it is intercepted it will not be understood. It can also utilize encryption to store customers' financial information and transactions. At the very least a bank should have a mechanism in place to encrypt its transmitted data (Snyder, 2005; Chiampa, 2004). These transmission lines can be secured by using 128 bit encryption schemes like Secure Sockets Layer (SSL). SSL gives the customer the trust that he/she is communicating with the actual bank's site and not an imposter site (Thibodeau, 2002).

Digital certificates are used by banks. A digital certificate is issued by a trusted third-party and is usually made up of the following: "sender's name, sender's public key, expiration date of the public key, name of certificate authority, unique serial number and the digital signature of the issuer" (Mackey, 2003). Verisign and Thawte are two of the major third-party verifiers in use today (Solomon and Chapple, 2005). IBM, through a relationship with Identus, is offering digital certificates to banks (Martens, 2005). Worthen discusses an ROI approach that an organization can take regarding seals (Worthen, 2003).

Access to Customer's Data

In many countries there are stringent policies that organizations must adhere to regarding who has access to customer data. In the United States, the Federal Trade Commission (FTC) has published guidelines known as the Fair Information Practices (FIP) recommendation (FTC, 2000). The European Community in its Data Directive covers the same general information. Of particular concern is the treatment of third party data and whether or not the customer must either "opt in" or "opt out" of bank's policies of data sharing (EU, 1995);(Scher, 2003). "The California Security Breach Information Act requires state agencies and businesses that collect personal information from Californians to promptly disclose certain security lapses or face severe penalties" (Francis, 2005).

Firewalls

A firewall is a function that is positioned at the front-end of a data communications network. Its purpose is to screen incoming transactions for improper activities. The firewall can be implemented in either the hardware, software or both. It can be thought of as a gatekeeper that keeps the organization's intranet secure from outsiders who have malicious intent. Firewalls can be combined with intrusion detection techniques and be implemented in a layered architecture. Firewalls are so commonplace today that many home and small business networks utilize their security capability. Ghosh (2001) points out, "firewalls are artificial barriers that no longer meet the needs of ubiquitous networks. That the distinction between inside and out is quickly fading."

Logging, Auditing and Monitoring

Since firewalls are meant to block out malicious activity and improper transactions in a bank's network, it is imperative that there be procedures in place to be able to audit bank activity on a periodic basis. "Recently adopted (US) federal rules require companies to employ strict safeguards and conduct routine security audits" (McWilliams, 2005). Banks should log all transactions in a network application noting time, place, authorization and nature of all transactions. These logs can also be employed in recovery operations as well as in traditional bank application audits. "The audit information records the information as it occurs. Auditing tools allow the administrator to find out who broke in and how, and help track down the culprit. The audit logs are often used in the prosecution of the culprit" (Pipkin, 2000). Banks can also have system software in place that monitors all activity going on in the

network. This software operates in the background and provides an additional layer of security protection to an organization.

Passwords and User Login Information

When a customer agrees to engage in e-commerce in a banking environment, he/she is usually assigned a user login and a password. The purpose of the user login is to tell the bank application who the intended party is that wants to use the system. This is referred to as the "identification" phase. Once the user logs in, that person must be "authenticated" by the bank application. The password allows the person to have a unique identifier. It can be something a person is, has or knows. Biometric technology is used in the first case whereas cards and passwords are used in the second and third situation. Passwords must be strong and not easily compromised. There are many suggestions available to guide a bank in selecting one approach versus another in its implementation policies.

Glossary of Terms

The proliferation of jargon surrounding the area of security has created a true dilemma for designers of web pages for banks. On the one hand, a bank wants to provide a designed level of security for its customers so that its objectives are achieved. Total security might not be either economically feasible or desirable from a customer friendly point of view. Yet, there is a very real desire on the part of some knowledgeable customers to know what security policies are being used by the bank that is the caretaker of their finances (Wood, et. al., 2004). By simply listing security policies in place, a bank risks overwhelming a part of the customer base that is confused by the jargon. For this reason, banks have begun to include both a glossary of security terms as well as "hot links" to additional web sites that further discuss some of the security practices.

Identity Theft

If e-commerce by banking institutions is to ever achieve its lofty predictions for success, it must find a way to earn the trust of the consumer regarding the potential for identity theft. Consumers want to believe that their transactions are safe in transmission and that once the data is resident on the bank's system their personal data will not be compromised. The literature is replete with harrowing stories of people that had their identity stolen and had a very difficult time returning to normalcy (Roth and Mehta, 2005). "Pharming and evil twins aren't yet widespread and certainly haven't become the huge problems phishing and spyware are. But they are insidious because they are harder to detect" (Delaney, 2005). Banks are increasingly making explicit statements on their web pages regarding the steps that they are taking to protect against identity theft. David Myron (2005), editor-in chief of Customer Relationship Management, asserts that "identity theft victims' assurance of security reflects comfort levels with online banking, and not their loyalty to a particular bank."

Timeout Feature

It is common practice to protect against a customer transaction that might not have been terminated properly. This might occur if a customer walks away from an ATM machine without "signing off" or if they take too long to process a transaction. The default condition by the bank's application system is to assume that there is problem and to end the transaction session. It is a trade-off between irritating a customer (in the case of a long pause in the activity) versus protecting the network from a stranger encountering an "open" session left by the previous customer. The fear is that the stranger will attempt to "piggyback" into the bank's system. Each bank sets its own timeout protocol based on the factors just discussed. For example, 10 minutes was a very common time limit used by banks in this study.

Statement on Useful Security Hints

Some banks have recognized that it is their best interest to have an educated consumer so they take extra effort in providing recommendations on how their customers might improve overall security. Suggestions on password selection, handling of cards and reporting potential compromises are but a few of these.

Section Summary

In this section we have discussed several security policies that were included in this research study of web site security policies of banks. Clearly, some are far more important than others. As we analyze the tabular results from the questionnaires from the three regions, you will be able to compare any similarities and differences among the three regions' banks.

RESULTS

The results are presented in the order in which the information appears on the questionnaire, which is included as Appendix I.Table 1 presents the data on how many pages were used by each region's banks to communicate their security policies. In all four regions either one or two pages were the most frequently used lengths for the banks' security statements.

Pages	Europe	Australia	Asia	U.S.
0	3	0	8	1
1	17	13	31	33
2	6	1	5	11
3	5	0	2	3
4	2	1	1	2
5	1	2	5	2
6+	6	3	8	8

Table 1: Number of Pages Devoted to Bank's Security Policy

Table 2 depicts the characterization of the level of detail in the various banks' 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). The Asian banks tended to be more detailed than the others in stating their security policies.

Level of Detail	Europe	Australia	Asia	U.S.
Very Detailed	12	10	29	18
Not Technical	15	8	15	30
Skimpy	13	2	16	12

Table 2: How Detailed is the Bank's Security Policy?

Table 3 shows that the European, Asian and U.S. banks typically have a link to the security statement on their home page. The Australian banks did not.

Is There a Link?	Europe	Australia	Asia	U.S.
Yes	36	6	44	47
No	4	14	16	13

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

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

Transmission Encryption of Data	Europe	Australia	Asia	U.S.
Yes	13	20	36	39
No	27	0	24	21

Table 4: Policy Statement on Encryption of Data During Transmission

Table 5 shows that most of the banks studied, regardless of region, did not have a stated policy statement on encryption during storage of data. When compared with Table 4 the results show that more attention was paid to encryption during transmission than to the storage of data..

Storage Encryption of Data?	Europe	Australia	Asia	U.S.
Yes	8	4	17	15
No	32	16	43	45

Table 5: Policy Statement on Encryption of Data During Storage

Table 6 shows that the U.S. Banks are more explicit in their statements regarding who has access to their customers' data. Both European and Asian banks seem to follow the same approach to reporting this type of information. Surprisingly, Australian banks showed a lower proportion of banks reporting than the other regions.

Access to Data Statement?	Europe	Australia	Asia	U.S.
Yes	17	4	24	41
No	23	16	36	19

Table 6: Does Security Policy Say Who Has Access to Data?

Table 7 shows that the Australian banks are more likely to explicitly state that firewalls are employed as an integral part of their network security policy. The Asian and U.S. banks report similar approaches on communication on firewalls with each other.

Firewall Statement?	Europe	Australia	Asia	U.S.
Yes	20	13	26	24
No	20	7	34	36

Table 7: Is There a Statement on Firewalls in Network Security?

Table 8 illustrates banks in all of the regions do not do an explicit job of reporting on the use of logs, audits and monitoring actions.

Logging, Auditing, Monitoring?	Europe	Australia	Asia	U.S.
Yes	8	6	14	21
No	32	14	46	39

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

Table 9 shows that in all of the regions, the banks visited in the study predominantly stated that user passwords were required. The banks in the U.S. and Australia were very strong in this area.

Is Password Required?	Europe	Australia	Asia	U.S.
Yes	23	19	33	57

No	17	1	27	3

Table 9: Is a Password Required to Use the Bank's Site?

Table 10 clearly distinguishes the security reporting policy of the Australian and U.S. banks when compared to the other two areas with respect to the use of logins.

Is User Login Required?	Europe	Australia	Asia	U.S.
Yes	13	20	33	56
No	27	0	27	4

Table 10: Is a User Login Required to Use the Site?

Table 11 shows that the banks in both Australia and the U.S. report about the same very emphatic use of stating that they use SSL for their sites. Banks in Europe, on the other hand, are almost the mirror image in their reporting format.

Use of SSL?	Europe	Australia	Asia	U.S.
Yes	11	20	33	52
No	29	0	27	8

Table 11: Does the Bank's Web Site State it Uses SSL?

Table 12 shows that the banks in all of the four regions do not believe that providing a glossary of terms is necessary for their customers. The results are remarkably similar.

Is There a Glossary of Terms?	Europe	Australia	Asia	U.S.
Yes	9	2	4	5
No	31	18	56	55

Table 12: Is There a Glossary of Terms on the Web Site.

Table 13 illustrates that the U.S. Banks are more explicit in warning customers about the possibility of identity theft. The banks in the other three regions do not have a statement on identity theft as a priority.

Statement on Identity Theft?	Europe	Australia	Asia	U.S.
Yes	14	5	6	31
No	26	15	54	29

Table 13: Is There a Statement on Identity Theft?

Table 14 shows that banks in Europe and especially Australia do state the existence of a timeout feature while only banks in Asia and the U.S. are less inclined to do so.

Is There a Timeout Feature?	Europe	Australia	Asia	U.S.
Yes	28	17	15	12
No	12	3	45	48

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

Table 15 shows that banks in Australia and Europe have a preference to include security tips directly on their web sites while those in the U.S. do so at a lesser extent. Only Asian banks had more banks not doing so than doing so on their web sites.

Statement on Security Tips?	Europe	Australia	Asia	U.S.
Yes	28	17	25	34
No	12	3	35	26

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

Table 16 summarizes quite effectively the fact that the U.S. banks' web sites appear to be more thorough in their content as well as being easier to read and comprehend by an overwhelming proportion. Fortunately, banks in all of the regions scored quite high in this area.

Easy to Read & Understand?	Europe	Australia	Asia	U.S.
Yes	32	17	37	58
No	8	3	23	2

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

SUMMARY AND CONCLUSIONS

As part of this phase of the research, and for the purpose of this paper, we visited the web sites of 180 banks representing four distinct regions of the global banking environment-Europe, Australia, Asia and the U.S. The focus was on the content and scope of the security statements that the banks 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 banks do not employ one or more of these security features. It only suggests that they did not 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 banks 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, banks will be more inclined to add some of these criteria in order to build customer trust (Rompei, 2005).

It is also interesting that these banks 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 banks (Bank and Conkey, 2005). "U.S. banking regulators have given the nation's banks an end 2006 deadline to introduce multi-factor authentication for high risk Internet transactions" (Ekers, 2005). This increased security should also manifest itself in an increased level of communication to the banks' customers (Vijayan, 2003). Global banks just cannot afford malicious attacks on their customers' financial information (Richmond, 2005; Acohido and Swarz, 2005).

In the future global banks must devote more attention to their internal controls and their security. For example, "early this year, the Federal Reserve Board told Citigroup to hold off making any more acquisitions until it improves its internal controls" (Myers, 2005). As global banks try to use more sophisticated data mining tools to better market services to their customers, they should devote commensurate attention to strengthening both their behind the scenes security policies and their manner of communicating them to their customers in an effective manner (Lamont, 2005).

Until global financial institutions can agree on an acceptable level of security policy disclosure to their customers that transcends national and regional boundaries, it will be up to individual banks to earn the trust of their clients. Pressure from national or regulatory trade block forces might speed this process up as in the case of the European Union or Hong Kong. Reliance solely on regulatory forces might not provide the impetus for this disclosure on a timely basis. Perhaps, the market place and the desire to be competitive in a potential desirable market will be the catalyst.

Another organizational issue that must be resolved is the probable existence of a bifurcated customer preference regarding the disclosure of security information present on a bank's web site. On the one hand, there are consumers who are technically savvy and they would naturally be expected to understand and expect to be informed about a site's web security policies. It is also plausible to hypothesize that there is also a segment of the population that does not have the least bit of interest in the statement of security policies utilized in a bank's web site. As long as this form of "blind trust" is not compromised then the customer will continue to assume that his bank has taken adequate security measures to protect his personal and financial data. The authors will continue to track global banks' security policy disclosure practices and monitor any changes that might occur.

REFERENCES

Acohido, Byron and Jon Swarz (2005),Cyber Cracking. *The Journal News*, November 7. Bank, David and Christopher Conkey (2005). New Safeguards for Your Privacy. *Wall Street Journal*, March 24.

Chiampa, Mark. (2004). Security Awareness: Applying Practical Security in Your World. Thomson: Course Technology. p. 141.

Cline, Jay (2003). The ROI of Privacy Seals. *Computerworld*, June 2, 42.

Day, Kevin (2003). Inside the Security Mind. Prentice Hall.pp 39-71.

Delaney, Kevin J. (2005). Evil Twins and Pharming. *Wall Street Journal*, May 17.

Directive 95/46/EC of the European Parliament and of the Council of the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement, (1995). October 24.

Ekers, John (2005).It's All in the Cards. *Security Products*, December. Francis, Bob (2005).Security Nightmares Come True. *Infoworld*, May 16.

FTC Study (2000). Privacy Online: *Fair Information Practices in the Electronic Marketplace*, A Report to Congress, May.

Ghosh, Anup K. (2001). Security and Privacy for E-Business. Wiley. P. 27.

Lamont, Judith (2005). Predictive Analytics: An Asset to Retail Banking Worldwide. *KM World*, November/December.

Mackey, David. (2003). Web_Security for Network and System Security Administrators. Thomson: Course Technology.

Martens, China (2005). IBM Offers Digital Certificates to Banks. *Network World*, July 11.

McWilliams, Gary (2005). Identity-Software Sales are Soaring. *Wall Street Journal*, May 12.

Moscato, Donald and Benjamin Robinson (2002). The Global Race to Compliance: Information Privacy in an Electronic Commerce Framework. *Communications of the IIMA*, Vol. 2, Issue 4, 111-120.

Moscato, Donald (2003). An Empirical Analysis of Web Site Privacy and Security by Industry. *Issues in Information Systems*, Vol. IV, Issue 1, 264-270.

Moscato, Donald and Eric Moscato (2004). An Assessment of Privacy and Security Policies of Global Financial Institutions. *Proceedings of Third International Business and Economy Conference*, January 2004.

Myers, Randy (2005). How Global is your Bank? *CFO Banking and Finance*, Fall.

Myron, David (2005). Online Banking: Consumer Trust versus Loyalty. *Customer Relationship Management*, September.

Pipkin, Donald L. (2000). Information Security. Prentice-Hall. 177.

Richmond, Riva. Banks Seek More Potent Online-Security Tools. *Wall Street Journal*, December 1.

Rompei, Adam. (2005). The World's Best Internet Banks. *Global Finance*, September, 31-35.

Roth, Daniel and Stephanie Mehta. (2005). The Great Data Heist. *Fortune*, May 16, 66-75.

Scher, David (2003). Europe's New High-Tech Role: Playing Privacy Cop to the World. *Wall Street Journal*, October 10, A1&A16.

Slemmons Stratford, Jean and Juri Stratford (1998). Data Protection and Privacy in the United States and Europe. *IASSIST Quarterly*, Fall, 17-20.

Snyder, Joel. (2005). Tale of the Tape: Encrypt Data Now. *Network World*, July 4,13.

Solomon, Michael G. and Mike Chapple. (2005). Information Security Illuminated. Jones and Bartlett. 228.

Thibodeau, Patrick (2002).Truste Says Licensing Changes Will Give Privacy Seal More Teeth. *Computerworld*, December 16, 12.

Vijayan, Jaikumar (2003).New Privacy Rules Could Mean Headaches for Financial Services IT. *Computerworld*, August 11, 7.

Wood, Wallace and Susan Haugen and Robert Behling (2004). Is Corporate America Meeting Its Information Privacy Responsibilities. *Issues in Information Systems*, Vol. V, No. 2, 720-726.

Worthen, Ben (2003). The ROI of Privacy Seals. *Computerworld*, June 2, p. 42.

APPENDIX I

Security Questionnaire

Background Information:

Industry _____

Date Visited:_____

Name of Company:_____

URL of Home Page:_____

URL of Security Page:_____

Number of Pages Devoted to the Security Policy Statement: _____

Is there a link to the security statement on the home page? Yes_____ No____

How Detailed is the Security Policy Statement? (Check one)

        Very Detailed (specific technologies used)_____
        Not Technical (general statement)_____
        Skimpy (1 or 2 lines)_____

Content Included in Policy Statement:

1. Policy on encryption during transmission of data: Yes_____   No_____
   (browser security level)

2. Policy on encryption during storage of data: Yes_____   No_____

3. What level of encryption is used (eg.128 bit SSL)   _____

4. Does policy say who has access to the data?   Yes_____   No_____

5. Is there a statement on network security (firewall)? Yes_____   No_____

6. Is there a statement on logging, auditing and monitoring?
                             Yes_____   No_____

7. Is a password required to use the site?   Yes_____   No_____

8. Is a username required to use the site?   Yes_____   No_____

9. Do they use SSL?   Yes_____   No_____

10. Is there a glossary of terms provided?   Yes_____   No_____

11. Is there a statement on identity theft?   Yes_____   No_____

12. Is there a timeout feature?   Yes_____   No_____

13. Is there a statement on useful security hints?   Yes_____   No_____

14. Is the security policy easy to read and understand? Yes_____   No_____

   Reason for conclusion_____
   _____
   _____
   _____