RISK ASSESSMENT REPORT

LIBR 514 K

APRIL 9, 2018

NISHTHA
17788647

RISK ASSESSMENT REPORT for Scotia Bank Website

Executive Summary

Date of the risk assessment: During the period of March 30, 2018 - April 9, 2018, an information security risk assessment was conducted for the desktop website of The Bank of Nova Scotia with URL **http://www.scotiabank.com/ca/en/0,,2,00.html**. The Bank of Nova Scotia, operating as Scotiabank, is a Canadian multinational bank. [1] The assessment has identified several risk items that can help the management to strengthen their website's internet security.

Purpose of the risk assessment: The purpose of this risk assessment report is to provide the management with information related to security of the website in the cyberspace. This report lists threat models & sources, vulnerabilities, probability, impact, and the likelihood of impact of threats to the website. This report will assist the management in taking decisions with regards to the online security of the website which is an important information component in their whole business structure. The bank needs to uphold all principles of the CIA (Confidentiality, Integrity, Availability) triad for the services provided by their website to the customers. This report evaluates the CIA principles against the threats to the website. This report addresses the impact that the website, as an information system, has on the banking operations for the business unit.

The scope of the risk assessment: The scope of this risk assessment report is restricted to evaluation of the online security of desktop website of Scotia Bank. This report has been conducted on all the information available on the official bank website and the documents made public by the bank related to their online security policies. This research includes any news reports or events about the online security of the website. This risk assessment is applicable only to the current version of the live website. It does not include the mobile banking application or telephonic services provided via the website. Also, the analysis has been conducted with a customer viewpoint which includes web services available to the customers with an online account.

- Access: Customer Account Access
- Network: SHAW Wi-Fi Home Network
- Information system name and URL: http://www.scotiabank.com/ca/en/0,,2,00.html
- Security categorization: Desktop website
- Browser: Google Chrome
- Information system (i.e., authorization) boundary: Bank user/ Customer
- Target Audience: Bank Management. Client Impact is being measured in terms of any breach

This is an initial risk assessment. The overall level of risk for the desktop version of the website is **HIGH**. The numbers of risks identified for each level of risk are listed below.

Very Low	2
Low	4
Medium	2
High	5
Very High	2

Body of the Report

1. **Purpose of the risk assessment**

   The purpose of this risk assessment is not only to highlight the risks associated with the website but also to suggest mitigation strategies (and best practices, wherever applicable) which, if employed, will reduce risk through the website for the business. However, this report is not entirely comprehensive of all threats and vulnerabilities to the IS, this assessment includes any known risks related to the NIST SP 800-30 standards selected for this system. This document can be updated after testing to include any vulnerabilities or observations by the independent assessment team. Data collected during this assessment may be used to support higher-level risk assessments at the mission/business or organization level.

2. **Identify assumptions and constraints**:

   Uncertainty in assumptions can affect organizational risk tolerance. Table D-2 from NIST 800-30 has been used as a base to identify threat sources. Since proper authorized access was not available to the technical details related to the website such as security measures in control, cryptographic mechanisms deployed, network security measures, data center and backup system, this risk assessment report does not include the initiatives undertaken by the management to secure their online systems. No related report was available online, which in fact is a good measure as audit or configuration reports have sensitive details which have the capability to make the system even more vulnerable.

3. **Risk tolerance inputs to the risk assessment:**

   Risk tolerance is the amount of risk that a business can take in comfortably. It is the capacity to withstand risks without panicking. However non- tangible aspects are also related to risk tolerance such as reputational damage or loss of goodwill in case a risk actuates to a successful attack. Appropriate business context is not available and authorized access is not granted so no concrete statement can be made about risk tolerance for the information system under analysis.

4. **Risk model and analytic approach:**

   This risk assessment follows a Qualitative Approach. This approach is used in because it is difficult to express a numerical measure of risk involved for a bank website with a customer access. This risk analysis is without adequate information and numerical data. So, this analysis can be used as an initial assessment to recognize the risk. [4]

THREAT LIKELIHOOD

- High: The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective

- Medium: The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.

- Low: The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

MAGNITUDE OF IMPACT

- Very High: The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.

- High: The threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

- Moderate: The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals' other organizations, or the Nation.

- Low: The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals' other organizations, or the Nation.

- Very Low: The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals' other organizations, or the Nation.

5. Rationale for risk-related decisions during the risk assessment process:

The risk assessment is being conducted for business management to understand the risks and vulnerabilities related to the website. The rationale behind risk decisions has been done from perspective of client impact i.e. how severe would the client be impacted in case any risk culminates to a successful attack.

6. Uncertainties within the risk assessment process:

The uncertainties within the risk assessment process can be contributed to the lack of information available to make sound decisions. This report does not include any numerical or historical data nor does it have details about the technology and controls already in place by the business. This report can be used as a best practice guideline and can assist the management in bridging the gaps at places where appropriate security controls have not been set up.

7. Risk assessment results

S.No	Risk Name/Num	Description	Probability	Impact	Overall	Mitigation
1	Data Breach [6]	Private individual data, from email addresses to social security details to credit card numbers, are at risk of getting into the wrong hands.	HIGH	HIGH	HIGH	One way to improve protection against data breaches is end-to-end encryption.
2	DDoS Distributed Denial Of Service	Adversary can use multiple compromised information systems to attack a single target, thereby causing denial of service for users of the targeted information systems.	HIGH	HIGH	HIGH	One way to protect the information system is to incorporate load balancing and failover solutions, which distributes

						traffic across several machines and bypasses downed servers.
3	Unauthorized Access	This risk is present when access to information system is not limited to authorized users. There can be entities acting on behalf of authorized users, or devices.	LOW	HIGH	MEDIUM	Enforced 2 or 3 factor authentication can prevent instances of unauthorized access.
4	Principle of Least Privilege	This risk is present when the Information system access is not limited to the types of transactions and functions that authorized users are permitted to execute.	LOW	LOW	LOW	Privileges should be assigned ona need-to-know basis. Minimum access should be granted to carry out the task or avail a service. Regular audits should be carried out to ensure that overdue or unauthorized accesses are revoked.
5	Separation of Duties	This risk is present when the Separation the duties for individuals is not implemented to reduce the risk of malicious activity without collusion.	VERY LOW	VERY LOW	VERY LOW	More than one person should be required to complete a task. This enforces internal control which prevents fraud or error.
6	Banking Trojans	Banking systems are susceptible to malicious programs which attempt to obtain confidential information about customers and clients using online banking. They focus on stealing bank account logins.	MEDIUM	HIGH	HIGH	All data should be backedup and encrypted. User should be made aware not to download email attachments which seem to ask confidential information nor should they provide such details on any login field of website.
7	Counterfeit/Spoof website.	Adversary can create duplicates of a legitimate websites. When users visit a counterfeit site, the site can gather information or download malware.	VERY HIGH	VERY HIGH	VERY HIGH	Packet filtering must be used to inspect packets before transmitting them to a network. Organizations should crawl the web with spoofing detection software to identify presence of counterfeit websites.
8	Phishing	In this case the attacks occur via email, instant messaging; commonly directing users to websites that appear to be legitimate sites, while actually stealing the entered information.	VERY HIGH	VERY HIGH	VERY HIGH	Users should be made aware to avoid clicking on hyperlinks within email communications. User should type the URL into the

						web browser instead. Suspicious attachments should not be downloaded. Instruct employees not to use business computers and workstations for non-business activities, such as web browsing or checking personal email.
9	Deliver known malware	In this risk the adversary uses common delivery mechanisms (e.g., email) to install/insert known malware (e. g., malware whose existence is known) into organizational information systems.	LOW	MEDIUM	VERY LOW	Users and employees should be made aware to avoid clicking on hyperlinks within email communications.
10	Insert malicious scanning devices (e.g., wireless sniffers) inside facilities.	In this risk the adversary uses postal service or other commercial delivery services to deliver to organizational mailrooms a device that is able to scan wireless communications accessible from within the mailrooms and then wirelessly transmit information back to adversary.	LOW	LOW	LOW	All the deliveries should be verified with the person whose name is on receiving address. Also all removable media and hardware component should be tried and tested on non business setup first.
11	Exploit vulnerabilities using zero-day attacks.	In this risk the adversary employs attacks that exploit as yet unpublicized vulnerabilities. Zero-day attacks are based on adversary insight into the information systems and applications used by organizations as well as adversary reconnaissance of organizations	LOW	HIGH	LOW	This risk can actuate into threat only if adversary has insider access and confidential details about the security set up of information system.
12	Conduct communications interception attacks.	In this risk the adversary takes advantage of communications that are either unencrypted or use weak encryption (e.g., encryption containing publically known flaws), targets those communications, and gains access to transmitted information and channels.	EDIUM	HIGH	MEDIUM	The most important way to improve protection against interception is end-to-end encryption to both data in transit and data at rest.
13	Cyber-physical attacks on organizational facilities.	Adversary conducts a cyber-physical attack on organizational facilities (e.g., remotely changes HVAC settings).	LOW	LOW	LOW	This can be mitigated by enforcing authorized access at every physical layer and at trust boundary of system.
14	Conduct brute force login attempts/password guessing attacks	In this risk the adversary attempts to gain access to organizational information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.	HIGH	HIGH	HIGH	Number of failed login attempts should be limited. Account lockout can delay the hack. CAPTCHA can be used to prevent automated

						attacks.
15	Social engineering to obtain information.	Externally placed adversary takes actions (e.g., using email, phone) with the intent of persuading or otherwise tricking individuals within organizations into revealing critical/sensitive information	HIGH	HIGH	HIGH	If the system is designed with an awareness of the dangers of social engineering in mind, the cases where one might be tempted to succumb to a social engineering attack — such as trying to work around an inconvenience in how the system works or give in to arguments of authority — can be obviated before they even arise.[7]

Table E-2 from NIST 800-30 has been used as a guidance tool to identify the threat events related to the information system under analysis. Risks corresponding to the related threat events have been summarised above.

8. **Time frame validity for the risk assessment:** This risk assessment is valid to support decisions related to online security of website till the time any concrete implementation changes are made to website. The time frame is till the time the current website (as of April 9, 2018) is available to users in current version.

Appendices

1. This risk assessment has been conducted individually as the part of graduate course requirement.
2. All risk assessment source information tables and any supporting evidence have been listed below (e.g., Tables from NIST 800-30)
3. See below for list of references and sources of information.

References:

[1] "Scotiabank." *Wikipedia*, Wikimedia Foundation, 6 Apr. 2018, en.wikipedia.org/wiki/Scotiabank.
[2] "Security Centre." *Security Centre | Scotiabank*, www.scotiabank.com/ca/en/0,,352,00.html.
[3] "Home." *HOME*, cissp.com/security-assessments/online-banking-assessment.
[4] Stoneburner, Gary, et al. "SP 800-30, Risk Management Guide for Information Technology Systems." *Author: Gary Stoneburner (NIST)*, csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01.
[5] "Performing a Security Risk Assessment." *Performing a Security Risk Assessment*, www.isaca.org/Journal/archives/2010/Volume-1/Pages/Performing-a-Security-Risk-Assessment1.aspx

[6] *Tech in Asia - Connecting Asia's Startup Ecosystem*, www.techinasia.com/talk/5-threats-website-security-2016.
[7] Perrin, Chad. “Mitigating the Social Engineering Threat.” *TechRepublic*, www.techrepublic.com/blog/it-security/mitigating-the-social-engineering-threat/.

Supporting sources of Information from NIST 800-30:

- Table D1-D8 from NIST 800-30
- Table E1-E5 from NIST 800-30
- Table F1-F6 from NIST 800-30
- Table H2-H4 from NIST 800-30
- Appendix K from NIST 800-30 for structure of Risk Assessment Report