RETOOLING CYBERSECURITY AS THE COMPETITIVE ADVANTAGE IN THE FINANCIAL SECTOR

Rajni Goel, Howard University, USA rgoel@howard.edu
Ayodele Mobolurin, Howard University, USA amobolurin@Howard.edu

Abstract

Banks and financial institutions have transformed into sophisticated technology companies that provide financial services as their core business. This digital transformation has added cybersecurity as an increasingly critical management concern in the financial sector for cyber-attacks and fraudulent transactions have become more frequent and widespread. Though traditionally the investments in security have been thought of as a defensive investment, we introduce a new perspective of the value of Cybersecurity investment. We propose that security investments must be leveraged as a competitive advantage and cyber security must be viewed as a strategic asset. If cybersecurity is embedded into the firm as an integral element of the firm's strategy, it can be used to differentiate the firm from its competitors. We present a concept of how financial "technology" institutions can realign their cyber security activities with the firm's strategic objectives and to a competitive advantage.

Introduction

Banks and financial institutions have transformed into sophisticated technology companies that provide financial services as a core business. Traditional services offered by the financial institutions are being disrupted by the financial technology (FinTech) sector. This disruption in the financial industry creates new opportunities for increased speed and agility, innovation and improved information security. The digital data has become a commodity, the primary asset in generating revenue since obtaining, processing, storing and transmitting information is seamlessly embedded in all financial and business processes. Thus, securing this commodity is increasingly a critical management concern in the financial sector as the number cyber-attacks and fraudulent transactions have become more frequent, more severely damaging and more widespread.

Now technology savvy financial organizations now realize that they can use this precise fear of cyber threats to their advantage; they should differentiate themselves from rivals who fail to protect their partner and customer information. Cybersecurity refers to the protection of valuable intellectual property and business information in digital form against theft and misuse. Cyber exposure extends throughout the financial organization and adds risks to success of achieving its multiple business objectives. This cyber risk originates from the communication networks when collaborating with global partners as well as from the greater customer access and transparency banks pride in providing.

We hypothesize that this risk creates a potential for opportunity, specifically in the financial sector. The breaches at Target, Home Depot, Sony, and most recently, Equifax exemplify to consumers the consequences and impact of lax security practices. The 2015 Ponemon Institute report [2] on megatrends in cybersecurity surveyed senior-level information technology (IT) and IT security leaders, many of whom expressed a growing support level of the idea cybersecurity can serve as a strategic advantage.

Stronger than required security practices can and will be the differentiator of one bank over another. This paper presents a roadmap how cybersecurity can be tooled as competitive advantage. Our research will prescribe the value of protecting customer data, securing networks, and controlling access as aiding in being business enablers. The core to the solution is provide consumers with the control to their security; consumers will balance their need for convenience with security. The banks and financial sector as a whole should repackage existing accessible security technology to marginally add value to their brand to promote customer driven security. If cybersecurity is embedded into the firm as an integral element of the firm's

strategy, it can be used to differentiate the firm from its competitors. Differentiating the company's IT security provides the edge over competitors.

Background and Motivation

Commercial and retail banking and general financial services customers are using digital channels to conduct business. Data indicates that highly regulated industries, as financial industries and health care have the most costly data breaches due to the fines and the higher-than-average rate of lost business and customers [2]. The limited published data on the cost of breaches has traditionally been a barrier in creating the value proposition models. Hence, the protection from the security mechanisms is intangible and hard to quantify. This also makes it difficult to calculate the return on investment (ROI) of expenditures on cyber security measures as these expenses traditionally are cannot be mapped to revenue.

But, as data is stratified throughout cyberspace, organizations must address this challenge of implementing cyber security risk strategies to protect and manage its multifaceted and unknowable inherent value. The challenge of quantifying value of intangible assets as information and cybersecurity can be related to the difficulty (at one time) of placing value on organizational culture and value of innovation uncertainty. But, now this is sold as a differentiating quality of a company; there now exist metrics to measure it's value.

Increasingly, surveys indicate how consumers have a high expectation of security when making mobile payments. The 2015 PwC Consumer Banking Survey shows the demands of retail banking customers. The Booz Allen survey [4] indicates that 66% of consumers expect banks to hold more responsibility than government securing financial assets and information. Also, consumers place security as a top criterion in selecting a banking or financial relationship as 80 percent of consumers consider a bank's ability to protect their personal information before opening a new account. Moreover, the survey indicates that 42 percent of consumers are likely to switch banks if a cyber security hack occurs in institution with which they bank.

Another study, Travelers Risk Index [6] reported the a32 percent of Americans are concerned about cyber risk and IoT (Internet of Things), especially related to threat of hacking of bank or financials. Similar sentiments were expressed by businesses. Though traditionally the investments in security have been thought of as a defensive investment, we introduce this new perspective of Cybersecurity as a value-driven investment. We propose that security investments must be leveraged as a competitive advantage and cyber security must be viewed as a strategic asset.

Framework

First, in order to frame the current cyber security landscape, we completed a SWOT analysis of the banking sector to first understand the industry and competitive forces.

Strengths of Leading Institutions: Technological Innovations

- Financial institutions have become digital firms
- Operate mission-critical networks, meet customer demands for innovative products and services, and gain customer trust and loyalty – all by involving cloud-based services, mobile technologies, multi-factor authentication technologies, and cybersecurity technologies

Threats

- Against this backdrop cyber criminals are increasingly deploying sophisticated tools, such as cloud-based botnets, exploitation of Near Field Communications, Distributed Denial of Service attacks on Cloud infrastructures, hacks of multi-factor authentication technologies using Trojans, Viruses, Malware, Phishing and Social Engineering.
- Interconnected business systems poses a threat of data and privacy breaches through 3rd party vendors' and affiliates' infrastructures. Threat is based on the resilience whole values chain and not just individual firm. A chain is as strong as its weakest link.

- Non-Traditional Financial Institutions/Non-Bank Banks (Investment Companies, Hedge Funds, Brokerages, etc.) offering innovative banking products and services to consumers
- Rivalry of Existing Competitors trying to gain market share.

Weakness

- Inadequate security infrastructure and investment to keep up with the pace of technological change. The institutions are in an arms race with cyber criminals.
- Regulatory compliance issues
- Exposure of customers' confidential data and the institutions' proprietary information assets to hackers (e.g. Sony Breach, Equifax Breach)
- Siloed cyber security and reactive defense
- Lack of enterprise-wide security consciousness and policy

Opportunities

- The volume of data and the sensitivity of customers to privacy means the institutions must keep their systems secure.
- Proactive Cybersecurity defense with capability to collect, analyzed, interpret malicious events and disseminate recommendations in real time.
- Leveraging existing cybersecurity technologies throughout the value chain.
- Cybersecurity must be designed into all process that use digital technology and not be a bolt-on or an after-thought
- Designing cybersecurity into all processes

Thus the *challenge* is in how financial institutions will meet expectations of customers who value convenience and innovative services embedded with only top-notch security.

Next, in order to better understand how an intangible commodity, as "cyber-security," can be a source of competitive advantage, we reviewed literature relating to a firm's culture (also intangible) provides sustained competitive advantage. Jay Barney in [7] describes how an aspect of a firm that is a source of superior financial performance, can be thought of providing an advantage. Hence of cyber-security to be of economic gain, adding some financial value, while being unique (rare) in some way. Competitors are using technological innovation to meet customer demands and gain market share, creating pressure on all to innovate and use technology to build market share or reignite growth.

The opportunities lie in implementing a robust cyber security strategy with robust features. A financial institution who can satisfy the consumer's desire for decreased IT complexity, coupled with an unparalleled service experience and at the same time provide air-tight security and digital privacy *will have* retain customers and attract new customers. It will be unique, add revenue, thus be a competitive advantage.

Recommendations

The analysis indicates how the market demands a financial institute leader to adapt to the dynamic threat vectors. C-suite executives must now view Cyber-security as a strategy to differentiate their financial service platforms. Reviewing the SWOT matrix provides the perspective of how potentially engaging customers to participate in informed decisions about protecting their digital financial information can be leveraged to enlist their trust in their banking services. We noted that the opportunities and overcoming weaknesses lie in information security; financial institutions must provide customers the ability to operate in a trusted environment. If customers know that the institution is investing in getting ahead of the attack, they will bank with confidence, providing the financial firms an advantage to innovate and build market share.

Small and medium sized banking firms who invest in incorporating the cybersecurity best practices into their business processes and operations are unique in setting themselves apart. They gain consumer trust

and position themselves to work with the large financial sector companies. For example, institutions implementing multi-factor authentication technology as a preventive measure (this process involves customer engagement and response) differentiates them from the non-users as well as from those who embedded this security measure after a breach or data leakage.

Technologies and processes to begin cyber security differentiation process include:

1. Lead efforts to create a board of directors who mandates that cybersecurity strategies align with business objectives of your financial firm and is part of the corporate enterprise strategy.
2. Prepare for Targeted Cyber attacks and deploy advanced authentication technologies to combat cyber fraud and breaches.
3. Collaborate with 3rd party vendors, partners and affiliates connected in inter-enterprise network to strengthen cyber defenses across the value chain.
4. Develop proactive measures against cyber-attacks.
5. Increase big data analytics capability and business intelligence in deploying cyber defenses.
6. Collaborate with technology companies that can offer capabilities and core competencies in the area of cybersecurity solutions to secure the inter-enterprise network

Conclusion

This paper offers a set of recommendations for financial firms and institutions, that addresses the need for increased cybersecurity in a constantly changing digital environment. All firms need to build trust and loyalty among their customers; by assuring them that their privacy is secure and protected by an advanced cybersecurity infrastructure.

References:

[1] Can cybersecurity provide competitive advantage?, Charles Cooper, Art of The Hack, March 2017 http://theartofthehack.com/can-cybersecurity-provide-competitive-advantage/

[2] 2015 Global Megatrends in Cybersecurity, by Ponemon Institute LLC, February, 2015. (http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf)

[3] Making Security A Competitive Advantage, Ed Sperlin, Forbes 100, May 10, 2010 https://www.forbes.com/2010/05/08/heartland-security-mastercard-technology-cio-network-elefant.html

[4]. "Consumer Expectations of Security in the Banking Industry," 2011 Booz Allen Hamilton and Zogby Survey Results

[5] Cyber Security for Financial Services: Strategies that Empower your Business, Drive Innovation and Build Customer Trust, Symantec White Paper, 2017 https://cyber-edge.com/wp-content/uploads/2017/01/Symantec-Financial-Services-White-Paper.pdf

[6] 2016 Travelers Risk Index," retrieved from Travelers website: www. travelers.com/prepare-prevent/risk-index/business/index.aspx

[7] "Organizational Culture: Can It Be a Source of Sustained Competitive Advantage?," Jay B. Barney, *The Academy of Management Review*, Vol. 11, No. 3 (Jul., 1986), pp. 656-665