S²ERC Project: Cyber Threat Intelligence Exchange Ecosystem: Economic Analysis

Report: Cybersecurity and the Financial Sector

Author: Joe Stuntz, MBA EP 14, McDonough School of Business

Status: Published

Date: 7 February 2014

Abstract

An examination of current initiatives in the financial sector to improve cybersecurity and information sharing.
Introduction

The financial industry and the infrastructure around it have faced attacks since the beginning of the industry such as bank robbers, insider fraud, and securities fraud. Historically these attacks have had little impact on the system as a whole as they were focused on one bank, one account, or one location. Today, while these types of attacks continue to be a concern for the industry, a new type of attack now exists that has the potential to steal substantially more money and information while providing a threat to the entire financial system. These attacks do not require access to the bank vault or a branch location, but are done through the networks and connections that the bank relies on to conduct business. Cyber-attacks are attempted for many reasons and are an increasing concern for all parts of the financial sector from the largest multinational firms to the very small firms focused on one particular area because of their ability to create such a large impact in a short amount of time. In a research report titled, Beyond the Horizon: A White Paper on Systemic Risk, the Depository Trust and Clearing Corporation (DTCC) found that 89% of responders considered cybersecurity a systemic risk due to the interconnectedness and dependencies throughout the system.\(^1\) It is because of this interconnectedness that these issues must be addressed and the industry is already responding with a number of efforts. While a major attack has not been successful in terms of taking down the whole system or a significant part of the system, the potential is there and the financial sector must continue to make progress to avoid this.

The financial sector today consists of firms of all different sizes, area of focus, technical capabilities, and resources. Some of these firms are very large multinational companies such as JP Morgan and Goldman Sachs while other firms in the sector are small local banks. In addition to these, there are firms like exchanges, hedge funds, trading firms and many others that might not be as well-known but are very important to the successful functioning of the markets. Historically many of these firms operated through telephone lines and pen and paper and were not as linked or connected as they are today. While this made operations much less efficient, it did limit the amount of systemic risk that an attack of any type could have. Now almost all firms participating in the sector are connected through multiple networks to ensure the availability of a connection and many pay for the highest speed connection possible to improve the timing of trades. This has resulted in a much faster and liquid market but does provide many more opportunities for an attack on one institution to spread to many others.

The environment around cybersecurity has changed substantially in the past few years. Previously cybersecurity was not a major concern as the attacks were not very complex and most actors did not have the technical capability to create an attack that would cause significant harm. As bandwidth and processing power increased exponentially and programming skills became more developed, the potential for bad actors to significantly harm an organization or even the entire sector became real. But with this increase in technology and capabilities for the bad actors came an increase in the defensive capabilities for the firms as well as an increase in the awareness of firm leadership to the potential threats. According to Mark Clancy, Managing Director of the DTCC, who testified to the Commerce Committee on behalf of American Bankers Association, Financial Services Roundtable, and Securities Industry Financial Markets Association, the current economy as a whole loses $100 billion to cybercrime as well as 508,000 jobs lost because of intellectual property loss and firms being put out of business by attacks. These numbers continue to grow and present a major challenge for the economy and especially the financial sector.

The Current Environment for the Financial Sector

The financial sector faces an issue that can impact them from many angles. A trading firm for example could be attacked directly through any number of technical methods which could bring down their business. Or a firm they are doing business with or have done business with has been attacked and the threat has now spread over the connections back to the trading firm who may have never been attacked directly but is now compromised. Finally, the firm and their business partners may have created excellent defenses that have kept the firms safe from attack, but an attacker manages to create a problem somewhere else that takes markets down and loses the trading firm money on their positions. An example of this would be on April 23, 2013, when a cyber-attack gained control of the Associated Press Twitter account. The attackers then proceeded to post a message about an explosion at the White House and the markets quickly lost 136 billion dollars on this news. As it was discovered that the message was a hack, the market recovered, but some firms had substantial losses if they had set stop losses or were using other trading strategies that were triggered by the massive drop in value.

To better understand the risks and how prepared the sector is for these risks there has been some recent research that gave some very meaningful numbers. According to the Financial Times, 53%

---

of the World Federation of Exchanges members have faced a cyber-attack recently and 59% said they do not have sufficient recovery protocols in case of a large attack\textsuperscript{4}. While these numbers are just about exchanges I believe the numbers across the sector are similar. The first number shows the massive amount of risk and total activity that is going on in the sector. If approximately 50% of all firms are getting attacked that is many thousands of firms just in the US and many of these firms will be attacked multiple times in a year and some even every day. The second number is even more concerning to me because there are always new developments in attacks and there is no way to defend against everything so for a firm not to have a good recovery protocol is a major problem.

Most experts believe that defending against all attacks is not possible and that the highest attainable level of security is stopping about 95% of all attacks. This seems like a high number but not unreasonable considering the amount of attacks that occur every day. Unfortunately current security levels are not close to 95% and it would be a major challenge to reach that level. According to Bloomberg, the 172 companies surveyed would have to increase spending by 774% on average to reach that 95% rate\textsuperscript{5}. I do not believe that any firm is willing to increase security spending by that amount even if they knew exactly what measures to take and spend resources on which they would not know. This is also a potential differentiating factor between very large companies that may be able to spend more on security although having more to protect versus smaller firms and this lack of resources may make smaller firms easier targets going forward. While it will be very hard for any company to budget the estimated needs to reach high security, in an April 10\textsuperscript{th} 2013 letter to shareholders, JP Morgan stated that they currently spend 200 million a year on information security and plan to increase this number dramatically over the next few years\textsuperscript{6} Many other companies have issued similar statements or plans to increase funding for their security which is a great start but is not enough to deal with the growing problem.

The growing security problem for firms in the financial sector can take many forms. Today the most common threats are Distributed Denial of Service (DDoS) attacks and Advanced Persistent Threats (APT). A basic description of a DDoS attack is the attempt by an attacker or multiple attackers to send so much traffic to the site or application that it shuts down and cannot process any legitimate traffic. A few years ago these were much less powerful but as connections have gotten better some attackers can now

\textsuperscript{4} The Financial Times, Nature of the Threat, \url{http://www.efinancialnews.com/story/2013-08-08/cyber-attacks-dtcc-nature-of-the-threat?ea9c8a2de0ee111045601ab04d673622}


control millions of computers as well as servers that can send exponentially more traffic than previously possible. Recent attacks have been measured as sending as much as 15 times the volume of traffic that the firm’s bandwidth could handle. DDoS attacks do not require extremely complicated code and are very common in the financial sector as seen by the issues that Wells Fargo and Bank of America had with their sites in the last year. Advanced Persistent Threats are much more complicated and can be many more targeted type attacks. These attacks use more challenging coding and are less frequent but very dangerous. Another challenge for the security of the financial sector is that security put in place must be able to deal with many different types of attacks coming from multiple places including outside firms, within the supply chain, or from external actors.

A recent real-world example of a cyber-attack is one that impacted Barclays in the UK. In this case, the hackers posed as engineers to gain access to a branch IT system. The fake engineers then attached a hardware device to the system and the device captured information that was going through the bank IT system. The hackers ended up using the information received from the hardware device to steal approximately 2.1 million dollars which was similar to an amount stolen from another branch in April. This example is a little different when compared to someone writing a complex APT that causes a lot of damage, but this more basic type of example is more likely to occur. When poor security practices are in place in the organization it allows hackers easier access points to the information they are looking for and they may not require extremely advanced skills if they are able to obtain physical access to the resource. Another well publicized example was of a group on the East Coast that originally drove around with a wifi scanner in their vehicle and waited to find a store with an open wireless network. They would then use this open network to get into the store’s system and copy information or put in a program that records any future information related to credit card numbers. The group would then copy the credit card information onto blank cards and withdraw the money from an ATM. Eventually they got more complicated and began to steal numbers and then have a dealer in the Eastern Europe sell the card numbers and share the profits. Eventually they even were able to access a payment processing firm’s system where they were able to collect a lot of the credit card information coming into the company. By the time they were finally stopped after the Eastern European dealer had been caught and evidence on the group in the US was discovered, they had stolen over 100 million credit card numbers. I feel this example is an important one because it involved weakness in a sector that was not the finance sector. The retail stores were using unsecured networks which allowed the hackers to

---

eventually get to a payment processing firm which is part of the financial sector. Another reason this is an important example is because the success of this attack was not because it was more complex. It was more successful because it found a very weak point in the system that was vulnerable. All a retail store would have had to do was secure the wireless network they were using and these issues never would have happened.

**What is happening today?**

There are many efforts going on today related to cybersecurity in the financial sector. Some of these are inside the financial sector and many of them also include the Federal Government. While these firms are extremely competitive, according to Mark Clancy, the financial sector understands that because of the interconnectedness of the industry and their business, everyone must improve their cybersecurity which makes cybersecurity a noncompetitive area and the sector is committed to working together⁹. One way the sector is working together is through the Financial Services Sector Coordinating Council (FSSCC) which was formed in 2002 and has 52 volunteer member associations. The FSSCC is focused on the protection of the financial sector and is supported by Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. Currently the FSSCC is working with the Federal Government on efforts around Executive Order 13636 related to cybersecurity for critical infrastructure and legislation proposed by the Senate Commerce Committee that is related to that Executive Order.

According to the FSSCC there are a number of challenges that are specific to the financial sector that need to be addressed by new activities. The first challenge is that different parts of the sector are regulated by different regulators with different guidance on Cybersecurity. Some firms are regulated by the SEC while others are regulated by Self Regulating Organizations such as MSRB, FINRA, and NFA. Insurance companies must work with state insurance regulators and for some insurance companies they also must deal with the Department of Health and Human Services when the privacy and security of long term care insurance gets involved¹⁰. Many of these standards and regulations are also impacted by the Gramm-Leach-Bliley Act of 1999 and how the Dodd Frank Act will be implemented. In this environment of a lot of regulations and the potential for conflicting information, one of the main focuses of the FSSCC is to make sure that the Executive Order efforts do not conflict with anything already being done

---


especially if the Executive Order efforts will require additional resources. While this is what the FSSCC wants to avoid, they are looking for this effort to provide additional support for practices such as information sharing as well as using a risk assessment that will prioritize the risk and vulnerabilities and working towards securing the supply chain.

The FSSCC considers information sharing to be the most critical line of defense in mitigating cyber risk. Information sharing is such a concern for the financial sector that there is an organization known as the Financial Services Information Sharing and Analysis Center (FS-ISAC) that focuses on risk mitigation tactics and information that helps organization address risk and vulnerabilities. Between the FS-ISAC and the FSSCC there are resources working to improve cybersecurity for all parts of the financial sector. Moving forward, these organizations will have an important role in working with other groups inside and outside of the Federal Government to make sure that initiatives such as the Cybersecurity Framework for Critical Infrastructure that is being directed by NIST not only has input from the financial sector but aligns with the current direction and strategy for the sector.

Executive Interviews

Many of the efforts that were mentioned above have a lot of participation and direction from large financial firms but less well known is the perspective of other firms. To do this a few executives of smaller or less well known entities answered questions about how their organizations deal with cybersecurity.

1. A member of a board for an exchange

Exchanges are what allow financial markets to work and if they are compromised then the attacker would have a path to get to almost any firm in the industry. Because of his position on the board this individual could have a valuable perspective on whether or not cybersecurity was a priority or had even made it into board conversations. The following are summaries of the questions and his answers.

• Who is responsible for cybersecurity in your organization? – The CIO
• Do you follow guidance from the Federal government and would you be open to voluntary standards they produce? - The Fed gives lots of guidance already, see


• Which agency would you like to see have governance or oversight of cybersecurity or should it be done by many agencies? – The SEC does not understand technology and other agencies do not understand the financial markets but not sure what mix is best.

• Is cybersecurity being incorporated with other risk management practices? – Yes, cybersecurity is part of overall risk management. We address it at the board level when we have our risk meetings.

• Is cybersecurity a concern for you? - The industry takes it very seriously, google Quantum Dawn

2. An owner of a private equity firm

This private equity firm is a small business, less than 25 people, and could hopefully provide insight into how an organization without an internal IT group or risk management group deals with cybersecurity. The following are summaries of the questions and his answers.

• Do you have cybersecurity concerns and if so have they changed your strategy or operations? – We consider the security of vendors we use. For example we outsource our IT function to an organization and we believe that they are state-of-the-art in their security

• Would your organization be open to implementing non-mandatory guidance from the Federal Government? - I believe both vendors we use would be open to implementing qualified guidance and we would be interested in seeing them implement it.

• Which agency should have oversight over cybersecurity? – I do not have an opinion on which agency should have oversight

• Is cybersecurity being incorporated into operations and risk management? - We do incorporate cybersecurity into everything we do, primarily by keeping documents out of email, and using face-to-face meetings to transfer critical information. We try to remember that anything we put in email could get into the hands of a hacker.

Ideally many executives could respond to these questions and provide us with additional information, but the two interviews provide insight and reasons for optimism. While they are in different parts of the financial sector with different responsibilities, both executives are aware and involved in how their organizations are dealing with cybersecurity. Both mentioned that cybersecurity was part of risk management and normal operations which means it has become part of the corporate culture which is great progress. They also both expressed openness toward guidance from the Federal Government which is good for the upcoming Cybersecurity Framework. Because of their different sizes
and resources how each organization handles cybersecurity is different but the similarities were encouraging.

The mention of Quantum Dawn by the first interviewee was a good sign as Quatum Dawn two just occurred in July and the results were announced in October. Quatum Dawn 2 “enabled over 500 participants from over 50 different entities across the financial sector to run through their cyber crisis response plans including how they would coordinate with the financial sector as a whole and with government agencies to share information.”

This exercise was declared a success but three areas were listed that the industry can improve upon:

- Sector wide incident response
- Systemic risk assessment
- Communication and information sharing

These findings echo the research available and concerns from members of the industry so hopefully this will lead to consensus on the way forward. Despite the need for improvement, the existence of a sector wide effort like Quantum Dawn shows the importance of cybersecurity and the seriousness of the responses from industry members.

Financial firms represent a vital piece of the US economy and are under constant threat of cyber-attack. Today while the threat is more advanced than ever, the sector has also made major improvements in the awareness of the threat, resources to fight the threat, and working inside and outside the sector to improve responses to the threat. Cybersecurity will continue to be an area of emphasis and because of the interconnectedness it cannot be done just on an individual firm basis, but by the entire sector and by the entire economy. It will be impossible to protect against every threat but by making small progress to improve the most vulnerable areas, large improvements in security can be made. As there is a constant fight for resources in any organization it will be crucial for cybersecurity to remain a priority to avoid potential disaster that will impact the entire country.

---