PUBLISHED SECURITY POLICIES OF WEB SITES OF GLOBAL BANKS OF MEXICO, CENTRAL & SOUTH AMERICA, CANADA AND THE U.S.

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 three-year period. The first phase emphasized the privacy policies of global banks and other businesses engaged in E-commerce [5, 6, 7]. 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 160 banks representing Mexico [20], Central and South America [40], Canada [40], and the U.S. [60].

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

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.

RESULTS

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.

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

Pages	Mexico	C & S.A.	Canada	U.S.
0	2	8	0	1
1	6	21	18	33
2	5	6	8	11
3	1	3	2	3
4	2	1	1	2
5	1	0	4	2
6+	3	1	7	8

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 Canadian banks relied on much more detail than the others in stating their security policies on a proportional basis.

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

Level of Detail?	Mex n=20	C & S.A. n=40	Ca n=40	U.S. n=60
Very Detailed	7 35%	6 15%	19 n=48%	18 n=30%
Not Technical	6 30%	22 55%	9 n=22%	30 n=50%
Skimpy	7 35%	12 30%	12 n=30%	12 n=20%

Table 3 shows that the Canadian and U.S. banks were more likely than the Central and South American banks to 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?	Mexico	C & S.A.	Canada	U.S.
Yes	11 55%	23 58%	38 95%	47 78%
No	9 45%	17 42%	2 5%	13 22%

Table 4 illustrates very clearly that the Canadian 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 is on how and what the banks communicate on their web pages.

Table 4. Policy Statement on Encryption of Data During Transmission

Trans-mission Encrypt of Data?	Mexico n=20	C & S.A. n=40	Ca n=40	U.S. n=60
Yes	9 45%	8 20%	30 75%	39 65%
No	11 55%	32 80%	10 25%	21 35%

Table 5 shows that none of the regions' banks 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 Encrypt of Data?	Mexico n=20	C & S.A. n=40	Ca n=40	U.S. n=60
Yes	5 25%	3 8%	13 33%	15 25%
No	15 75%	37 92%	27 67%	45 75%

Table 6 again shows that the Canadian and U.S. banks are more explicit in their statements regarding who has access to their customers' data. Both Mexico and the other Central and South American banks seem to follow the same approach to reporting this type of information.

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

Access to Data Statement?	Mex. n=20	C & S.A. n=40	Ca n=40	U.S. n=60
Yes	5 25%	19 48%	27 68%	41 68%
No	15 75%	21 52%	13 32%	19 32%

Table 7 shows that none of the regions' banks are more likely to explicitly state that firewalls are employed as an integral part of their network security policy. However, the Central and South American banks are less likely to comment than the North American banks.

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

Firewall Comment?	Mex. n=20	C & S.A. n=40	Canada n=40	U.S. n=60
Yes	4 20%	5 13%	18 45%	24 40%
No	16 80%	35 87%	22 55%	36 60%

Table 8 illustrates very emphatically that North American banks do a more explicit job of reporting on the use of logs, audits and monitoring actions than do the other two regions.

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

Logging, Auditing, Monitoring?	Mex n=20	C & S.A. n=40	Ca n=40	U.S. n=60
Yes	3 15%	8 20%	15 38%	21 35%
No	17 85%	32 80%	25 62%	39 65%

Table 9 shows that the North American banks were overwhelmingly more likely to state that passwords

were required to use the site. The rate declined the farther south you went.

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

Is Password Required?	Mex n=20	C & S.A. n=40	Ca n=40	U.S. n=60
Yes	10 50%	8 20%	35 88%	57 95%
No	10 50%	32 80%	5 12%	3 5%

Table 10 clearly distinguishes the security reporting policy of the Central and South American Banks when compared to the other two regions' banks.

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

Is User Login Required?	Mex n=20	C & S.A. n=40	Ca n=40	U.S. n=60
Yes	11 55%	7 18%	30 75%	56 93%
No	9 45%	33 82%	10 25%	4 7%

Table 11 shows that the banks in Central and South America are the least likely to explicitly report the use of SSL on their web sites. Whereas, both the U.S. and Mexico have the highest proportional rate followed by Canada.

Table 11. Does the Site State That it Uses SSL?

Use of SSL?	Mex n=20	C & S.A. n=40	Canada n=40	U.S. n=60
Yes	15 75%	8 20%	29 73%	52 87%
No	5 25%	32 80%	11 27%	8 13%

Table 12 shows that the vast majority of banks studied do not include a glossary of terms on their web sites. Mexican banks had the highest percentage at one third.

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

Is There a Gloss-ary of Terms?	Mex n=20	C & S.A. n=40	Ca n=40	U.S. n=60
Yes	5 25%	0 0%	8 20%	5 8%
No	15 75%	40 100%	32 80%	55 92%

Table 13 illustrates that North American Banks are more explicit in warning customers about the possibility of identity theft. The banks of Mexico and Central and South America report about 10 percent having statements on identity theft on their web sites.

Table 13. Is There a Statement on Identity Theft?

State-ment on Identi-ty Theft?	Mex n=20	C & S.A. n=40	Ca n=40	U.S. n=60
Yes	5 25%	1 3%	28 70%	31 52%
No	15 75%	39 97%	12 30%	29 48%

Table 14 shows that most banks, by a wide margin, do not state the existence of a timeout feature. The only region that had more than fifty per cent reporting was Canada.

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

Is There a Timeout Feature?	Mex n=20	C & S.A. n=40	Ca n=40	U.S. n=60
Yes	3 15%	1 3%	23 58%	12 20%
No	17 85%	39 97%	17 42%	48 80%

Table 15 shows that the North American banks are much more inclined to have a section of their web sites devoted to security tips and that inclination decreases the farther south you go.

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

State-ment on Secur-ity Tips?	Mex n=20	C & S.A. n=40	Canada n=40	U.S. n=60
Yes	11 55%	7 18%	34 85%	34 57%
No	9 45%	33 82%	6 15%	26 43%

Table 16 summarizes quite effectively the fact that the North American banks' web sites appear to be more thorough in their content as well as being easier to read and comprehend.

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

Easy to Read & Under-stand?	Mex n=20	C & S.A. n=40	Canada n=40	U.S. n=60
Yes	13 65%	28 70%	40 100%	58 97%
No	7 35%	12 30%	0 0%	2 3%

SUMMARY AND CONCLUSIONS

The focus of this paper 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. From the data in this study, it appears that the banks in both Canada and the U.S. make a greater effort at explicitly reporting the security policies that are in place. Banks in Mexico also seem to be more explicit in their reporting than those in Central and South America. 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[9].

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 [2]. "U.S. banking regulators have given the nation's banks an end 2006 deadline to introduce multi-factor authentication for high risk Internet transactions" [3]. This increased security should also manifest itself in an increased level of communication to the banks' customers [10]. Global banks just cannot afford malicious attacks on their customers' financial information [1]. 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" [8]. 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 [4].

REFERENCES

1. Acohido, B. & Swarz, J. (2005). Cyber Cracking, *The Journal News*, Nov. 7, D1-D2.
2. Bank, D. & Conkey, C. (2005). New Safeguards for Your Privacy, *Wall Street Journal,* March 24, D1.
3. Ekers, J. (2005). It's All in the Cards, *Security Products*, December, 34-37.
4. Lamont, J. (2005). Predictive Analytics: An Asset to Retail Banking Worldwide, *KM World*, November/December, 16,17,27 or http://www.kmworld.com/Articles/ReadArticle.aspx?ArticleID=14587.
5. Moscato, D. & Robinson, B. (2002). The Global Race to Compliance: Information Privacy in an Electronic Commerce Framework, *Comm. of the IIMA, 2*(4), 111-120.

6. Moscato, D. (2003). An Empirical Analysis of Web Site Privacy and Security By Industry, *Issues in Information Systems*, *4*(1), 264-270.
7. Moscato, D. & Moscato, E. (2004). An Assessment of Privacy and Security Policies of Global Financial Institutions, *Proc. of Third Int'l Bus. and Econ. Con*.,2004.
8. Myers, R. (Fall 2005). How Global is your Bank? *CFO Banking and Finance*, 24-30 or http://www.cfo.com/article.cfm/5009997/c_5038012?f=insidecfo.
9. Rompei, A. (2005). The World's Best Internet Banks, *Global Finance*, Sep, 31-35.
10. Vijayan, J. (2003). New Privacy Rules Could Mean Headaches for Financial Services IT, *Computerworld*, August 11, 7.