Risk Analysis Report of Data Breaches in BOA & FIS

By: Shivani Gautam

Industry:	Bank & Financial Services
Region of Focus:	US
Attribution:	High Confidence
Records:	First & last name exposure of company employees.
Scenario:	Social Engineering attacks

INTRODUCTION:

36th Annual conference by an organization of Risk Managers (RMA Group) posted details of attendee's which included first and last names of employee's which caused problem as they deal with sensitive information.

In this risk assessment report, risk managers of company C1-BOA and C2-FIS attended the conference and assessment is carried out for calculating how much risk and a company is vulnerable to risk.

"How first name & last name exposure, be a threat to company?"

First thought comes by an email id;

- If taken example of MNSU college mail: Shivani.Gautam@mnsu.edu; i.e. first & last name have been used, which can be used to attain other phone no, address, email accounts can be hacked, or even financial (transfer of money using id via linked accounts); easiest ones we can think of.
- Hacker can do much more by diving deep.

Assessment:

Using FAIR tool, analysis based on factors: Threat event frequency (TEF), primary losses, secondary losses and secondary loss magnitude with secondary loss event frequency, vulnerabilities have been obtained for both scenarios.

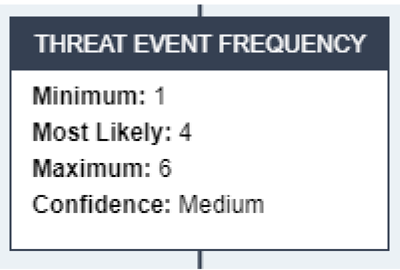
Results:

Accordingly obtained results have been laid down in the report and due to higher number of TEF, a higher loss exposure and enforced controls lead to higher loss amount as well as vulnerability from these attacks in BOA & FIS. These companies are both related to bank and finance and exposure can lead to huge amount of loss.

C1: Data Breaches in Bank of America
Threat actor: Non-state actor
Threat effect: Confidentiality, Integrity, Availability

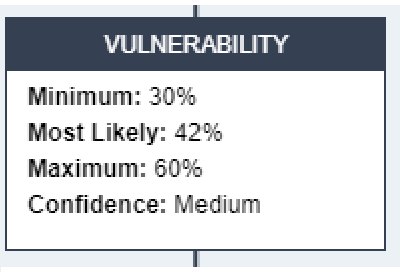
The Bank of America Corporation (abbreviated as BoA): American multinational investment bank and financial services company based in Charlotte, North Carolina with central hubs in New York City, London, Hong Kong, and Toronto. Bank of America was formed through NationsBank's acquisition of BankAmerica in 1998. It is the second largest banking institution in the United States, after JP Morgan Chase.

Rationale: Considered 4 times a day because of the threats and the amount spent and according to the reports* collected how much vulnerable the financial company is towards social engineering attacks.



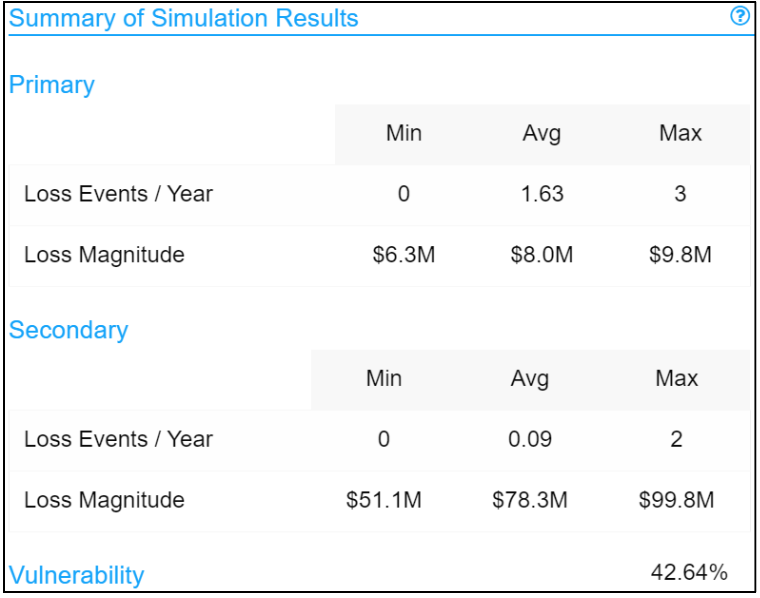
THREAT EVENT FREQUENCY

Minimum: 1
Most Likely: 4
Maximum: 6
Confidence: Medium



VULNERABILITY

Minimum: 30%
Most Likely: 42%
Maximum: 60%
Confidence: Medium



Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	0	1.63	3
Loss Magnitude	$6.3M	$8.0M	$9.8M

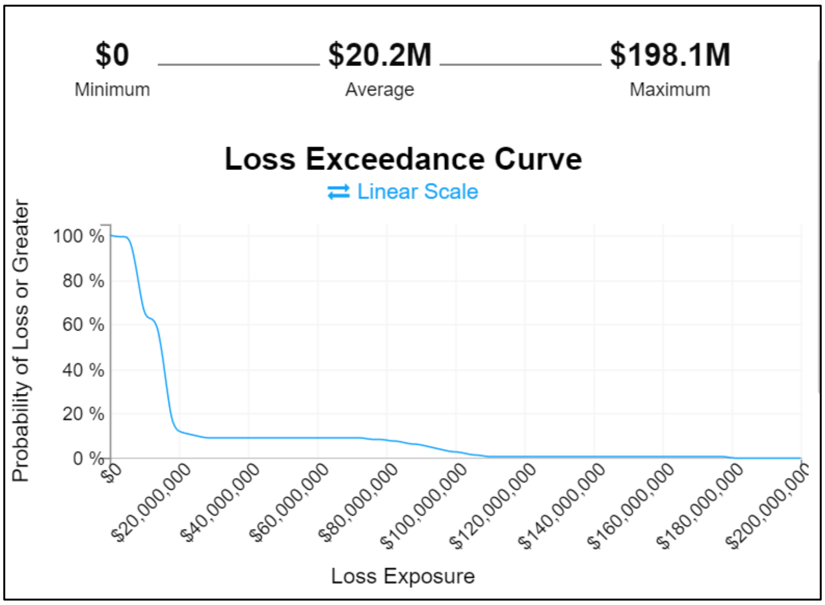
Secondary

	Min	Avg	Max
Loss Events / Year	0	0.09	2
Loss Magnitude	$51.1M	$78.3M	$99.8M

Vulnerability 42.64%

Assumption: Analysis using the data available on internet and reports about the TEF and vulnerabilities faced by BOA, is considered as a fact that happened because of exposure of employee's data as per the scenario of 76% card breaches for data.**

Risks



Company:	Bank of America
Valuation:	$288,050,000,000
Employees:	204,490
Location:	United States

Recommendations:

- Access privileges
- Securing email gateways
- Patching & Configuration
- Policies and Authentication

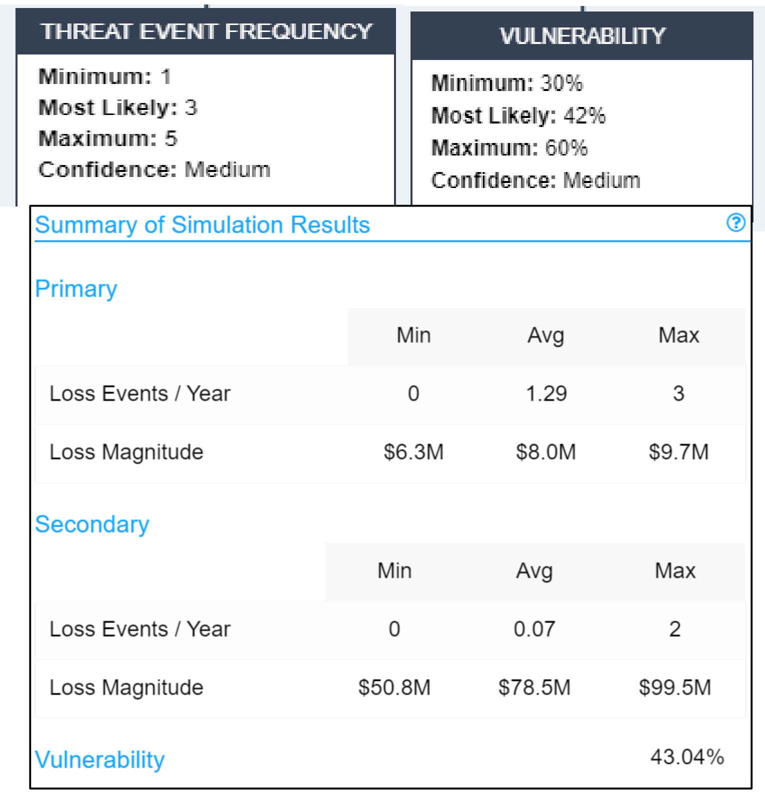
Vulnerability 42.64%

* https://www.bankinfosecurity.com/bank-america-responds-to-breach-a-4487
** https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide

C2: Data Breaches in Fidelity National Information Services
Threat actor: Non-state actor
Threat effect: Confidentiality, Integrity, Availability

Fidelity National Information Services, Inc. (FIS) is a financial services technology company. The Company operates through three segments: Integrated Financial Solutions (IFS), Global Financial Solutions (GFS), and Corporate and Other. It is focused on serving the North American clients for transaction and account processing, channel solutions, digital channels, risk and compliance solutions, and services. and the financial institutions, international financial institutions with a range of capital markets and asset management and insurance solutions.

Rationale: Considered four times a week because of the threats and the amount spent in years like 2012,2013 and according to the reports** collected how much vulnerable the financial company is towards social engineering attacks.



THREAT EVENT FREQUENCY

Minimum: 1
Most Likely: 3
Maximum: 5
Confidence: Medium

VULNERABILITY

Minimum: 30%
Most Likely: 42%
Maximum: 60%
Confidence: Medium

Summary of Simulation Results

Primary

	Min	Avg	Max
Loss Events / Year	0	1.29	3
Loss Magnitude	$6.3M	$8.0M	$9.7M

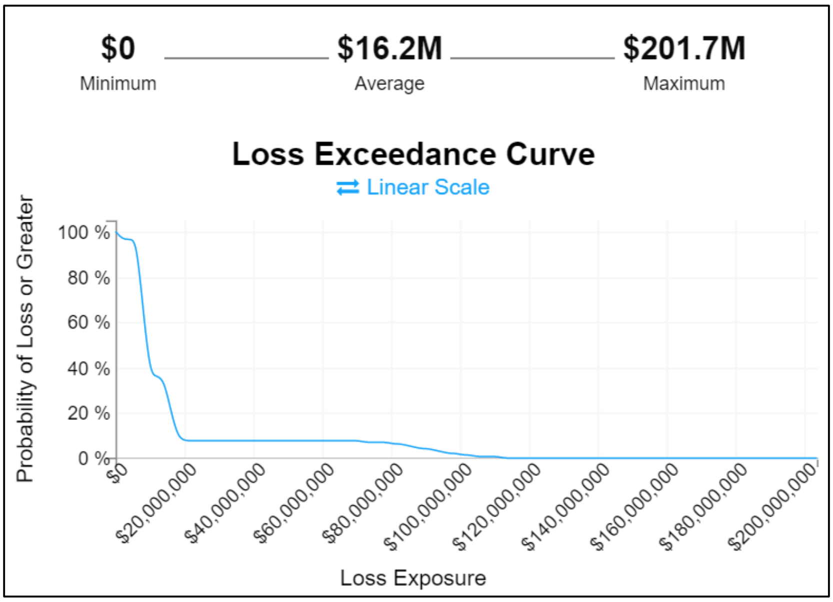
Secondary

	Min	Avg	Max
Loss Events / Year	0	0.07	2
Loss Magnitude	$50.8M	$78.5M	$99.5M

Vulnerability 43.04%

Assumption: Analysis using the data available on internet and reports about the TEF and vulnerabilities faced by FIS, is considered as a fact that happened because of exposure of employee's data as per the scenario*.

Risks



$0	$16.2M	$201.7M
Minimum	Average	Maximum

Loss Exceedance Curve

Company:	FIS
Valuation:	$30,830,000,000
Employees:	53,000
Location:	United States

Recommendations:

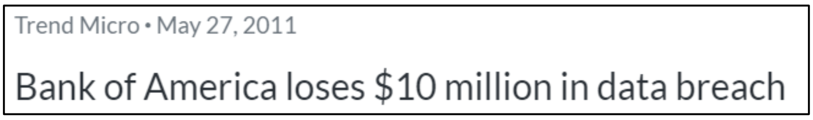
- Access privileges
- Securing email gateways
- Patching & Configuration
- Policies and Authentication

Vulnerability 43.04%

* https://www.firemon.com/real-world-breach-shows-prioritizing-vulnerabilities-matters/
** https://krebsonsecurity.com/2013/06/fdic-2011-fis-breach-worse-than-reported/#more-20876

RESEARCHES:

RESEARCHES FOR BANK OF AMERICA:

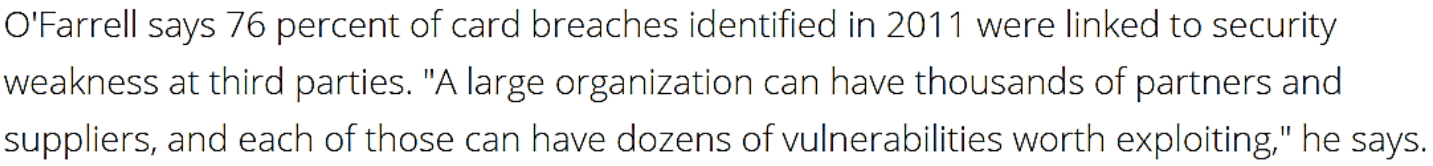


Trend Micro • May 27, 2011

Bank of America loses $10 million in data breach

DNSSEC not enabled

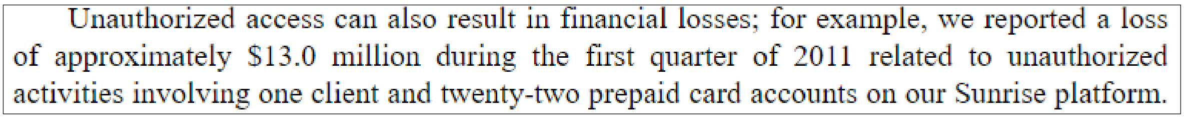
Source: https://www.upguard.com/security-report/bankofamerica



O'Farrell says 76 percent of card breaches identified in 2011 were linked to security weakness at third parties. "A large organization can have thousands of partners and suppliers, and each of those can have dozens of vulnerabilities worth exploiting," he says.

Source: https://www.bankinfosecurity.com/bank-america-responds-to-breach-a-4487

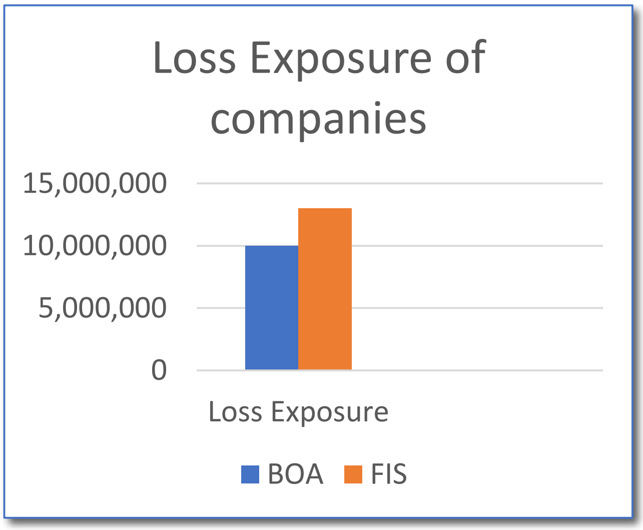
RESEARCHES FOR FIS:

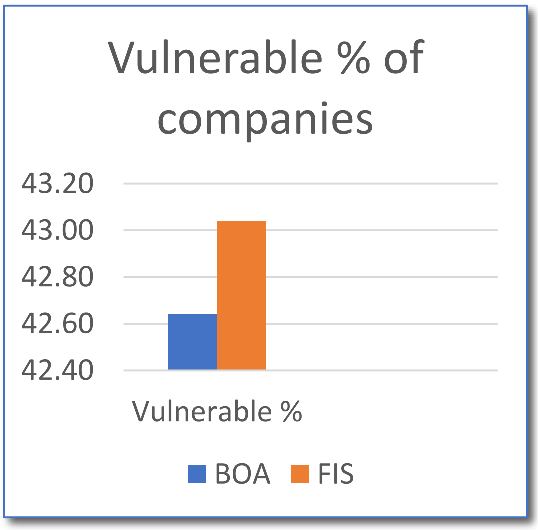


Unauthorized access can also result in financial losses; for example, we reported a loss of approximately $13.0 million during the first quarter of 2011 related to unauthorized activities involving one client and twenty-two prepaid card accounts on our Sunrise platform.

Source: https://www.sec.gov/Archives/edgar/data/1136893/000113689312000017/fis-201112312011.htm

C1 & C2 : Comparison & Similarities





Both BOA & FIS Inc. facing data breaches in the years of 2011-13 having similar percentage of loss because of different social engineering threats faced by the company where one of the factor was exposure of company employee's name. We obtained the average annualized loss exposure summing up more the number of participants of the conference more vulnerable including other threats and attacks according to the reports accessed.