CLOUD COMPUTING AND INFORMATION SECURITY IN BANKING

Dominique Louis, Pace University, Seidenberg School of Computer Science and Information Systems,
163 Williams Street, New York, N.Y. 10038, 212-346-1687, capital402000@yahoo.com

ABSTRACT

In the digital revolution that continues to evolve, highly effective web-related technologies become more ubiquitous, diffusing every organizational level. The paper focuses on the current banking environment, where the adoption of cloud computing solutions provides a great deal of flexibility and a wider variety of services, but, breeds an excellent environment for security violations with profound implications on organizational image. Threats, defenses, and regulation are discussed, while some questions for further study are also comprised.

INTRODUCTION

Financial institutions have always used information technology as a technical wherewithal to achieve competitive advantage and differentiate themselves in the market place. In the contemporary landscape, banks espouse the internet-related capabilities that integrate disparate external sources of service into robust heterogeneous networks, as scheme to accommodate core functionality requirements beyond organizational boundaries. Admittedly, a new prototype evolves that unleashes unanticipated concerns associated with security breaches, financial loss, and reputational damage. The paper objectives align Background, Advantage, Risks, Threats, Violation Techniques, Proactive Defense Mechanisms, Notable Breaches, Survey Findings, Federal Regulation, The COBIT Framework, Suggested Measures, Building a Security Edifice, and Future Directions. The research type is purely descriptive.

BACKGROUND

Incipiently, organizations encompassed compiled software applications to enhance their industry share. Progressively, providers emerged who developed, installed, and maintained internal viable architectures to support and facilitate resilient and reliable operations. Yet, technology proliferates and matures, causing natural inevitable decay of systems. In the existing globally interconnected corporate climate, the explosive growth trajectory of outsourced services obscures proprietary infrastructures that become operationally inadequate and outdated. [6]

ADVANTAGE

The core benefit of encapsulating cloud computing applications as a path to organizational efficiency is attributed to the enormous ***cost-effectiveness advantage*** they yield, which empowers firms to implement superior-technology standards at reduced costs, with no extra resources, or hardware requirements. [6]

RISKS

Cloud computing entails risks that revolve around three elements: **Privacy** (Integrity of information), **Availability** (Data accessibility), and **Obsolescence/Outdated Systems** (Operationally stalwart IT infrastructures). Consequently, it is of utmost significance for banks and other organizations to remain eternally vigilant of risks that might compromise their information resources and assets, such as *Continuous dependency on third-party providers, Loss of control over data environment (physical or logical), No data availability should service is interrupted by provider, Liability (privacy and legal) when security breaches occur*, *Data locations not obviously defined*, *Data interference (meddling),* and *Challenges in the protection of trade secrets*. [6]

THREATS

Technical innovations facilitate rogue penetration by outsiders to the core of how organizations perform their functions. Hence, the not-for-profit Cloud Security Alliance highlights important threats that stem from *Unlawful use, Flawed application programming interfaces, Data loss and leakage*, *Account, service and traffic interception*, and *Shared technology vulnerabilities*. [6] Essentially, a great deal of the cyber attacks increase in the banking industry derives from **mobile banking** devices – particularly smartphones – combined with owners' frequent negligence to install the most basic security features, such as phone locking with a code. [4] Arguably, smartphones are considered *entryways* to sensitive information, since they create environment for attacks. For that reason, Google assessed the removal of 22 deficient Android applications from its framework in December 2011. [14] **Card processing firms** also constitute a vulnerable nerve center for cybercrime, since they concoct raw data converged from various retailers and banks. [8] In the business environment, **insiders** such as *system administrators* as well as those with *privileged access credentials* pose greater potential risk for security abuses of all types of organizational employees for two reasons. Administrators might violate organizational policy when – challenged by user demands – they connect printers on network segments where not permissible. In addition, disgruntled database, network or system administrators may turn nefarious by intercepting data, embedding logic bombs, or granting themselves system access beyond their entitlements. [10]

VIOLATION TECHNIQUES

Social engineering, or **phishing** or **spear-fishing** is the method to defraud online bank customers into taking a particular action, or divulging critical information. [13] Besides, miscreants have invented an *intrusive software* called Zeus bot, or Zeus Trojan that disguises its activity to appear like legitimate traffic, aiming to seize user's information and gain entry into users' banking applications. Once installed Zeus quietly intercepts passwords, account numbers, and other information required to log into online banking systems. It is worth noting that the stealthy program defeats banking authentication processes, because it becomes inactive *only after* the user has entirely signed in to ensure total login validity [12]

PROACTIVE DEFENSE MECHANISMS

Basic security standards encompass the use of **strong passwords**, consisting of eight or more upper and lower case, numeric and special characters that *should not be shar*ed, but, *be frequently changed*, especially after employee termination. Additionally, employees should be *disallowed* to access personal e-mails, *visit* unauthorized Web sites, or *download* unauthorized applications. Lastly, *virus* and *malware protection programs* should be installed, while employee behavior should be *prescribed* by providing organizational security procedures. [12] **Security Information and Event Management (SIEM)** systems are technological advancements of highly configured statistical algorithms that reconnoiter huge quantities of network events from their internal or external point of origin, and isolate suspicious activity by correlating the interrelationships of those events. Thus, SIEMs are justifiably deemed successful cost-effective investments, as they enable significant reduction of security losses that subsequently increases enterprise revenues. [7] To inhibit hostile takeovers of customer accounts by external intruders, banks enforce **strong multi-factor authentication** controls to make discovery of obscure hidden connections with customer accounts exceedingly difficult to succeed. [2] Notably, Bank of America applies a multi-layered security platform called Phishing Net where *different controls at different points converge in a transaction process, so that control weaknesses compensate for by each other's strength*. [5] In the same sphere, the C*alledPhoneFactor* procedure used by United Bank and Trust in Ann Arbor, Michigan places phone calls to customers who process high-risk online American Clearing House (ACH) transactions to verify their authenticity. Alternatively, banks decisively **disable customer online access** once fraudulent behavior is detected. [9] With respect to **insider risks**, the Trustware Smart Tag Data Control has been endorsed by the American Banking Association as a platform *to protect data stored rather than protecting the devices through which data traverse*. [1] Lastly, it is vitally important that **IT Operations** are designed with *separation of duties,* which implies *fragmented concentration of power* in any individual. In extension, IT employees should be assigned *no* entry level to the actual monitoring feature, thus, *no* capability to disable/enable the crucial mechanism per their convenience. [10]

NOTABLE BREACHES

In 2009, the card processing firm Heartland Payments Systems experienced a breach that may have affected 100 million cards, having paid close to $140 million in fees to the credit card companies. In May 2011, 360,000 Citigroup accounts were breached and almost 220,000 cards were replaced. In August 2011, two breaches at Citigroup's Japanese card unit center compromised customer information, but, no personal identification numbers and card security codes that the bank was able to protect. [11]

SURVEY RESULTS

The **Financial Services Information Sharing and Analysis Center (FS-ISAC)** that coordinates with the Department of Homeland Security on security issues, released findings of an American Bankers Association survey that encompassed 95 financial institutions and 5 service providers. In 2011, the total number of attacks targeted to seize control of bank accounts was increased to 314 as opposed to 239 in 2010, and 87 in 2009. [9] Also, a Javeline Strategy and Research identity fraud study found that 32% of Smartphone owners do not update to a new operating system when it becomes available, 62% do not use a password on their home screen, and 32% save login information on their device. [4] In contrast, a survey for online banking security conducted by the global domain registrar Melbourne IT in November 2011 found that 47% of U.S. consumers check that the online site looks familiar, 46% look for a padlock symbol on the web browser, 45% read the web address at the top to make sure it is correct, 42% look for an https:// in front of the URL, 6% do nothing, and 15% do not use online banking. [3]

FEDERAL REGULATION

The **Federal Financial Institution Examination Council (FFIEC)** has issued the *Authentication in an Internet Banking Environment Guidance* in October 2005, with a supplement to it on June 28, 2011, which assembles a comprehensive **risk management** protocol for financial institutions based on three needs: *Performing risk assessments, Implementing effective strategies for mitigating identified risks,* and *Raising customer awareness of potential risks*. Therefore, banks are expected to conduct frequent **risk assessment*s*** enforcing **layered security** application*s* to identify risks, such as *Detect and respond to suspicious activity, Control administrative functions, Identify devices,* and *Use sophisticated challenge questions (back-up).* In addition, customers should become aware of *Provided and not provided protections*, *Circumstances* under which institutions may have to contact customers, *Suggestions* on how to perform their own risk assessments, and *Institutional Contacts* for security-related issues. [5]

THE COBIT FRAMEWORK

Corporate managers realize the IT contribution in the attainment of optimal organizational performance. The COBIT framework introduced by ISACA is an IT governance toolset that enables organizations to integrate business operations, legislative requirements, and security controls in the quest for greater efficiency. Coalescing around the concept of *control,* COBIT has been widely embraced by banks for its *continuous monitoring and auditing capabilities* as vehicle for fruitful operational efficiency. [Fig. 1,15]

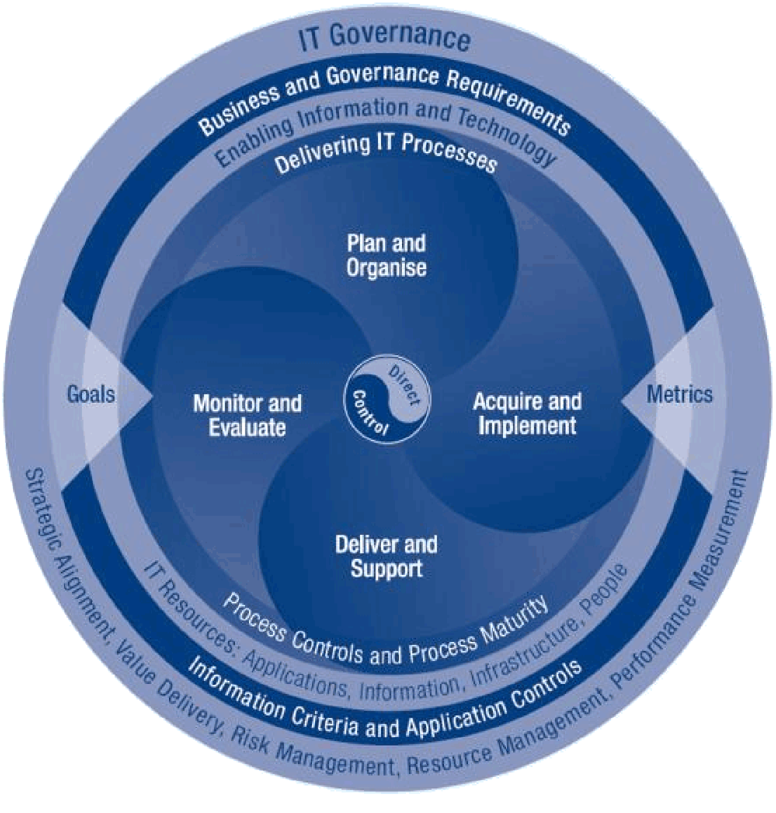
IT Governance
Business and Governance Requirements
Enabling Information and Technology
Delivering IT Processes
Plan and Organise
Goals
Monitor and Evaluate
Direct
Control
Acquire and Implement
Metrics
Deliver and Support
Process Controls and Process Maturity
IT Resources: Applications, Information, Infrastructure, People
Information Criteria and Application Controls
Strategic Alignment, Value Delivery, Risk Management, Resource Management, Performance Measurement

Fig 1, The COBIT Framework

SUGGESTED MEASURES

Security risks necessitate stronger authentication methods, such as *Biometrics, One-Time Passwords and Transaction Codes* known to the financial institution and user, *Security Tokens, Rules-Based Artificial Intelligence* (i.e. authentication scoring), and *Transaction Data Analysis and Scoring*. [12]

BUILDING A SECURITY EDIFICE

Financial institutions continue to evolve incrementally as mobile-based, real-time, and open-access enterprises. Unlike other banking systems, the **mobile payments** vital component is a unique whole value chain with the broadest number of players, since delivery service, phone carrier, physical device security, plus lots of additional partners coherently converge to consolidate seamless output. Therefore, it is significant for banks to *build partnerships with heightened security providers*, since institutions are ultimately held accountable for their partners. [16] It is, also, extremely important for banks to maintain an **information-sharing** and analysis center for information exchange with the industry, *collaboration with the government* and *cross-sector information sharing*, given that a number of cyber attacks are designed to cause multi-industry damage, rather than just financial industry damage. [16] Software **applications** also emerge as challenges to organizational structures, being multi-layered compilations that engulf elements from mainframe, middleware, and end-device domains. As a result, security features should be built upfront in the design phase of program interoperability, while developers should be appropriately educated on how to implement successful configurations. [16] The decisive distinction between *compromised financial data* and *breaches of financial institutions* holds that many of the financial data breaches occur *not within*, but outside financial institutions, yet, with a corrosive effect that negatively impacts their reputational image. Consequently, institutions should establish clear expectations with **third parties** bound to accommodate financial data, while stringent controls should also be enforced to ensure security of data residing outside their borders. [16]

FUTURE DIRECTIONS

Issues for further investigation are:
Question 1: *Can classes of customers be identified whose transactions require higher, specific security measures due to breach likelihood?*
Hypothesis 1: *When special classes of customers are identified whose transactions require higher, specific security measures, banks should apply security controls tailored to those specific needs.*
Question 2: *Does granting system administrators extra authentication privileges impact organizational performance?*
Hypothesis 2: *Granting system administrators extra authentication privileges* ***within their duties*** *increases organizational agility; if* ***beyond duties****, it increases vulnerability to threats.*
Question 3: *Should a bank CEO also be a CIO so as to have total control over IT operations?*
Hypothesis 3: *When a Bank CEO is IT literate and controls the CIO's function, CEO and CIO roles can be fulfilled on separate levels.*

CONCLUSION

Banking institutions strive to provide high-quality financial products and services as a direction to become consistently competitive. Albeit, organizations adopt outsourced cloud computing services in their functionality, the new atmosphere allows security threats to propagate with extreme velocity. To brilliantly manage challenges, banks invest heavily in security architectures intended to reduce losses and prevent threats to information assets from materializing. Yet, most importantly, financial institutions are enforced to adhere to stricter federal controls, aiming to remediate, defend, and suppress intrusions that, aside from financial loss, also cause reputational damage that might be irreparable. Consequently, financial institutions should implement more rigorous controls in accordance with regulatory objectives, so as to retain viability and performance in the increasingly hostile electronic environment.

REFERENCES

[1] ABA Posts Free Communications ToolBox for Bank Members, *ABA Bank Marketing*, June 2011, Vol. 43 Issue 5, p40-40, 2/3p

[2] Crosman, Penny, B of A Steps Up the Fight Against Pesky Foe: Phishers, *American Banker*, Feb. 1, 2012, Vol. 177 Issue 17, p1-3, 2p

[3] Crosman, Penny, Fake Websites Work, *Bank Technology News*, Nov. 2011, Vol. 24 Issue 11, p15-15, 1p

[4] Cyber Attacks are Soaring, How to thwart them, *ABA Banking Journal*, June 2012, Vol. 104 Issue 6, p22-28, 3p

[5] FFIEC Release Supplemental Guidance on Internet Banking Authentication, *Federal Financial Institutions Examination Council*, June 28, 2011 http://www.ffiec.gov/press/pr062811.htm

[6] Ginovsky, John, Clouds in that cloud? *ABA Banking Journal*, April 2011, Vol. 103 Issue 4, P20-24, 49

[7] Graves, Peter, The Invisible Risk-Network Security, *ABA Banking Journal*, June 2, 2011

[8] Greenberg, Andy, Millions of Master Card and Visa Cards Reported Compromised in Processor, *Forbes.com*, March 30, 2012, p30-30, 1p

[9] Messmer, Ellen, Banks: Hackers More Aggressive in Attacking Customer Accounts, *Computer World*, June 14, 2012

[10] Messmer, Ellen, Sys admin gone rogue is biggest insider threat, *Network World*, Sept. 27, 2010, Vol. 27 Issue 18, p11-13, 3p

[11] Notable Data Breaches of 2011, *Bank Technology News*, Sep. 2011, Vol. 24 Issue 9, p25-25, 1/2p

[12] Proctor, Ken, Back to the Future, *Credit Union Management*, April 2011, Vol. 34 Issue 4, p12-14, 3p

[13] Quitter, Jeremy, Hack Attack: Bank Business Customers Best Beware, *American Banker*, May 23, 2012, Vol. 177 Issue 80, p1-5, 2p

[14] Savitz, Eric, 2012 Data Security Trends: A look At The Risks Ahead, *Forbes*.com, Jan 16, 2012, p13-13, 1p

[15] The COBIT Framework, *Information Systems Audit and Control Association (ISACA)* http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

[16] Yurcan, Bryan, The Cybersecurity Imperative: How Banks can Combat Cybercrime, *Bank Systems and Technology Online*, Sept. 4, 2012