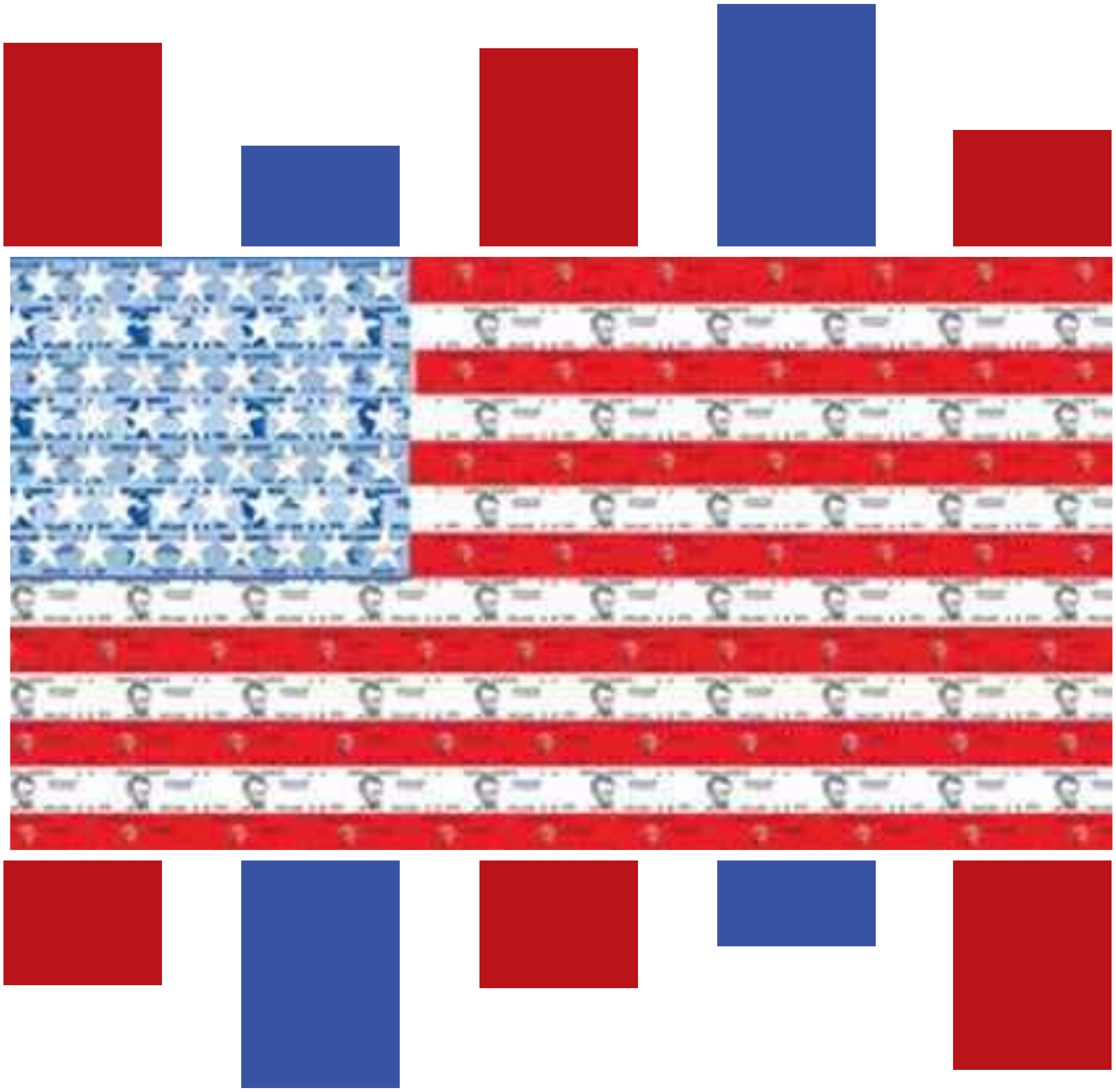
U.S. Bank of Cyber: An analysis of Cyber Attacks on the U.S. Financial System

by Crimmins, Falk, Fowler, Gravel, Kouremetis, Poremski, Sitarz, Sturgeon, Zhang
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086



U.S. Bank of Cyber

An analysis of Cyber Attacks on the U.S. Financial System

Under the Direction of Dr. Sam Liles

Written by:
(In Alphabetical Order)
Danielle Crimmins
Courtney Falk
Susan Fowler
Caitlin Gravel
Michael Kouremetis
Erin Poremski
Rachel Sitarz
Nick Sturgeon
Yulong Zhang

CNIT 58100 Spring 2014

Executive Summary

PURDUE
UNIVERSITY

CYBERFORENSICS LABORATORY

CNIT 58100 Spring 2014

The following paper looks at past cyber attacks on the United States financial industry for analysis on attack patterns by individuals, groups, and nationstates to determine if the industry really is under attack. The paper first defines the terms used, then explains the theory and paradigm of cyber attacks on the U.S. financial industry. Following is a graphical and detailed timeline of known cyber attacks on the U.S. financial industry reaching from 1970 through 2014. Four attack cases are chosen to be researched in summary and four attack cases are chosen to be researched in depth. These cases include: Kalinin & Nasenkov, Mt. Gox, Stock Market Manipulation Scheme, Project Blitzkrieg, Union Dime Savings Bank Embezzlement, National Bank of Chicago Wire Heist, and an attempted Citibank Heist. An analysis then explores attack origination from individuals, groups, and/or nation states as well as type of attacks and any patterns seen. After gathering attacks and creation of a timeline, a taxonomy of attacks is then created from the analysis of attack data. AStrenghts, Weakness, Opportunities, and Threats (S.W.O.T.) analysis is then applied to the case study Heartland Payment Systems.

Table of Contents

Table of Figures

Introduction

The prevalence of technology is changing the way that financial crimes are being carried out. Many financial institutions offer services such as online banking, electronic bill pay, mobile banking apps, and digitized bank statements that are sent via email. These online services provided by financial institutions result in large amounts of personal, private, and sensitive data being stored electronically on servers. The need to keep up with the technology demands sometimes means security measures may be lacking, making both the individual clients and the financial institution itself vulnerable to a cyber attack. A cyber attack may be on a small scale, such as stealing an individual's identity or credit card number electronically, or it may be a large scale attack, such as shutting down or temporarily interrupting the function of a financial institution, such as a bank or even the stock exchange. A cyber attack may be perpetuated by a single individual, organized group, or even a nation state, and the motives for such an attack vary greatly based on the goals and intentions of the attacker.

An individual perpetuating a cyber attack on a financial institution or their client is likely doing it for personal gain, out of retaliation, or simply to be a nuisance. While an individual instance of identitytheft may not seem financially significant to anyone external to the victim, identity theft cost consumers over five billion dollars and cost financial institutions over 48 billion dollars over the course of 2008. In addition to identity theft, other common cyber attacks on businesses, individuals and institutions include fraud and espionage, both of which can also be financially devastating. A 2011 report from the Ponemon Institute, a privacy and information management firm, the average data breach in the United States ends up costing 6.75 million dollars, ranging as high as 31 million dollars[1].

If the cyber attack is led by a nation state or a group acting on their behalf, and the target is an external entity to that nation state, the attack could be considered an act of war depending on the intent and severity of resultant damage. A successful attack that originated from a group that considers the United States to be an enemy country that disrupts the activity of any critical infrastructure entity, could be considered an act of war.

The modern day economy of the United States is extremely dependent on information technology systems and cyber. Critical infrastructure is a term that refers to any organization essential to the national economy, including financial, energy, transportation, and telecommunication entities, as well as waste, water, public health, and similar government services[2]. A successful, malicious cyber attack on any of these entities of the United States critical infrastructure could potentially be devastating to the well being of citizens, as well as financially devastating to the government.An attack wouldn't necessarily have to be targeted on a financial institution to damage the economy; an attack on any critical infrastructure has the potential to additionally damage the United States financially. A successful attack on the federal banking industry could potentially bankrupt individuals, destroy businesses, devastate the economy or prevent the federal government from being able to function as it needs to.

This paper looks into the history of the United States financial industry and the attacks taken against it by the use of cyber. By looking at the attacks taken place and researching the attack types and originating known attacker we are able to look into the patterns used by groups, individuals, and nation states in their attacks against the United States financial industry. For the ease of continuity the following terms are defined as they are used in this paper.

[1] Shackelford, S. (2012). Should your firm invest in cyber risk insurance? Retrieved from www.sciencedirect.com

[2] Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. Retrieved from www.sciencedirect.com

Definitions

Breaches:
Refers to loss of PII controlamounting to actual or potential compromise, including: unauthorized disclosure; unauthorized acquisition or access; or any similar situation involving unauthorized use through inappropriate PII access (1) potential or confirmed; (2) within the agency or outside the agency; and (3) regardless of format, whether physical (paper) or electronic[3].

Critical Infrastructure:
Any organization essential to the national economy, including financial,energy, transportation, and telecommunication entities, as well as waste, water, public health, and similar government services[4].“systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (Sec. 1016(e)). Critical sectors include: agriculture, food, water, public health, emergency services, government defense industrial base, information and telecommunications, energy, transportation banking and finance, chemical industry, and postal and shipping[5]”.

Cyber: Norbert Wiener gives the earliest modern definition of cyber as, “the science of control and communication in the animal and the machine[6]”.

Cyber attacks: Hathaway et.al. define cyber attack from the legal standpoint as an attack meant to undermine the functioning of computer systems with political, personal, or national security goals[7].

Cybercrime: “cybercrime can be understood as an attack on the confidentiality, integrity and accessibility of an entity’s online/computer presence or networks and information contained within[8]”.

Cyberwar: “the use of computers to disrupt the activities of an enemy country[9]” .

Denial of Service (DoS): DoS attacks deny legitimate users access to services and data[10]. Attacks can target service endpoints or network connections so long as the end result is degradation to the point of uselessness.

Digital Evidence: Information stored or transmitted in binary form that may be relied on in court[11].

Effect: Effects are the short term outcomes from an attack. If an attack where a bombing then the effects of the attack are human casualties and property damage**.**

[3] OMB Memorandum M 07 16 dated May 22, 2007, Subject: A Safeguarding Against and Responding to the Breach of Personally Identifiable Information

[4] Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. Retrieved from www.sciencedirect.com

[5] Moteff, J., & Parfomak, P. (2004, October). Critical infrastructure and key assets: definition a identification. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

[6] Wiener, N. (1948). Cybernetics, or Control and Communication in the Animal and the Machine. New York: John Wiley & Sons.

[7] Hathaway, O., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel J.(2012) The Law of Cyber Attack. California Law Review, vol. 100, pp. 817 886.Retrieved from http://

[8] OICU IOSCO. 2013 (2013). Cyber Crime, Securities Markets and Systemic Risk. IOSCO.

[9] Oxford Dictionary. 2014 Oxford Dictionary. (2014, March 19). Cyberwar. Retrieved from www.Oxforddictionaries.com/us/definition/American_english/cyber war

[10] US CERT. (2009, November 4). Security Tips (ST04 015): Understanding Denial of Service Attacks. Washington D.C.: Retrieved from http://www.uscert.gov/ncas/tips/ST04 015.

[11] NIJ. (2008). NIJ Special Report Electronic Crime Scene Investigation: A Guide for FirstResponders (2nd ed.). Washington D.C.: U.S. Department of Justice.

Definitions Cont.

Financial Cyber attack: "Conduct of large scale, politically or financially motivated conflict based on the use of offensive and defensive capabilities to disrupt digital systems, networks and infrastructures, including the use of cyber based weapons or tools for non state/transnational actors in conjunction with other forces for political ends[12] .

Financial Industry:
Financial: "the management of large amounts of money, esp. by governments or large companies"[13]. I*ndustry:* "economic activity concerned with the processing of raw materials and manufacture of goods in factories"[14].

Fraud: Fraud is defined in the legal sense as the deliberate deception in order to cause damage[15].

Hacktivists:
Class of hacker who publicly breaks into computer systems as a form of protest[16].

Impact:
Impacts, when contrasted with effects, are long term impacts of an attack. In the case of a bombing then impacts are the psychological damage done to human victims or policy changes made in response by political leaders.

Infrastructure:
"The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole"[17].

Intrusion: An intrusion happens when an attacker gains access to confidential data or computing systems[18].

Man in the Middle (MITM):
"Considered an active eavesdropping attack, MITM works by establishing connections to victim machines and relaying messages between them. In cases like these, one victim believes it is communicating directly with another victim, when in reality the communication flows through the host performing the attack"[18].

Non Nation State Actors:
"Organizations lacking formal or legal status as a state or as an agent of a state"[19].

[12] (Cyber Conflict Studies Association. (2012). Addressing cyber instability. Executive Summary.

[13] Google. (2014). Define. Retrieved March 18, 2014, from Google: www.google.com

[14] Google. (2014). Define. Retrieved March 18, 2014, from Google: www.google.com

[15] Legal Information Insitute. (n.d.). Wex Legal Dictionary: Fraud. Retrieved from: http://www.law.cornell.edu/wex/fraud

[16] McCormick, T. (2013, April 29). Hacktivism: A Short History. Foreign Policy. Retrievedfrom: http://www.foreignpolicy.com/articles/2013/04/29/hacktivism

[17] Moteff, J., & Parfomak, P. (2004, October). Critical infrastructure and key assets:definition a identification. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

[18] Federal Bureau of Investigation (FBI). (n.d.) Computer Intrusions. Retrieved from:http://www.fbi.gov/about us/investigate/cyber/computer intrusions

[19] Sanders, C. (2010, March 17). Understanding Man in the Middle Attacks: ARP Cache Poisoning (Part 1). Retrieved December 4, 2013, from Windows Security:http://www.window security.com/articlestutorials/authentication_and_encryption/Understanding Man in the Middle Attacks ARP Part1.html

[20] DeLuca, C.D. (2013). The need for international laws of war to include cyber attacks involving state and non state actors. Pace International Review OnlineCompanion 278. Retrieved from http://digitalcommons.pace.edu/cgi/viewcontent.cgi?

Definitions Cont.

Social Engineering:
"A non technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures (Rouse, 2006)."

Phishing:
In computing, phishing(spoofing) is a form of a social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message (Kaspersky, 2014).

Spear Phishing:
Spear phishing is a special case of phishing attack. Whereas phishing succeeds by attacking a large number of users with a generic message, spear phishing targets previously identified individuals with messages tailored to the users' interests. The hope for attackers is that a message that is more relevant to the target is more likely to succeed (Peltier, 2001 p. 21).

Risk: The chance that a threat exercises or exploits a vulnerability (Peltier, 2001 p. 21).

Soft Target:
Targets with poor or missing protection mechanisms (Stewart, 2011). The existence of a soft target suggests that other targets exist with stronger security, making the soft target easier and more desirable to attack in comparison.

Threat:
An actor or event that exploits a vulnerability.

Vulnerability:
A weakness of an asset or group of assets that can be exploited by one or more threats where an asset is anything that can has value to the organization, its business operations and their continuity, including information resources that support the organization's mission (ISO 27005).

A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy (IETF RFC 2828).

War:
Aggression and invasion of one nation upon another nation. For a conflict tomeet the definition of war as put forth by the United Nations then it must be between two nations and the aggression must be unprovoked (Wilmshurst, 2008).

[21] Rouse, M. (2005, April). Cyber. Retrieved March 17, 2014, from SearchSOA: http://searchsoa.techtarget.com/definition/cyber

[22] Kaspersky. (2014) Spear Phishing. Retrieved from: http://usa.kaspersky.com/internetsecurity center/definitions/spear phishing#.U1lHBlf0kWZ

[23] Peltier, TR. (2001). Information Security Risk Analysis. Auerbach.

[24] Stewart, S. (2011, January 27). The Moscow Attack and Airport Security. STRATFOR Global intelligence. Retrieved from: http://www.stratfor.com/weekly/20110126 moscow attack airport security

[25] (ISO 27005)

[26] (IETF RFC 2828)

[27] Wilmshurst, E. (2008). Definition of Aggression. United Nations Audiovisual Library of International Law. Retrieved from: http://legal.un.org/avl/pdf/ha/da/da_e.pdf

What is the financial system? The financial system is an interconnected system of companies and organizations that handle capital; It exists to grow and transfer wealth. Banks, stock and equities markets, and insurance agencies are all parts of a complex, intertwined network whose data represents the accumulated wealth of individuals and nation states alike. The financial system is now heavily reliant upon computers and computer networks in order to perform their functions[28]. Computers are now an integral part of the financial system and because of this attacks on these computers are a mechanism for attacking the financial system as a whole. There are two classes of attacks relevant to threats on the financial system: threats to wealth at rest, and threats to systems that transmit wealth.

Wealth at Rest

When wealth is at rest it exists as currency in bank accounts, capital investments, or other assets. Depending on the type of asset targeted by an attack, the wealth can either be transferred away (i.e. stolen) or destroyed. Destroying wealth is accomplished by various means. If the asset targeted is physical then it can be destroyed outright. The possible complication for the attacker here is that insurance exists in various forms to mitigate against these kinds of loss based attacks. If the asset is properly insured then an attacker may only succeed in temporarily denying use of the asset, or if the asset is insured at a replacement value less than its estimated value a partial loss of wealth for the amount of value not covered by insurance.

There exists mitigation's against theft as well. Banks and credit card companies often offer protection against fraud and the reimbursement of funds in event of theft. In this case it is the financial firms themselves that absorb the cost of the lost wealth, passing the costs on to the consumer in terms of higher fees and/or lower returns.

Counterfeiting currency undermines value in the global marketplace. A fact of macroeconomics is that the more printed currency exists the less it is worth. This is why nations jealously guard their rights to print and issue currency. Counterfeiting happens with individual criminals looking to make money but even nation states like Germany during the Second World War[29] or the modern North Korean government[30]use counterfeiting as a weapon to either harm another nation or line their own pockets on a global scale.

[28] Whiteside, T. (1979). Computer Capers: Tales of Electronic Thievery, Embezzlement and Fraud. Ty Crowell.

[29] Malkin, L. (2006). Krueger's Men: The Secret Nazi Counterfeit Plot and the Prisoners ofBlock 19.

[30] Nanto, D. K. (2009). North Korean Counterfeiting of U.S. Currency. CongressionalResearch Service. Retrieved from http://www.fas.org/sgp/crs/row/RL33324.pdf

Cont.

Wealth in transmission

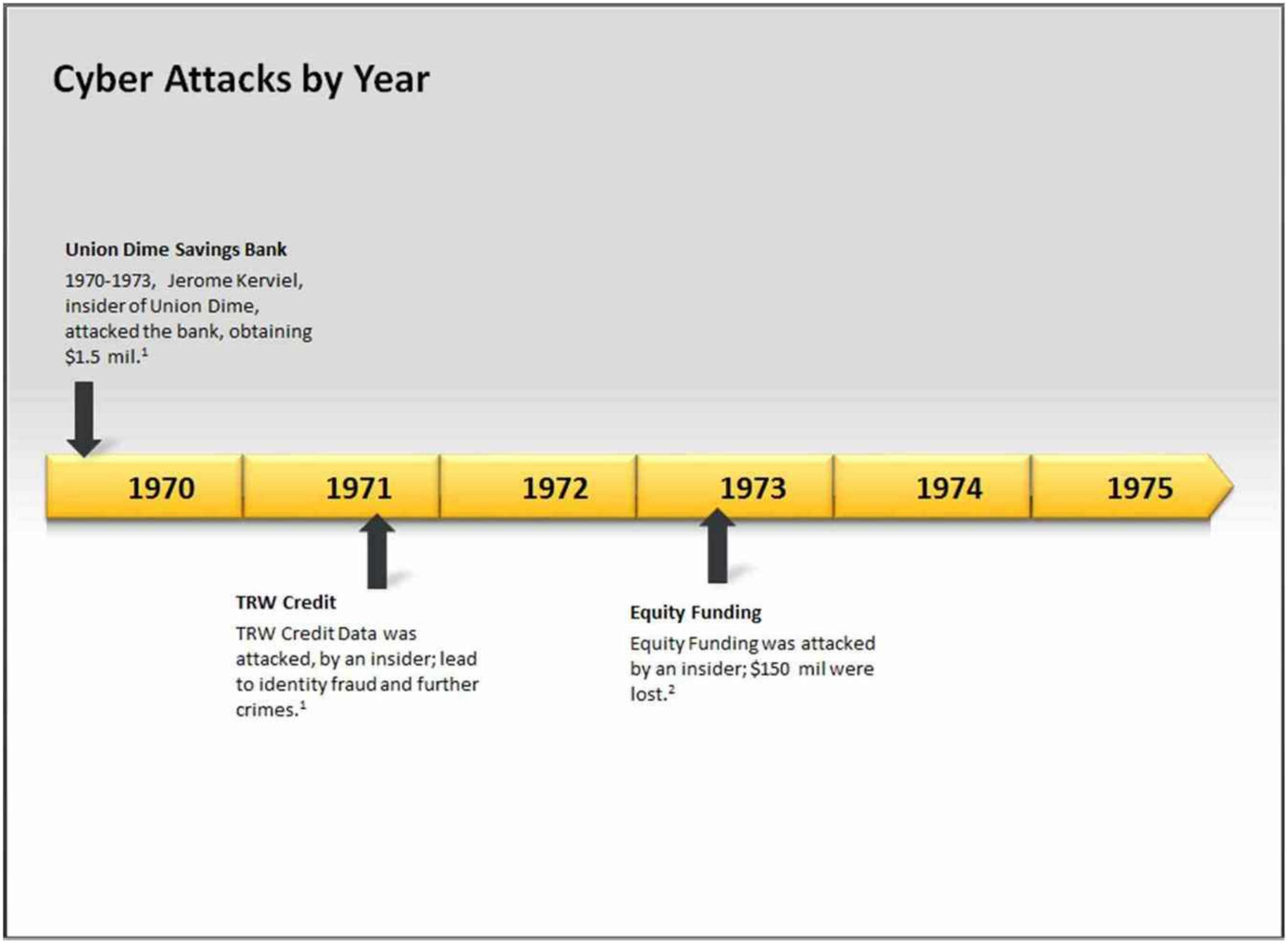
The second class of attacks on financial systems is targeting the means of wealth transmission. In modern times wealth is transmitted electronically around the world. High speed trading is a form of finance that is especially sensitive to small disruptions in transmission. Speed is of such critical importance that a trader only Internet service profile built a whole new communications line between New York and Chicago to exploit market inequalities[31]. The new line reduced data transmission speeds by a fraction of a second and quickly became a favorite of traders. If an attacker were able to slow transmission speeds by a similar amount, or corrupt enough data to require retransmission, then they would cause lost trading opportunities, destroying wealth.

A party that cannot move their wealth, but instead is forced to hold their wealth in place, is losing value on their wealth. Existing wealth must generate a rate of return greater than that of inflation otherwise its net value is decreasing. That’s why hiding physical money under a mattress is a bad idea because while the money sits there not earning interest it is actually decreasing in value.So if an attacker can destroy a little wealth by slowing down transmission speeds then could they destroy more wealth by taking down the data link entirely? In the short term, yes, but not in the long term. Financial institutions like the stock markets have such in depth accounting systems that they can roll back entire trading systems. If any problems were detected then it would be reversed at the earliest possible opportunity. If the data lines themselves were cut then a day or two of trading time might be lost, but all major exchanges have hot and cold back up sites. A day or two of lost trading is insignificant in the long run. One conclusion is that in order to cause as much financial damage and loss as possible, an attacker must maintain a sustained attack for as long as possible without being detected. Detection leads to remediation and repair by the target.

The end goal of the attack reveals something about the priorities of the attacker. If the attack is small scale and distributed across many users such as bank credential fishing or ransoming people’s own files back to them, then the attacker is most likely trying to transfer other people’s money into their own accounts. This is the act of a criminal acting independent of higher direction. The amount of money gathered by these operations is significant for an individual criminal but insignificant to the likes of a nation state. If the attacks are on critical infrastructure, long term in nature, or designed to undermine the healthy and confidence of a financial system then that suggests motives more aligned with those of nation states.

[31] Steiner, C. (2012). Automate This: How Algorithms Came to Rule Our World. Portfolio.

All of the data collected to create this timeline of cyber attacks against the U.S. financial industry were collected via open source resources. The attacks chosen are those our team felt best related to our previously defined terms of cyber attack and financial industry. Forty seven different attacks spanning over 44 years from 1970 to 2014 were chosen to be included within this timeline. The attacks range anywhere from an individual attacking the industry up to a nation state attacking the U.S. financial industry. A comprehensive and detailed list of the attacks is after the timeline graphical representation, in Table 1, which then leads into specific case studies chosen to represent different attack types within different decades. Notice within the graphical timeline how the amount of reported cyber attacks relating to the financial industry progressively gets larger as time goes on. This does not necessarily state that there were less attacks on the financial industry between 1970 late 1990's but could be that there were not as many reported in terms of by the use of cyber attacks.



Cyber Attacks by Year

Union Dime Savings Bank

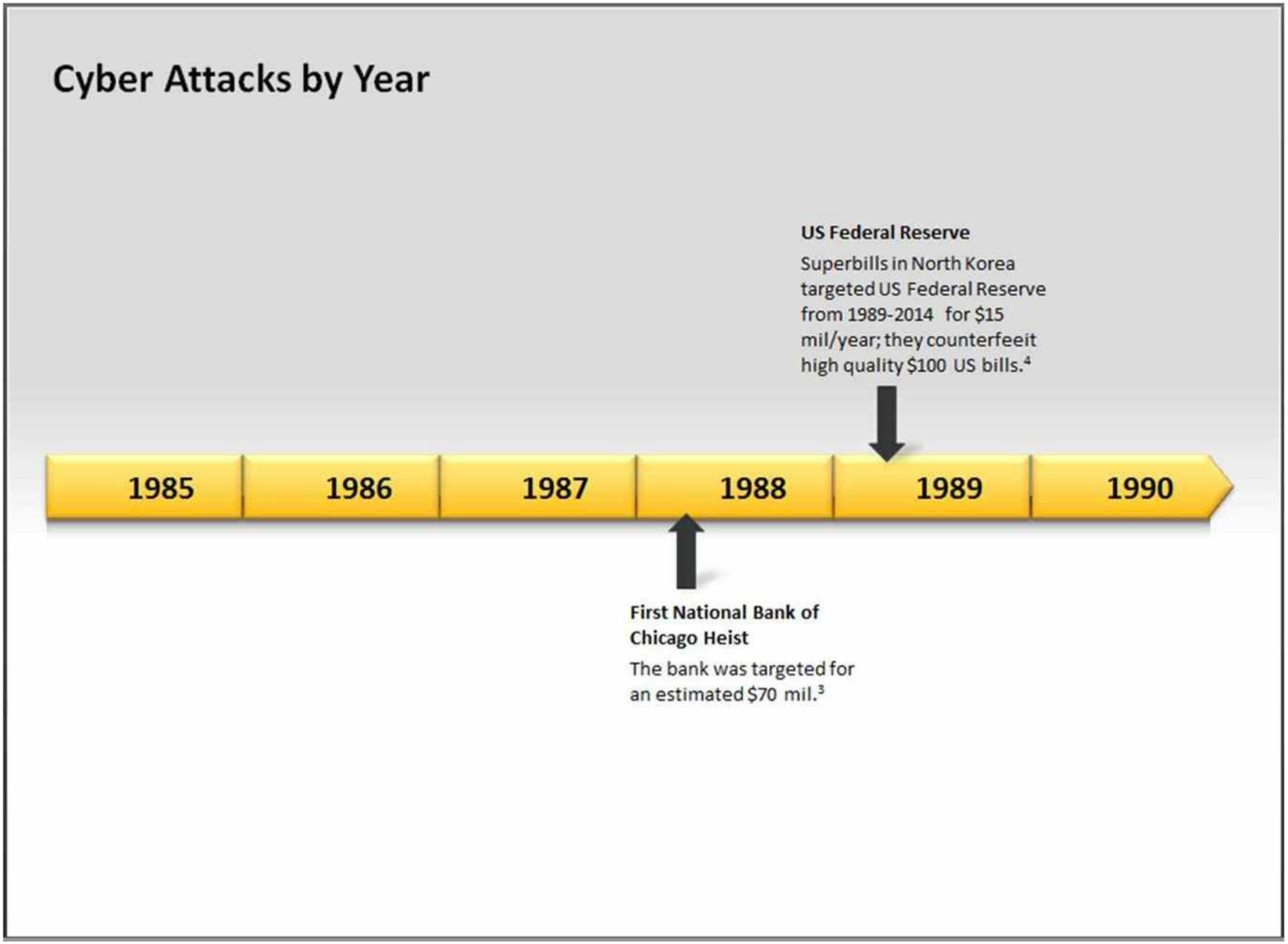
1970-1973, Jerome Kerviel, insider of Union Dime, attacked the bank, obtaining $1.5 mil.[1]

TRW Credit

TRW Credit Data was attacked, by an insider; lead to identity fraud and further crimes.[1]

Equity Funding

Equity Funding was attacked by an insider; $150 mil were lost.[2]



Cyber Attacks by Year

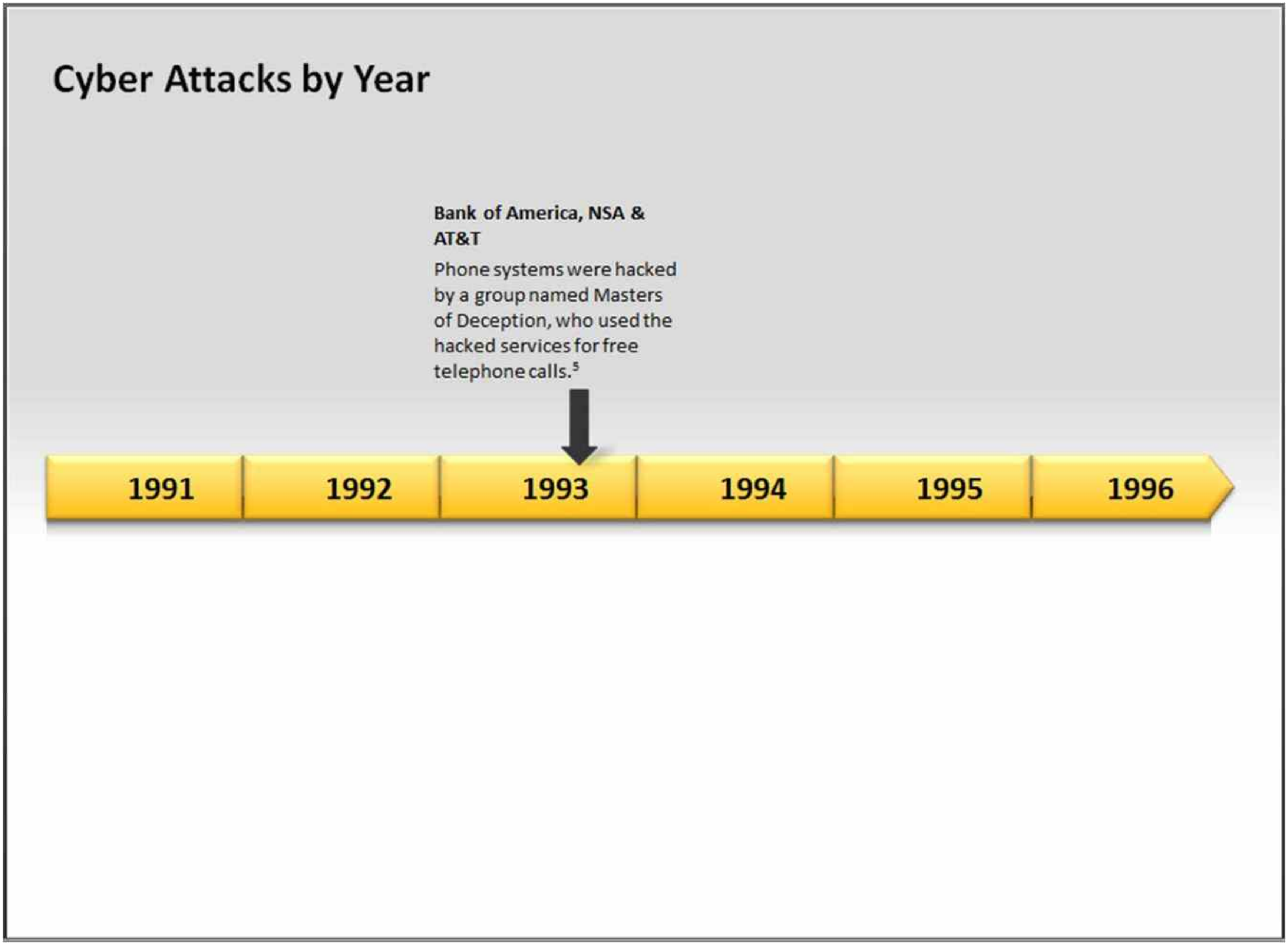
US Federal Reserve

Superbills in North Korea targeted US Federal Reserve from 1989-2014 for $15 mil/year; they counterfeeit high quality $100 US bills.[4]

1985 1986 1987 1988 1989 1990

First National Bank of Chicago Heist

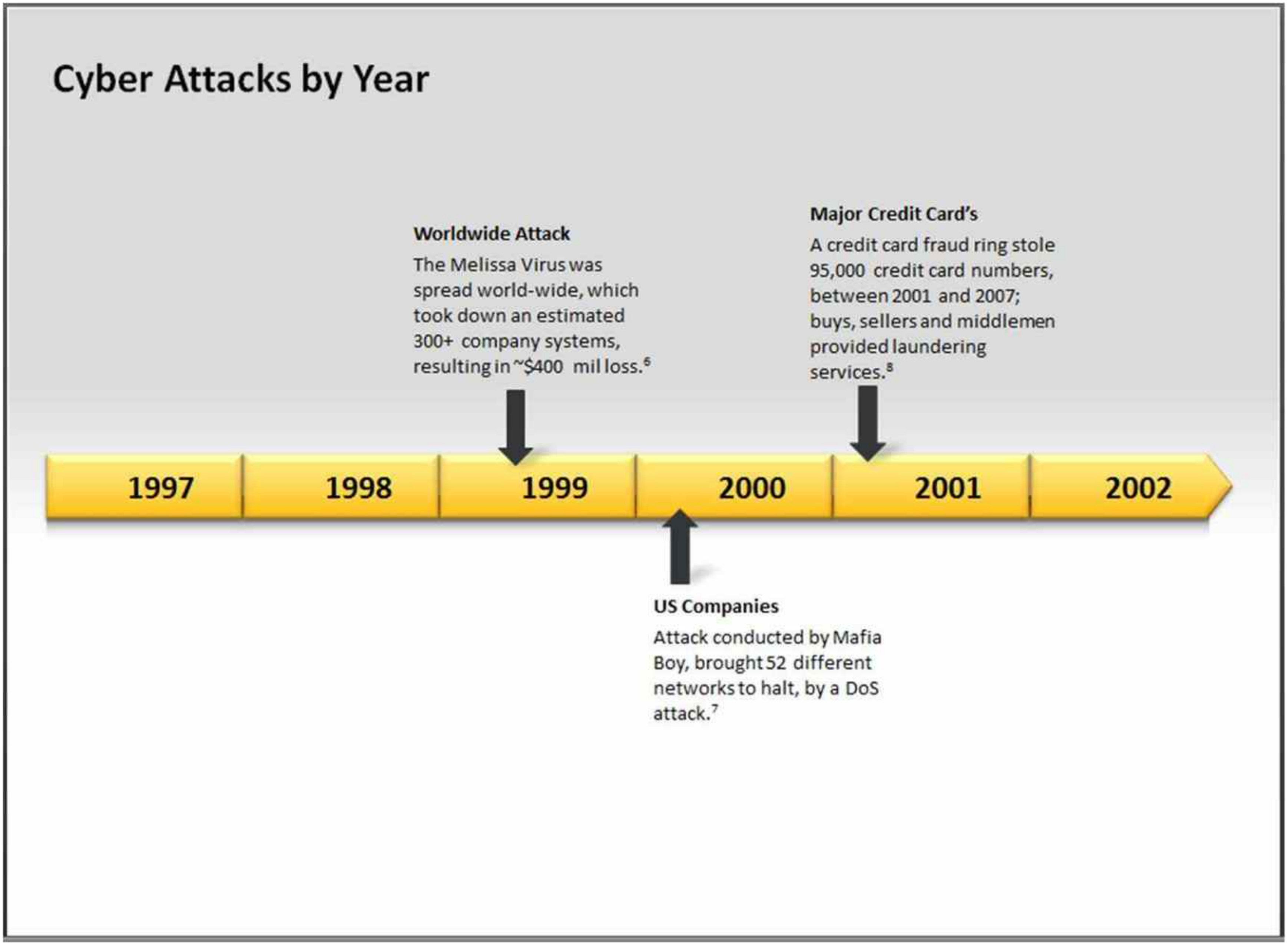
The bank was targeted for an estimated $70 mil.[3]



Cyber Attacks by Year

Bank of America, NSA & AT&T

Phone systems were hacked by a group named Masters of Deception, who used the hacked services for free telephone calls.[5]



Cyber Attacks by Year

Worldwide Attack

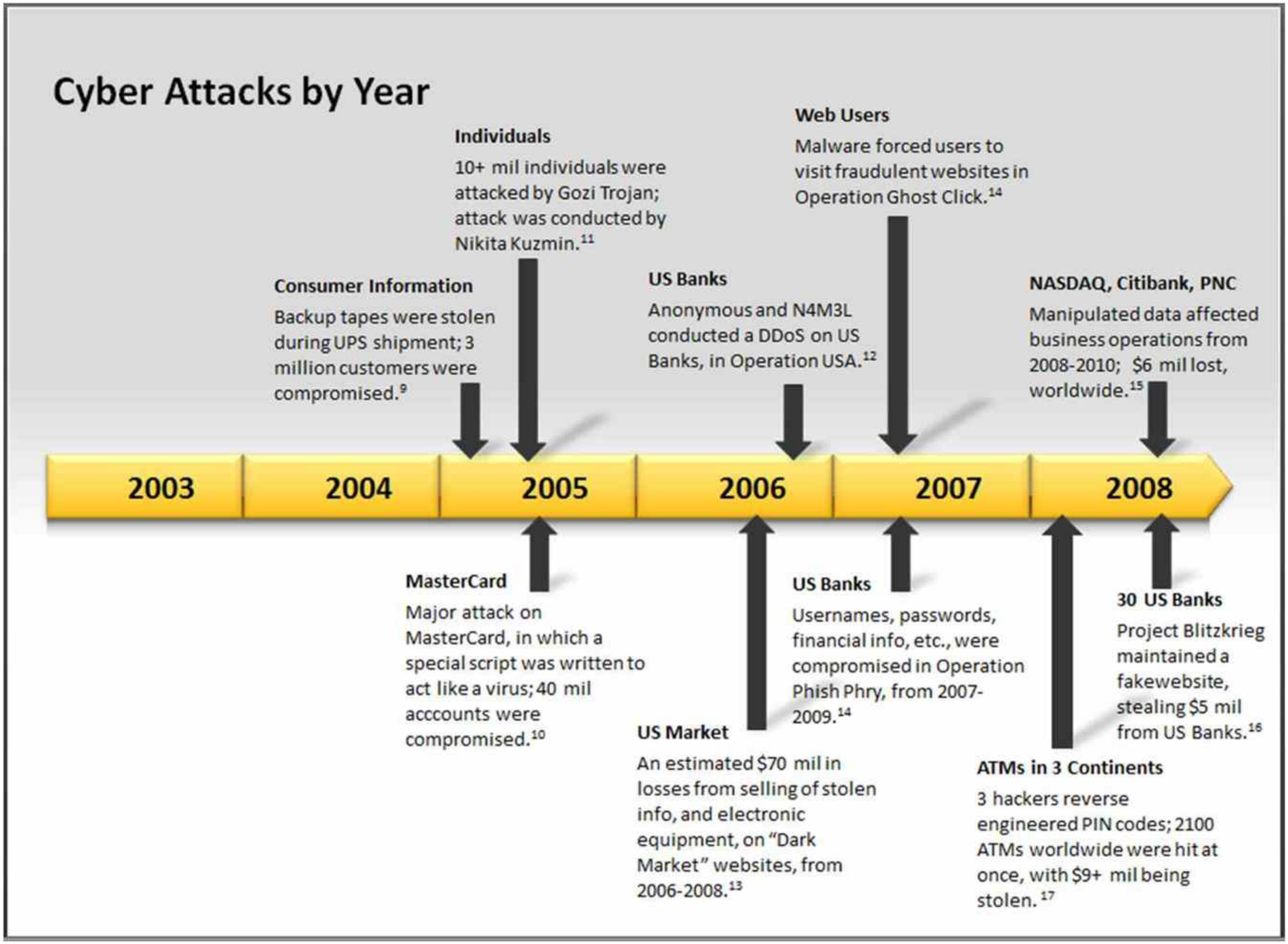
The Melissa Virus was spread world-wide, which took down an estimated 300+ company systems, resulting in ~$400 mil loss.[6]

US Companies

Attack conducted by Mafia Boy, brought 52 different networks to halt, by a DoS attack.[7]

Major Credit Card's

A credit card fraud ring stole 95,000 credit card numbers, between 2001 and 2007; buys, sellers and middlemen provided laundering services.[8]



Cyber Attacks by Year

Consumer Information

Backup tapes were stolen during UPS shipment; 3 million customers were compromised.[9]

Individuals

10+ mil individuals were attacked by Gozi Trojan; attack was conducted by Nikita Kuzmin.[11]

MasterCard

Major attack on MasterCard, in which a special script was written to act like a virus; 40 mil acccounts were compromised.[10]

US Banks

Anonymous and N4M3L conducted a DDoS on US Banks, in Operation USA.[12]

US Market

An estimated $70 mil in losses from selling of stolen info, and electronic equipment, on "Dark Market" websites, from 2006-2008.[13]

Web Users

Malware forced users to visit fraudulent websites in Operation Ghost Click.[14]

US Banks

Usernames, passwords, financial info, etc., were compromised in Operation Phish Phry, from 2007-2009.[14]

NASDAQ, Citibank, PNC

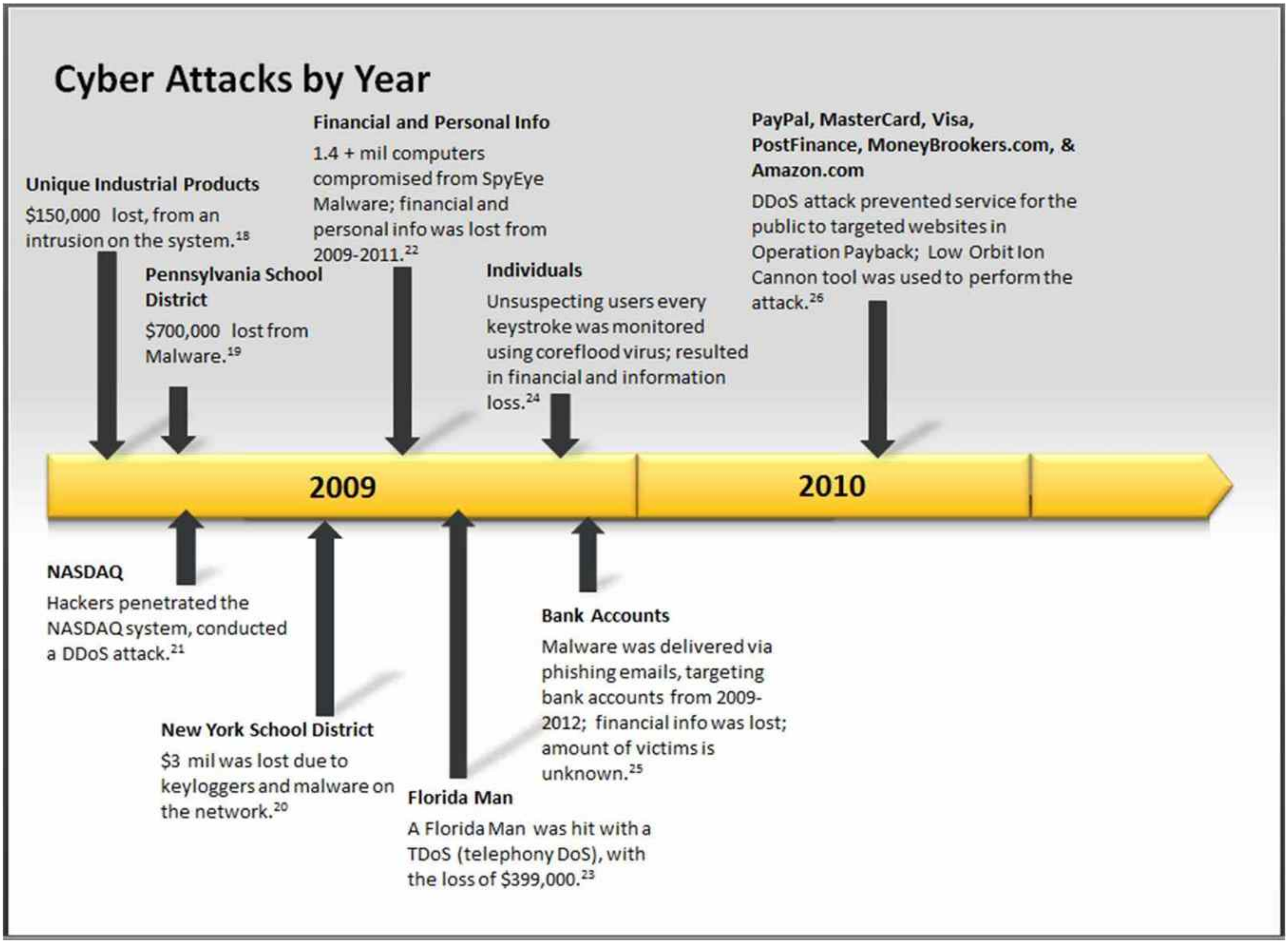
Manipulated data affected business operations from 2008-2010; $6 mil lost, worldwide.[15]

ATMs in 3 Continents

3 hackers reverse engineered PIN codes; 2100 ATMs worldwide were hit at once, with $9+ mil being stolen.[17]

30 US Banks

Project Blitzkrieg maintained a fakewebsite, stealing $5 mil from US Banks.[16]



Cyber Attacks by Year

Unique Industrial Products

$150,000 lost, from an intrusion on the system.[18]

Pennsylvania School District

$700,000 lost from Malware.[19]

Financial and Personal Info

1.4 + mil computers compromised from SpyEye Malware; financial and personal info was lost from 2009-2011.[22]

Individuals

Unsuspecting users every keystroke was monitored using coreflood virus; resulted in financial and information loss.[24]

PayPal, MasterCard, Visa, PostFinance, MoneyBrookers.com, & Amazon.com

DDoS attack prevented service for the public to targeted websites in Operation Payback; Low Orbit Ion Cannon tool was used to perform the attack.[26]

NASDAQ

Hackers penetrated the NASDAQ system, conducted a DDoS attack.[21]

New York School District

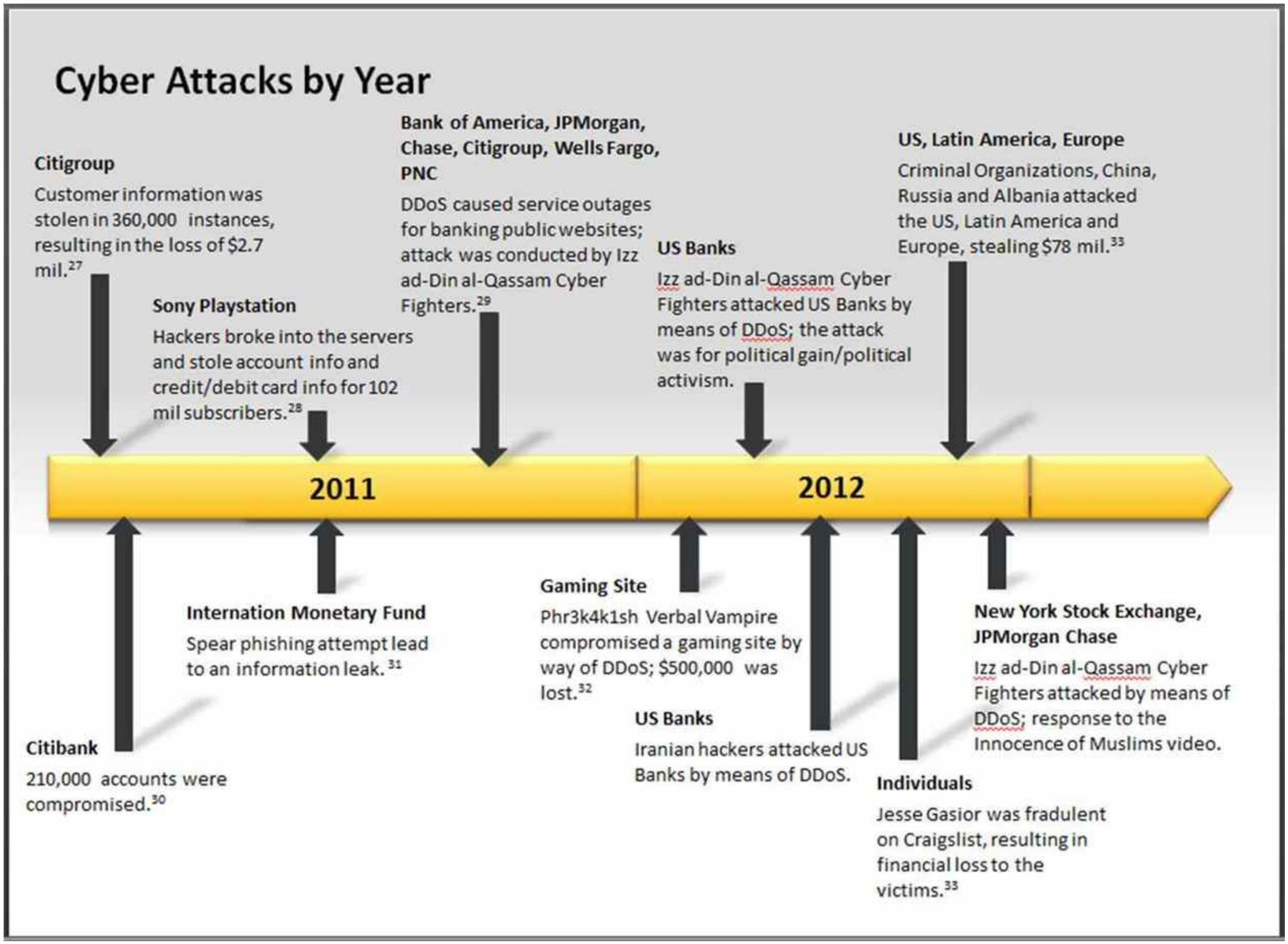
$3 mil was lost due to keyloggers and malware on the network.[20]

Florida Man

A Florida Man was hit with a TDoS (telephony DoS), with the loss of $399,000.[23]

Bank Accounts

Malware was delivered via phishing emails, targeting bank accounts from 2009-2012; financial info was lost; amount of victims is unknown.[25]



Cyber Attacks by Year

Citigroup

Customer information was stolen in 360,000 instances, resulting in the loss of $2.7 mil.[27]

Sony Playstation

Hackers broke into the servers and stole account info and credit/debit card info for 102 mil subscribers.[28]

Bank of America, JPMorgan, Chase, Citigroup, Wells Fargo, PNC

DDoS caused service outages for banking public websites; attack was conducted by Izz ad-Din al-Qassam Cyber Fighters.[29]

US Banks

Izz ad-Din al-Qassam Cyber Fighters attacked US Banks by means of DDoS; the attack was for political gain/political activism.

US, Latin America, Europe

Criminal Organizations, China, Russia and Albania attacked the US, Latin America and Europe, stealing $78 mil.[33]

Citibank

210,000 accounts were compromised.[30]

Internation Monetary Fund

Spear phishing attempt lead to an information leak. [31]

Gaming Site

Phr3k4k1sh Verbal Vampire compromised a gaming site by way of DDoS; $500,000 was lost.[32]

US Banks

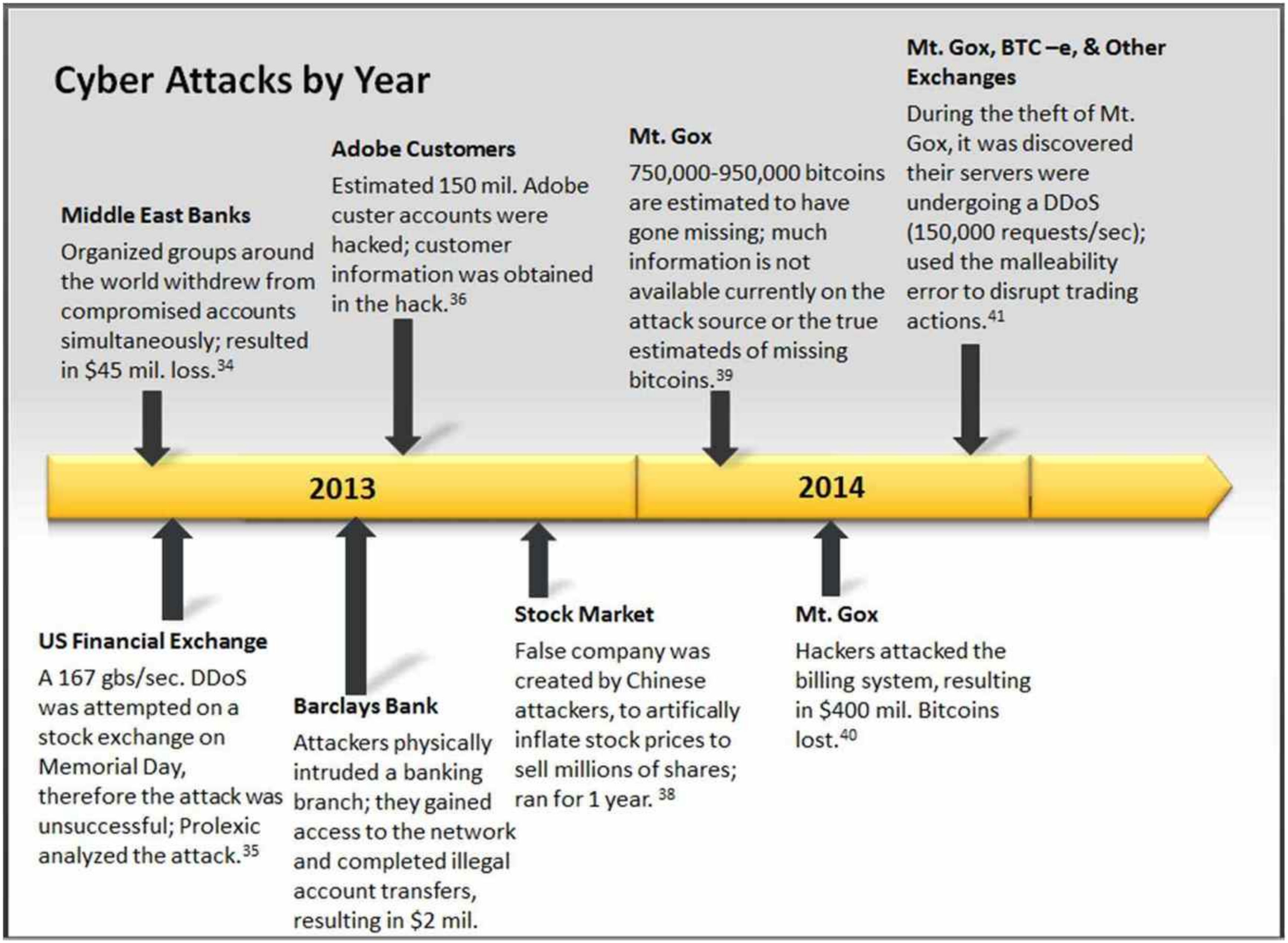
Iranian hackers attacked US Banks by means of DDoS.

Individuals

Jesse Gasior was fradulent on Craigslist, resulting in financial loss to the victims.[33]

New York Stock Exchange, JPMorgan Chase

Izz ad-Din al-Qassam Cyber Fighters attacked by means of DDoS; response to the Innocence of Muslims video.



Cyber Attacks by Year

Middle East Banks

Organized groups around the world withdrew from compromised accounts simultaneously; resulted in $45 mil. loss.[34]

Adobe Customers

Estimated 150 mil. Adobe custer accounts were hacked; customer information was obtained in the hack.[36]

Mt. Gox

750,000-950,000 bitcoins are estimated to have gone missing; much information is not available currently on the attack source or the true estimateds of missing bitcoins.[39]

Mt. Gox, BTC –e, & Other Exchanges

During the theft of Mt. Gox, it was discovered their servers were undergoing a DDoS (150,000 requests/sec); used the malleability error to disrupt trading actions.[41]

US Financial Exchange

A 167 gbs/sec. DDoS was attempted on a stock exchange on Memorial Day, therefore the attack was unsuccessful; Prolexic analyzed the attack.[35]

Barclays Bank

Attackers physically intruded a banking branch; they gained access to the network and completed illegal account transfers, resulting in $2 mil.

Stock Market

False company was created by Chinese attackers, to artifically inflate stock prices to sell millions of shares; ran for 1 year. [38]

Mt. Gox

Hackers attacked the billing system, resulting in $400 mil. Bitcoins lost.[40]

Table of Attacks

S. YEAR	E. YEAR	NAME	TARGET	OUTCOME	ATTACK TYPE (KEYWORDS) ADVERSARY	SOURCE OF ATTACK (WHO)	SOURCE S OF ATTACK TYPE	MOTIV.	DESCRIPTION	SOURCE
1970	1973	Jerome Kerviel	Union Dime Savings Bank	$1.5 million stolen	Theft	American	Multiple	Financial		Whiteside 1979, Harrington, E. B. (2012). The sociology of financial fraud.,Finel-Honigman, I. (2009). A cultural history of finance. Routledge.
1971	1971	TRW Credit Data	TRW Credit Data	Enabled further crime	Fraud	Americans	Multiple	Financial		Whiteside 1979
1973	1973	Equity Funding Corporation of America Scandal	Equity Funding	$150 million in losses	Fraud	Americans	Multiple	Financial		Whiteside 1979, Dirks, R. L., & Gross, L. (1974). The Great Wall Street Scandal (pp. 57-64). McGraw-Hill., Ermann, M. D., & Lundman, R. J. (1982). Corporate deviance. New York: Holt, Rinehart, and Winston.
1988	1988	First National Bank of Chicago heist	First National Bank of Chicago	targeted for an estimated $70 million	Theft	unknown	Unknown	Financial	The First National Bank of Chicago was attacked during a "computer heist". An estimated $70 million dollars was targeted.	Trigaux, 2000 (will try to find more sources to cross reference numbers),Forester, T., & Morrison, P. (1990). Computer crime: new problem for the information society. Prometheus, 8(2), 257-272.
1989	2014	Superbills	United States Federal Reserve	$15 million per year to the DPRK	Counterfeiting	North Korea	Nation-state	Financial	North Korea counterfeits high quality $100US bills.	Nanto, 2009, Perl, R. F., & Nanto, D. K. (2006). North Korean counterfeiting of US currency. Currency Interventions, Fluctuations and Economic Issues, 71., Gaylord, M. S. (2008). The Banco Delta Asia affair: The USA patriot act and allegations of money laundering in Macau. Crime, law and social change, 50(4-5), 293-305.
1993	-	Masters of Deception	Bank of America NSA, & AT&T	phone systems were hacked	Intrusion	Masters of Deception	Group	Financial	The phone systems of. few companies including Bank of America, the NSA and AT&T were hacked by a group to use the hacked services for free calls	Riggs, B. (1993). Masters of deception trial brought to a close. Computer Fraud & Security Bulletin, 1993(12), 8-9.

1999		Melissa virus	World Wide	took down around 300 company systems resulting in an estimated $400 million loss	Intrusion	David Smith	Individual	Inconclusive	David Smith released the Melissa virus and it spread like a wild fire to different systems all around the world. An estimated 300+ companies were affected and an estimated $400 million was at loss	HacknMod, 2013., Garber, Lee, "Melissa Virus Creates a New Type of Threat," Computer , vol.32, no.6, pp.16,19, June 1999 doi: 10.1109/MC.1999.769438. Gold, Jeffrey Chicago Daily Law Bulletin, Dec 9, 1999, Vol.145(240), p.1
2000		Mafia Boy	U.S. companies	52 different networks were brought to a halt	DoS	Mafia Boy	Individual	Inconclusive	about 75 computers spread over 52 different networks were brought down after a DoS attack from 'Mafia Boy'.	Travis, 2013., Gary Genosko Fibreculture Journal, 2006(9).,Hancock, Bill Computers & Security, 2000, Vol.19(6), pp.496-496
2001	2007	Credit card fraud ring	Credit card number trafficking, identity theft	95,000 credit card numbers	Theft	Unknown	Unknown	Financial	Fraud ring trafficking in stolen information. Ring contained buyers, sellers and middlemen providing laundering services. Relied on digital currency.	White Collar Crime Center, 2014
2005	2005	Backup tapes stolen during UPS shipment	Consumer information	3.900,000 customers compromised	Theft	Unknown	Unknown	Financial	Backup tapes stolen during shipment	Privacy Rights Clearinghouse, 2014., Zeller, t., (2005, June 7). New York Times.
2005		MasterCard major attack	MasterCard	40 million compromised accounts	Intrusion	unknown	Unknown	Financial	MasterCard was attacked by what was described as a 'special script which acted like a virus'. This attack resulted in around 40 million accounts to be compromised.	Sahadi, 2005., Dash, E. & Zeller, T. (2005, June18). New York Times.
2005	2005	Gozi	Individuals	$10 Million +	Intrusion	Nikita Kuzmin	Group	Financial		Albanesius, 2013., United States V. Kuzmin, Nikita 11Cr. 387. Federal Bureau of Investigation (2013, January 23). Three alleged international cyber criminals responsible for creating and distributing virus that infected over one million computers and caused tens of millions of dollars in losses charged in Manhattan federal court. New York Field Office.
2013	2013	Operation USA	US Banks	N/A	DoS	Anonymous, N4M3LE55	Group	Political		Rail, 2013, Kovacs, 2013.,

					CR3W				
2006	2008	‘Dark Market’ Takedown	sell stolen financial information, and electronic equipment for carrying out financial crimes	$70 million in potential losses	Theft	56 arrests worldwide	Multiple	Financial	established websites called “Dark Market,” where they bought and sold credentials and other illegal information	‘Dark Market’ Takedown, 2008., FBI (2008). Dark Market Takedown. Exclusive Cyber Club for Crooks Exposed. Greenberg, A. (2013). End of the Silk Road.
2007	2009	Operation Phish Phry	usernames, passwords, financial account details et al.	U.S. banks, and more than 1000 victims; about $1.5 million lost	Intrusion	Nearly 100 people charged	Multiple	Financial	Operation Phish Phry, cyber fraud: cheat the users to give sensitive information	Operation Phish Phry, 2009. FBI (2009). Operation phish phry, major cyber fraud takedown. Retrieved from http://www.fbi.gov/news/stories/2009/october/phishphry_100709. inger, B. (2012, May 15). Feds catch their illegal limit in operation phish phry. Forbes. Retrieved from http://www.forbes.com/sites/billsinger/2012/05/15/feds-catch-their-illegal-limit-in-operation-phish-phry/
2007	2011	Operation Ghost Click	manipulate users' web activity like to visit webs unknown	infect about 4 million computers; 500,000 infections in the U.S; at least $14 million lost	Intrusion	a sophisticated Internet fraud ring, six people arrested	Multiple	Financial	DNS malware is used to force customers to fraudulent websites	Operation Ghost Click, 2011. FBI (2011). International cyber ring that infected millions of computers dismantled. Retrieved from http://www.fbi.gov/news/stories/2011/november/malware_110911. Arthur, C. (2011, November 10). FBI shuts down ghost click botnet of 4m pcs as 7 face charges. Retrieved from http://www.theguardian.com/technology/2011/nov/10/ghost-click-botnet-infected-computers-millions
2008	2010	Kalinin and Nasenkov	NASDAQ servers, Citibank, PNC	monetary loss	Intrusion	Kalinin and Nasenkov	Unknown	Financial	Manipulated data to affect business operations of NASDAQ. Stole over 6 million dollars from over 400,000 accounts by stealing account information, creating debit cards and withdrawing money from ATMs all over the world	US Attorney’s Office, 2013. Beekman, D. (2013, July 26). U.S Hackers hit companies like Nasdaq, 7-Eleven for $300 million, prosecutors say. NY Daily News. Retrieved from http://www.nydailynews.com/news/national/russians-ukrainian-charged-largest-hacking-spree-u-s-history-article-1.1408948#ixzz3090hSFfQ Retrieved from http://www.nydailynews.com/news/national/russians-ukrainian-charged-largest-hacking-spree-u-s-history-article-1.1408948#ixzz3090hSFfQ
2008	2008	Project Blitzkrieg	30 U.S. Banks	$5 Million	Intrusion	vorVzakone	Individual	Financial		Sherstobitoff, 2012, Tsukayama, 2012, Krebs, 2012. Kerr, D. (2012). Threat of mas cyberattacks on u.s. banks is real, MacAfee warns. CNET. Retrieved from http://www.cnet.com/news/threat-of-mass-cyberattacks-on-u-s-banks-is-real-mcafee-warns/

2008	2008	2,100 ATMs Worldwide Hit at Once	cashes in the ATM from three continents	the thieves walked off with a total of more than $9 million in cash	Intrusion	Three 20-something Eastern Europeans and an unnamed person called simply “Hacker 3.”	Multiple	Financial	reverse-engineered the PIN codes from the encrypted system, and raised money that could be withdrawn from debit cards	High-Tech Heist, 2009. FBI (2009). 2100 High tech heist: ATMs hit at once. Retrieved from http://www.fbi.gov/news/stories/2009/november/atm_111609. Wlasuk, A. (2011). How to steal 20 million dollars in a single day. Business Computing World. Retrieved from http://www.businesscomputingworld.co.uk/how-to-steal-13-million-dollars-in-a-single-day/
2009	2009	Unique Industrial Products	Unique Industrial Products	150000	Intrusion	Unknown	Group	Financial		McMillian, 2009
2009	2009	Pennsylvania School district	Pennsylvania School district	700000	Intrusion	Unknown	Group	Financial		Associated Press, 2009. FBI (2011). Cyber security: Threats to the financial sector. Retrieved from http://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector
2009	2009	New York School District	New York School District	$3 Million	Intrusion	Unknown	Group	Financial		Schaffhauser, 2010. FBI (2009). Cyber security: Threats to the financial sector. Retrieved fromhttp://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector
2009	2009	Nasdaq hit by Hackers	NASDAQ	0	DoS	Unknown	Group	Financial		Whittaker, 2013
2009	2011	Botnet Bust	financial and personally identifiable information	infected more than 1.4 million computers, cause financial and personally identifiable information lost	Intrusion	Aleksandr Andreevich Panin conspired with others, including Hamza Bendelladj	Multiple	Financial	advertise and develop various versions of SpyEye in online criminal forums	“Botnet Bust,” 2014. FBI (2014). SpyEye mastermind pleads guilty. Retrieved from http://www.fbi.gov/news/stories/2014/january/spyeye-malware-mastermind-pleads-guilty/spyeye-malware-mastermind-pleads-guilty. U.S. Attorney’s office. (2014). Cybercriminal pleads guilty to developing and distributing notorious spyeye malware. Retrieved from http://www.justice.gov/usao/gan/press/2014/01-28-14.html
2009	2009	Florida TDoS	Florida man	399000	DoS	Unknown	Group	Financial		KnowB4, 2011. Spoto, D. (2011). CyberCrime extracts $399,000 from Florida dentists’ account; Internet security awareness could have thwarted attack. PRWeb. Retrieved from http://www.prweb.com/releases/2011/4/prweb8338409.htm. Holtfreter, R.E. (2011). Identity thieves could have your number. Fraud. Retrieved from http://www.fraud-magazine.com/article.aspx?id=4294969152
2009	2009	Botnet Operation Disabled	recording unsuspecting users’ every keystroke; control the servers	Botnet Operation Disabled; personal and financial information lost	Intrusion	A high-tech group, with no one caught	Multiple	Inconclusive	Coreflood virus as key program to remotely control PCs illegally	Botnet Operation Disabled, 2011., Zetter, K. (2011). With court order, FBI hijacks coreflood botnet, sends kill signal. Wired. Retrieved from http://www.wired.com/2011/04/coreflood/. US-CERT (2012). Coreflood Trojan botnet. Retrieved from https://www.us-cert.gov/security-publications/technical-information-paper-coreflood-trojan-botnet

2009	2012	Malware Targets Bank Accounts	Bank Accounts	financial information lost, the number of people who are infected remains unknown	Intrusion	Unknown hackers	Group	Financial	Delivered via Phishing E-Mails, once be on the website, automatically download the malware	Malware Targets Bank Accounts, 2012. FBI (2012). Gameover malware targets bank accounts. Retrieved from http://www.fbi.gov/news/stories/2012/january/malware_010612/malware_010612.
2010	2011	Operation Payback	PayPal, MasterCard, Visa, PostFinance , MoneyBrookers.com, Amazon.com	varying levels of service outages for the public websites of the targets	DoS	people under the umbrella Anonymous , 13 indicted formally	Group	Political	a reactionary DDOS attack on many websites using the Low Orbit Ion Cannon (LOIC) tool. The trigger event was financial institutions ceasing to process transactions to the WikiLeaks organizations. **The information on this attack greatly varies, read about 20 reports, varying from assessments of mass havoc on the targets to being nothing more than an annoyance.	Pras, A., Sperotto, A., Moura, G., Drago, I., Barbosa, R., Sadre, R., ... & Hofstede, R. (2010). Attacks by “Anonymous” WikiLeaks proponents not anonymous.Laville, S. (2012). Anonymous cyber attacks cost paypal 3.5 million. The Guardian Retrieved from http://www.theguardian.com/technology/2012/nov/22/anonymous-cyber-attacks-paypal-court. Schwartz, M.j. (2013). Operation payback: Feds charge 13 on anonymous attacks. Dark Reading. Retrieved from http://www.darkreading.com/attacks-and-breaches/operation-payback-feds-charge-13-on-anonymous-attacks/d/d-id/1111819?
2011	2011	Citigroup Attack	Citigroup	360,000 instances of customer information were stolen, or 3400 accounts for 2.7 million	Intrusion	unknown	Unknown	Financial	basically a url/resource locater traversal attack was left open on the wb app since 2008. Aguably a major case of negligence. Other than that really few details about the attack	Booton, J. (2011). Hackers Gain Data Access to 200,000 Citi Bank Cards. McMillan, R. (2011). Citigroup hackers made 2.7 million. ComputerWorld. Retrieved from http://www.computerworld.com/s/article/9217932/Citigroup_hackers_made_2.7_million. Smith, A. (2011). Citi: Millions stolen in may hack attack. CNN. Retrieved from http://money.cnn.com/2011/06/27/technology/citi_credit_card/
2011	2011	Sony PlayStation attack	Sony PlayStation servers	monetary loss	Intrusion		Group	Financial	Hackers broke into Sony PlayStation servers and stole account information such as login and password, and credit/debit card info for over 102 million subscribers	Shackelford, 2012. Richmond, S. (2011). Millions of internet users hit by massive Sony PlayStation data theft. London Telegraph. Retrieved from http://www.telegraph.co.uk/technology/news/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html. Reynolds, I. (2011). Sony CEO apologizes for data theft; shares fall 2 percent. Reuters. Retrieved from http://www.reuters.com/article/2011/05/06/uk-sony-idUKLNE74505420110506?type=companyNews

2011	2011	Bank of America, JPMorgan, Chase, Citigroup, Wells Fargo Attack	Bank of America, JPMorgan, Chase, Citigroup, Wells Fargo, PNC	varying levels of service outages for the public websites of the targets	DoS	Izz ad-Din al-Qassam Cyber Fighters	Nation-State	Political	peak levels were 70 GPS, analyzed by Prolexic company. The attack tool utilized was itsoknoproblembro (similar to LOIC but more features) where there are different types of flood attacks and configurations(SSL, TCP, ICMP...) and can do multiple attacks simultaneously. Also, this level of traffic is much beyond the source of a few participating hacktavists, this required sufficient resources.	Finkle,J. (2012, September).Exclusive: Iranian hackers target Bank of America, JP Morgan, Citi| Reuters. Retrieved March 2014, from http://www.reuters.com/article/2012/09/21/us-iran-cyberattacks-idUSBRE88K12H20120921. Nkashima, E. (2012). Iran blamed for cyberattacks on U.S. banks and companies. Washington Post. retrieved from http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html
2011		Citibank part 2	Citibank	210,000 accounts to be compromised	unknown	unknown	Unknown	Inconclusive	Citibank was attacked causing around 210,000 accounts to be compromised	Moscaritolo, 2011. Thomas, K. (2011). Citigroup hacks nabs data from 210k customers. PCWorld. Retrieved from http://www.pcworld.com/article/229891/Citigroup_Hack_Nets_Over_200k_in_Stolen_Customer_Details.html. International Business Times. (2011). Citigroup admits data breach after a month, 210,000 customer information hacked. Retrieved from http://www.ibtimes.com/citigroup-admits-data-breach-after-month-210000-customers-information-hacked-644741
2011		IMF attacked	International Monetary Fund (IMF)	Information leak	Intrusion	unknown	Unknown	Inconclusive	IMF was attacked via a spear phishing attack that resulted in an information leak.	Harnden, 2011. NYCIFT (2011). Spear phishing incidents on the rise. Citywide Information Security Awareness Newsletter. Retrieved from http://www.nyc.gov/html/doitt/downloads/pdf/newsletter_security_201106.pdf.
2012	2012	phr3k4k1sh	Gaming Site	500000	DoS	phr34k1sh verbal vampire	Individual	Financial		Internet Crime Complaint Center, 2011
2012	2012	Operation High Roller	U.S., Latin American European	$78 Million	Intrusion	Criminal Organizations: China, Russia, Albania	Group	Financial		Tendulkar, 2013, Menn, 2012. Phneah, E. (2012). Operation high roller auto-targets bank funds. CNET. Retrieved from http://www.cnet.com/news/operation-high-roller-auto-targets-bank-funds/. Sanburn, J. (2012). How exactly do cybercriminals steal 78 million?. Time. Retrieved from http://business.time.com/2012/07/03/how-exactly-do-cyber-criminals-steal-78-million/.

2012	2012	Craigslist Fraud	Individuals	N/A	Fraud	Jesse Gasior	Individual	Financial		Internet Crime Complaint Center, 2012. FBI (2012). Pittsburg man charged with using craigslist to find victims to defraud. Retrieved from http://www.fbi.gov/pittsburgh/press-releases/2012/pittsburgh-man-charged-with-using-craigslist-to-find-victims-to-defraud. Associated Press. (2012, May 23). Pittsburg man charged in craigslist ticket scam. The Denver Post.
2013	2013	ATM Heist/Raid	Middle East Banks	$45 million stolen in worldwide ATM raids	Fraud	multiple connected groups and criminal organizations, an American new York city cell was convicted	Group	Financial	a globally executed bank withdrawal run. Essentially, an organized attack reached its peak when withdrawal groups throughout the world simultaneously withdrew funds from compromised accounts.	Dye, J. (2013, May 9). Huge cyber bank theft spans 27 countries| Reuters. Retrieved from http://www.reuters.com/article/2013/05/09/net-us-usa-crime-cybercrime-idUSBRE9480PZ20130509. Santora, M. (2013, May 9). In hours, thieves took 45 million in atm scheme. NY Times. Kirk, J. (2013, November 13). Six more arrested in breathtaking atm theft. PCWorld.
2013	2013	US Financial Exchange DDOS attempt	US Financial Exchange	attack averted	DoS	unknown	Unknown	Inconclusive	attempted 167 gbs /sec DDOS attempt on a stock exchange, the DDOS protection company Prolexic analyzed it. The attack happened on the memorial holiday and thus no systems were online regardless. No other information on target, possible source etc... Prolexic disclosed the minimum	Egan, M. (2013, May).Financial Exchange Blitzed by Massive Memorial Day Cyber Attack | Fox Business. Retrieved March 2014, from http://www.foxbusiness.com/technology/2013/05/30/financial-exchange-blitzed-by-massive-memorial-day-cyber-attack/. Prolexic. (2013). Ddos attacks against global markets. Retrieved from http://www.prolexic.com/kcresources/white-paper/global-market/DDoS_attacks-against_Global_Markets_whitepaper_US_020314.pdf
2013	2013	Hackers obtain Adobe customer information	Consumer identification and encrypted accounts	Estimated 3 million Adobe account information	Intrusion	Unknown	Unknown	Financial	Adobe products websites hacked to obtain customer information during purchases	Privacy Rights Clearinghouse, 2014. King, R. (2013, October 3). Adobe hacked, 3 million accounts hacked. CNet. Schwartz, M.J. (2013, October 4). Adobe customer security compromised: 7 facts. Information Week.

2013	2013	Barclays Attack	Barclays Bank	$2 million in illegal account transfers, most recovered	Fraud	UK Gang	Group	Financial	Attackers physically placed a router and a keyboard video mouse in one of the branches(meaning physical intrusion). Somehow in an undisclosed manner, this allowed the attackers to gain access to the network and information and thus do illegal account transfers	Dixon, H. (2013, September). Barclays hacking attack gang stole £1.3 million, police say - Telegraph. Retrieved March 2014, from http://www.telegraph.co.uk/news/uknews/crime/10322536/Barclays-hacking-attack-gang-stole-1.3-million-police-say.html. BBC (2013, September 20). Barclays bank computer theft: Eight held over 1.2 million haul. Retrieved from http://www.bbc.com/news/uk-england-24172305
2013	2013	Securities fraud	Stock manipulation	Artificially inflating stock prices to sell millions of shares	Fraud	China based perpetrators	Group	Financial	Created false company on NASDAQ that ran for a year before discovery. Perpetrated a classic 'pump and dump' scheme to bilk investors out of millions.	White Collar Crime, 2104
2014	2014	Mt.Gox Bitcoin exchange data breach attack	Mt. Gox	yet to be determined. Sources report 750000-950000 bitcoins have gone missing	Intrusion?	unknown	Unknown	Inconclusive	There is so much speculation around this breach. At the very least the, exchange itself Mt.Gox is being very sketchy about it. They claim that the well-known "malleability" attack on the bitcoin exchange architecture is responsible for this attack, However, quite recently a study by Swiss researchers stated that only 400 bitcoins could have been stolen by via the malleability attack; aka they are calling "BS" to Mt.Gox's entire argument about how the bitcoins were lost.	Cutler, K. (2014, March). Mt.Gox Posts New Statement On Alleged Bitcoin Theft, Bankruptcy Filing | TechCrunch. Retrieved March 2014, from http://techcrunch.com/2014/03/03/mt-gox-posts-new-statement-on-alleged-theft-bankruptcy-filing/. Popper, N., RAbrams, R. (2014, February 25). Apparent theft at Mt. Gox shakes bitcoin world. Retrieved from http://www.nytimes.com/2014/02/25/business/apparent-theft-at-mt-gox-shakes-bitcoin-world.html

2014	2014	Bitcoin DDOS attack	Mt. Gox, Bitstamp, BTC -e and other exchanges	outages, and more confusion to the entire Mt.Gox narrative	DoS	unknown other than Europe and US IPs	Group	Inconclusive	During the collapse and controversial theft that Mt. Gox went through, their servers were also undergoing a large DDOS attack (150,000 requests/sec). Interestingly the type of DDOS that is occurring utilizes the component of the malleability error to disrupt trading actions.	Hornyak, T. (2014, February 11). Bitcoin exchanges hit by DDoS attacks - Computerworld. Retrieved from http://www.computerworld.com/s/article/9246249/Bitcoin_exchanges_hit_by_DDoS_attacks. Chirgwin, R. (2014, March 10). Mt. Gox fielded massive ddos attack before collapse. Retrived from http://www.theregister.co.uk/2014/03/10/mt_gox_fielded_massive_ddos_attack_before_collapse/
2014	2014	Bitcoin collapse	Mt. Gox Bitcoin exchange	$400 million in bitcoins lost	Intrusion	Unknown hackers	Group	Financial	Hacked into the billing system	Lee, 2014. Greenberg, A. (2014, February 13). Silk road 2.0 'hack' blamed on bitcoin bug, all funds stolen. Forbes.

Sources for Timeline
Whiteside 1979, Harrington, E. B. (2012). The sociology of financial fraud.,Finel-Honigman, I. (2009). A cultural history of finance. Routledge.
Whiteside 1979
Whiteside 1979, Dirks, R. L., & Gross, L. (1974). The Great Wall Street Scandal (pp. 57-64). McGraw-Hill., Ermann, M. D., & Lundman, R. J. (1982). Corporate deviance. New York: Holt, Rinehart, and Winston.
Trigaux, 2000 (will try to find more sources to cross reference numbers),Forester, T., & Morrison, P. (1990). Computer crime: new problem for the information society. Prometheus, 8(2), 257-272.
Nanto, 2009, Perl, R. F., & Nanto, D. K. (2006). North Korean counterfeiting of US currency. Currency Interventions, Fluctuations and Economic Issues, 71., Gaylord, M. S. (2008). The Banco Delta Asia affair: The USA patriot act and allegations of money laundering in Macau. Crime, law and social change, 50(4-5), 293-305.
Riggs, B. (1993). Masters of deception trial brought to a close. Computer Fraud & Security Bulletin, 1993(12), 8-9.
HacknMod, 2013., Garber, Lee, "Melissa Virus Creates a New Type of Threat," Computer , vol.32, no.6, pp.16,19, June 1999 doi: 10.1109/MC.1999.769438. Gold, Jeffrey Chicago Daily Law Bulletin, Dec 9, 1999, Vol.145(240), p.1
Travis, 2013., Gary Genosko Fibreculture Journal, 2006(9).,Hancock, Bill Computers & Security, 2000, Vol.19(6), pp.496-496
White Collar Crime Center, 2014
Privacy Rights Clearinghouse, 2014., Zeller, t., (2005, June 7). New York Times.
Sahadi, 2005., Dash, E. & Zeller, T. (2005, June18). New York Times.
Albanesius, 2013., United States V. Kuzmin, Nikita 11Cr. 387. Federal Bureau of Investigation (2013, January 23). Three alleged international cyber criminals responsible for creating and distributing virus that infected over one million computers and caused tens of millions of dollars in losses charged in Manhattan federal court. New York Field Office.
Rail, 2013, Kovacs, 2013.,
‘Dark Market’ Takedown, 2008., FBI (2008). Dark Market Takedown. Exclusive Cyber Club for Crooks Exposed. Greenberg, A. (2013). End of the Silk Road.
Operation Phish Phry, 2009. FBI (2009). Operation phish phry, major cyber fraud takedown. Retrieved from http://www.fbi.gov/news/stories/2009/october/phishphry_100709. inger, B. (2012, May 15). Feds catch their illegal limit in operation phish phry. Forbes. Retrieved from http://www.forbes.com/sites/billsinger/2012/05/15/feds-catch-their-illegal-limit-in-operation-phish-phry/
Operation Ghost Click, 2011. FBI (2011). International cyber ring that infected millions of computers dismantled. Retrieved from http://www.fbi.gov/news/stories/2011/november/malware_110911. Arthur, C. (2011, November 10). FBI shuts down ghost click botnet of 4m pcs as 7 face charges. Retrieved from http://www.theguardian.com/technology/2011/nov/10/ghost-click-botnet-infected-computers-millions
US Attorney’s Office, 2013. Beekman, D. (2013, July 26). U.S Hackers hit companies like Nasdaq, 7-Eleven for $300 million, prosecutors say. NY Daily News.
Retrieved from http://www.nydailynews.com/news/national/russians-ukrainian-charged-largest-hacking-spree-u-s-history-article-1.1408948#ixzz3090hSFfQ
Sherstobitoff, 2012, Tsukayama, 2012, Krebs, 2012. Kerr, D. (2012). Threat of mas cyberattacks on u.s. banks is real, MacAfee warns. CNET. Retrieved from http://www.cnet.com/news/threat-of-mass-cyberattacks-on-u-s-banks-is-real-mcafee-warns/
High-Tech Heist, 2009. FBI (2009). 2100 High tech heist: ATMs hit at once. Retrieved from http://www.fbi.gov/news/stories/2009/november/atm_111609. Wlasuk, A. (2011). How to steal 20 million dollars in a single day. Business Computing World. Retrieved from http://www.businesscomputingworld.co.uk/how-to-steal-13-million-dollars-in-a-single-day/
McMillian, 2009
Associated Press, 2009. FBI (2011). Cyber security: Threats to the financial sector. Retrieved from http://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector
Schaffhauser, 2010. FBI (2009). Cyber security: Threats to the financial sector. Retrieved fromhttp://www.fbi.gov/news/testimony/cyber-security-threats-to-the-financial-sector
Whittaker, 2013
“Botnet Bust,” 2014. FBI (2014). SpyEye mastermind pleads guilty. Retrieved from http://www.fbi.gov/news/stories/2014/january/spyeye-malware-mastermind-pleads-guilty/spyeye-malware-mastermind-pleads-guilty. U.S. Attorney’s office. (2014). Cybercriminal pleads guilty to developing and distributing notorious spyeye malware. Retrieved from http://www.justice.gov/usao/gan/press/2014/01-28-14.html
KnowB4, 2011. Spoto, D. (2011). CyberCrime extracts $399,000 from Florida dentists’ account; Internet security awareness could have thwarted attack. PRWeb. Retrieved from http://www.prweb.com/releases/2011/4/prweb8338409.htm. Holtfreter, R.E. (2011). Identity thieves could have your number. Fraud. Retrieved from http://www.fraud-magazine.com/article.aspx?id=4294969152

Botnet Operation Disabled, 2011., Zetter, K. (2011). With court order, FBI hijacks coreflood botnet, sends kill signal. Wired. Retrieved from http://www.wired.com/2011/04/coreflood/. US-CERT (2012). Coreflood Trojan botnet. Retrieved from https://www.us-cert.gov/security-publications/technical-information-paper-coreflood-trojan-botnet

Malware Targets Bank Accounts, 2012. FBI (2012). Gameover malware targets bank accounts. Retrieved from http://www.fbi.gov/news/stories/2012/january/malware_010612/malware_010612.

Pras, A., Sperotto, A., Moura, G., Drago, I., Barbosa, R., Sadre, R., ... & Hofstede, R. (2010). Attacks by "Anonymous" WikiLeaks proponents not anonymous.Laville, S. (2012). Anonymous cyber attacks cost paypal 3.5 million. The Guardian Retrieved from http://www.theguardian.com/technology/2012/nov/22/anonymous-cyber-attacks-paypal-court. Schwartz, M.j. (2013). Operation payback: Feds charge 13 on anonymous attacks. Dark Reading. Retrieved from http://www.darkreading.com/attacks-and-breaches/operation-payback-feds-charge-13-on-anonymous-attacks/d/d-id/1111819?

Booton, J. (2011). Hackers Gain Data Access to 200,000 Citi Bank Cards. McMillan, R. (2011). Citigroup hackers made 2.7 million. ComputerWorld. Retrieved from http://www.computerworld.com/s/article/9217932/Citigroup_hackers_made_2.7_million. Smith, A. (2011). Citi: Millions stolen in may hack attack. CNN. Retrieved from http://money.cnn.com/2011/06/27/technology/citi_credit_card/

Shackelford, 2012. Richmond, S. (2011). Millions of internet users hit by massive Sony PlayStation data theft. London Telegraph. Retrieved from http://www.telegraph.co.uk/technology/news/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html. Reynolds, I. (2011). Sony CEO apologizes for data theft; shares fall 2 percent. Reuters. Retrieved from http://www.reuters.com/article/2011/05/06/uk-sony-idUKLNE74505420110506?type=companyNews

Finkle,J. (2012, September).Exclusive: Iranian hackers target Bank of America, JP Morgan, Citi| Reuters. Retrieved March 2014, from http://www.reuters.com/article/2012/09/21/us-iran-cyberattacks-idUSBRE88K12H20120921. Nkashima, E. (2012). Iran blamed for cyberattacks on U.S. banks and companies. Washington Post. retrieved from http://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html

Moscaritolo, 2011. Thomas, K. (2011). Citigroup hacks nabs data from 210k customers. PCWorld. Retrieved from http://www.pcworld.com/article/229891/Citigroup_Hack_Nets_Over_200k_in_Stolen_Customer_Details.html. International Business Times. (2011). Citigroup admits data breach after a month, 210,000 customer information hacked. Retrieved from http://www.ibtimes.com/citigroup-admits-data-breach-after-month-210000-customers-information-hacked-644741

Harnden, 2011. NYCIFT (2011). Spear phishing incidents on the rise. Citywide Information Security Awareness Newsletter. Retrieved from http://www.nyc.gov/html/doitt/downloads/pdf/newsletter_security_201106.pdf.

Internet Crime Complaint Center, 2011

Tendulkar, 2013, Menn, 2012. Phneah, E. (2012). Operation high roller auto-targets bank funds. CNET. Retrieved from http://www.cnet.com/news/operation-high-roller-auto-targets-bank-funds/. Sanburn, J. (2012). How exactly do cybercriminals steal 78 million?. Time. Retrieved from http://business.time.com/2012/07/03/how-exactly-do-cyber-criminals-steal-78-million/.

Internet Crime Complaint Center, 2012. FBI (2012). Pittsburg man charged with using craigslist to find victims to defraud. Retrieved from http://www.fbi.gov/pittsburgh/press-releases/2012/pittsburgh-man-charged-with-using-craigslist-to-find-victims-to-defraud. Associated Press. (2012, May 23). Pittsburg man charged in craigslist ticket scam. The Denver Post.

Dye, J. (2013, May 9). Huge cyber bank theft spans 27 countries| Reuters. Retrieved from http://www.reuters.com/article/2013/05/09/net-us-usa-crime-cybercrime-idUSBRE9480PZ20130509. Santora, M. (2013, May 9). In hours, thieves took 45 million in atm scheme. NY Times. Kirk, J. (2013, November 13). Six more arrested in breathtaking atm theft. PCWorld.

Egan, M. (2013, May).Financial Exchange Blitzed by Massive Memorial Day Cyber Attack | Fox Business. Retrieved March 2014, from http://www.foxbusiness.com/technology/2013/05/30/financial-exchange-blitzed-by-massive-memorial-day-cyber-attack/. Prolexic. (2013). Ddos attacks against global markets. Retrieved from http://www.prolexic.com/kcresources/white-paper/global-market/DDoS_attacks-against_Global_Markets_whitepaper_US_020314.pdf

Privacy Rights Clearinghouse, 2014. King, R. (2013, October 3). Adobe hacked, 3 million accounts hacked. CNet. Schwartz, M.J. (2013, October 4). Adobe customer security compromised: 7 facts. Information Week.

Dixon, H. (2013, September). Barclays hacking attack gang stole £1.3 million, police say - Telegraph. Retrieved March 2014, from http://www.telegraph.co.uk/news/uknews/crime/10322536/Barclays-hacking-attack-gang-stole-1.3-million-police-say.html. BBC (2013, September 20). Barclays bank computer theft: Eight held over 1.2 million haul. Retrieved from http://www.bbc.com/news/uk-england-24172305

White Collar Crime, 2104

Cutler, K. (2014, March). Mt.Gox Posts New Statement On Alleged Bitcoin Theft, Bankruptcy Filing | TechCrunch. Retrieved March 2014, from http://techcrunch.com/2014/03/03/mt-gox-posts-new-statement-on-alleged-theft-bankruptcy-filing/. Popper, N., RAbrams, R. (2014, February 25). Apparent theft at Mt. Gox shakes bitcoin world. Retrieved from http://www.nytimes.com/2014/02/25/business/apparent-theft-at-mt-gox-shakes-bitcoin-world.html

Hornyak, T. (2014, February 11). Bitcoin exchanges hit by DDoS attacks - Computerworld. Retrieved from http://www.computerworld.com/s/article/9246249/Bitcoin_exchanges_hit_by_DDoS_attacks. Chirgwin, R. (2014, March 10). Mt. Gox fielded massive ddos attack before collapse. Retrived from http://www.theregister.co.uk/2014/03/10/mt_gox_fielded_massive_ddos_attack_before_collapse/

Lee, 2014. Greenberg, A. (2014, February 13). Silk road 2.0 'hack' blamed on bitcoin bug, all funds stolen. Forbes.

Case Studies: In Short

Perpetrators: Kalinin and Nasenkov

Event Timeframe: November 2008 – December 2010

Target: NASDAQ servers, Citibank, PNC

Countries with Individuals/Companies Affected: United States, Estonia, Canada, Great Britain, Russia, and Turkey[32].

Purpose: Financial gain

Synopsis: Kalinin and Nasenkov are two Russian hackers who infiltrated NASDAQ stock market operations and installed malicious software and stole and deleted sensitive data that affected business operations. In separate instances, these two hacked into the financial institutions of Citibank and PNC and obtained account data that allowed them to access thousands of individual's bank accounts, allowing them to withdraw millions of dollars fraudulently through ATMs in six different countries[32].

Results: Over six million dollars stolen from approximately 400,000 accounts[32].

Methods: Kalinin and Nasenkov obtained bank account numbers, card verification values, personal identification numbers, then encoded this stolen data onto magnetic strips of plastic ATM cards. This allowed them to withdraw money from victims' accounts through ATMs. Malware placed in the computer network that processed ATM transactions by the hackers recorded data passing over the network and exported it to an external computer[32].

[32] US Attorney's Office. (2013, July 25). Manhattan U.S. attorney and FBI assistant director in charge announce charges against Russian national for hacking

Mt. Gox

Perpetrator(s): Unknown

Event Timeframe: July 2010 – February 2014

Target: Mt. Gox Bitcoin Exchange

Countries with Individuals/Companies Affected: Japan, United States, India, Panama, and all European countries(Cutler, 2014).

Purpose: Financial gain

Synopsis: Mt. Gox was a bitcoin exchange based in Tokyo that experienced security breaches that resulted in around 850,000 bitcoins valued at around $450 million going missing and suspected stolen. It has been reported that 200,000 bitcoins have been recovered in an old digital wallet; speculations include this was a result of mismanagement, fraud, theft, or hackers, however, the investigation is still ongoing as of April 2014 (Cutler, 2014)

Results: Mt. Gox has halted transactions and filed bankruptcy; they still cannot account for 650,000 bitcoins, valued at over $350 million (Cutler, 2014).

Methods: On June 19, 2011, a hacker allegedly compromised a Mt. Gox auditor's computer and illegally dropped the bitcoin price to drop to one cent, then transferred a large quantity of bitcoins to himself/herself. The hacker allegedly used the exchange's software to profit from the fraudulently obtained bitcoins. In October 2011, two dozen transactions that appeared in the block chain sent 2609 BTC to invalid addresses, and the bitcoins were assumed to be lost. The company released a statement on February 10, 2014, claiming that a bug in the bitcoin software makes it possible for someone to alter transaction details to make it appear a transaction did not appear when it in fact did, causing the software to resend the bitcoins since the transaction appear to proceed improperly (Cutler, 2014).

[33] Cutler, K. (2014, March). Mt.Gox Posts New Statement On Alleged Bitcoin Theft, Bankruptcy Filing | TechCrunch. Retrieved March 2014, from http://techcrunch.com/2014/03/03/mt gox posts new statement on alleged theftbankruptcy filing/

Case Study #3

Stock Market Manipulation Scheme

Perpetrators: Sherman Mazur, Ari Kaplan, Grover Nix IV, Regis Possion, Edon Moyal, Mark Harris, Joey Davis, Curtis Platt, Dwight Brunoehler[33].

Event Timeframe: February 2013

Target: US Stock Market

Countries with Individuals/Companies Affected: United States

Purpose: Financial gain

Synopsis: Stock manipulation fraud is not a new concept, but in this recent case, as many as 14 individuals are accused of conspiring in schemes that defrauded investors out of over $30 million. Two large scale fraud schemes occurred where the conspirators gained control of the majority of the stock of publicly traded companies, often co opting company management. They hid their stocks in offshore accounts and manipulated the market to create illegal profits for themselves. The conspirators targeted marginal companies from areas where they could easily advertise breakthroughs to increase trading volume and price, such as pharmaceutical companies, green technology, entertainment, and hair restoration[34].

Results: More than 20,000 investors lost over $30 million when the artificially inflated stock prices collapsed[34].

Methods: Conspirators concealed stock control by purchasing shares and transferring them to offshore accounts. They fraudulently inflated stock prices and trading volumes to exaggerate trading activity and attracted investors through market campaigns and misleading reports[34].

[34] US Attorney's Office. (2013, July 25). Manhattan U.S. attorney and FBI assistant director in charge announce charges against Russian national for hacking

Case Study #4

Project Blitzkrieg

Perpetrator: VorVzakone[35]

Event Timeframe: 2008 – 2012

Target: 30 US Financial Institutions

Countries with Individuals/Companies Affected: United States, Ukraine, Romania, and Russia[34].

Purpose: Financial gain

Synopsis: Project Blitzkrieg was perpetuated by an individual identifying himself/herself as VorVzakone. The ambitious functioning of Project Blitzkrieg and the way it was advertised by VorVzakone led to speculation the event was part of a law enforcement sting, however McAfee's Ryan Sherstobitoff and other security researchers believe the threat was credible[35].

Results: Around five million dollars stolen[35].

Methods: VorVzakone created a Trojan program based off an older piece of malware called Gozi; the new piece of malware has been named Gozi Prinimalka by the RSA. Two versions of the malware have been developed, the first was deployed in 2008 and used command and control servers in the Ukraine. The second was first seen in 2012 and was used against servers hosted in Romania. Both versions of Gozi Prinimalka targeted customers of US Banks by detecting when victims accessed banking websites and stealing log in credentials and associated account data, and then using the fraudulently obtained credentials to transfer money, withdraw funds, and wire the money out of the country[35].

[35] Sherstobitoff, R. (2013). Analyzing Project Blitzkrieg, a Credible Threat (pp. 18). Santa Clara, CA: McAfee Labs.

1973 Union Dime Savings Bank Embezzlement

In Short:
From 1970 1973, a Chief Teller of New York's Union Dime Savings Bank cleverly manipulated the internal account and interest computer system of customer accounts to take assets out of the system[36]. Over 3 years, the teller withdrew $1.5 million (~8 million at current value) without any obstacles from the bank or authorities[37]. Eventually the teller was discovered indirectly by a police operation aimed at illegal gambling, of which the teller was a part of.

Target:
Union Dime Savings Bank branch located at 300 Park Ave in New York City.

Source:
Chief Teller at the Union Dime Savings Bank branch at 300 Park Ave Roswell Steffan. As chief teller, he supervised all the tellers at the branch and had access to the information system that allowed manual alteration of account balances. Roswell was also a 9 year employee of the bank[38].

In Detail:
The mechanics of this attack were relatively straightforward, and just sophisticated enough to not raise alarm. Roswell Steffan simply manually reduced the value of customer accounts that were recorded and withdrew the money. Now at scheduled times, the bank would conduct automated (via the computer account system) interest accumulation for the accounts[38]. Some accounts would be processed on some days while other accounts on others. Roswell Steffan, of course, knew this and would use this protocol to stay undetected. When one set of accounts were up to be processed for interest, Roswell Steffan would make sure if the set of accounts included ones that he withdrew from, he would shift money from other accounts that were not up for interest accumulation. He would repeat this whenever accounts that he had taken from were up for interest accumulation[38]. This went on for 3 years, and reported to be undetected by any authority[36] [37] [39] .

Authorities eventually got a tab on Steffan by an initially unconnected raid on a bookie operation. They had discovered Steffans name extensively on a list for making substantially large bets. It eventually was determined that Steffan was making bets to the turn of many times his annual salary($11,000) almost on a daily basis. Authorities eventually worked with banking officials to confirm Steffans actions[40].

Conclusion:
Another example of an insider attack is this financial embezzlement case was at its core a lack in oversight and trust in the system. No one double checked Steffan's operations and complete trust was laid with the accounting system. The accounting system also had a clear flaw in its operation as it allowed malicious transfers and withdrawals.

[36] Business World (2013, July). Rethinking Banking Rules. Retrieved from http://www.businessworld.in/news/finance/rethinking banking rules/976830/page 1.html

[37] Bishop, M., Peisert, S., Engle, E., Whalen, S., & Gates, C. (2009). Case Studies of an Insider Framework. University of California Davis.

[38] Associated Press (1973, March 23). $1.5 million Fraud Laid to Bank Aid. Toledo Blade[Toledo], p. 10

[39] Associated Press (1973, March 23). Big Embezzlement Charged to Teller. Spokane Chronicle[Spokane], p. 1.

[40] Associated Press (1973, March 23). $1.5 million Fraud Laid to Bank Aid. Toledo Blade[Toledo], p. 10

In depth Case Study #2

1988 First National Bank of Chicago Wire Heist

In Short:
In 1988, 7 individuals attempted to illegally transfer about $69.7 million from the First National Bank of Chicago from the corporate accounts of United Airlines, Merill IYnch& Co. and Brown Forman Corp. through multiple engineered wire transfers[40]. The plan called for 2 transfer hops, the initial transfer of the funds from First National Bank of Chicago to Citibank and Chase Manhattan in New York City, and then subsequently transferred to the Facobank and Creditanstalt banks in Vienna, Austria[40]. The funds did go through the first transfer to the New York City banks but were halted by authorities before being transferred to the Vienna banks[41].

Target:
The First National Bank of Chicago (aka First Chicago at the time) was the target of the 1988 plot[41]. The bank was a Chicago based retail and commercial bank that started in 1983. The bank experienced many mergers and was eventually merged under Chase. The specific component of First Chicago that was targeted was the over the phone wire transfer service[42]. This service allowed account holders with the appropriate credentials to call in and request wire transfers[42].

Source:
The source of the attempted heist were 7 individuals, 2 of which were low level employees of the First National Bank of Chicago[40]. The two employees were Otis Wilson and Gabriel Taylor. Wilson was reported to be a clerk and Taylor worked in the wire transfer department[41, 42]. The other individuals were Armand Moore, Neal Jackson, Leonard Strickland, Ronald Carson and Herschel Bailey[42]. It was stated at the time by US Attorney Anton Valukas that the leader of the group was Armand Moore[41]. This was also concluded in where Moore was said to be the initiator of the, LA times operation[41].

Attack Details:
The planning the operation was reported to have begun in March 1988 when Armand Moore questioned Herschel Bailey if he knew anyone who worked at First Chicago[42]. Herschel Bailey responded that he knew Otis Wilson, who was a bank teller at First Chicago[42]. Otis Wilson, the brought in Gabriel Taylor, was also an employee of the bank, but worked as a wire transfer clerk[42, 43].Gabriel Taylor was key as he held the pivotal position of being able to legally conduct wire transfers. He provided account numbers and credentials of target accounts to the group[43]. The plan was for one of the other members to call Gabriel Taylor at the bank (while working) and place a wire transfer request with him[44, 45]. The wire request would appear legitimate as the fake requester's had the legitimate account numbers and appropriate credentials.

[41] Secter, B. (1988, May 18). 7 Charged in $70 Million Chicago Bank Embezzlement Scheme   Los Angeles Times. Retrieved from http://articles.latimes.com/1988 05 19/news/mn 4838_1_embezzlement scheme

[42] Associated Press (1989, June 8). High Tech Heist Almost Paid Off. Spokane Chronicle[Spokane], p. 1.

[43] Possley, M., & Cohen, L. (1988, May 19). $70 Million Bank Theft Foiled   Chicago Tribune. Retrieved from http://articles.chicago tribune.com/1988 05 19/news/8803180387_1_chase manhattan bank wire transfers sources

[44] Associated Press (1989, June 8). High Tech Heist Almost Paid Off. Spokane Chronicle[Spokane], p. 1.

[45] Possley, M., & Cohen, L. (1988, May 19). $70 Million Bank Theft Foiled   Chicago Tribune. Retrieved from http://articles.chicago tribune.com/1988 05 19/news/8803180387_1_chase manhattan bank wire transfers sources

At this point, the three other members were also established within the group and the operation was set. On May 13, 1988 Herschel Bailey posing as a representative from Merrill Lynch called Gabriel Taylor to conduct a wire transfer to the tune of $24.37 million from Merill Lynch account at First Chicago to a bank in New York(either Chase Manhattan or Citibank)[44]. Gabriel Taylor processed the request like any other and followed procedure. Gabriel Taylor also called back Herschel Bailey back using Herschel Bailey's home number to confirm the wire transfer, as if he was calling back a Merill Lynch representative at the company[44]. The importance of this was that it was the policy of First Chicago to record all wire transfer phone calls and check that the correct transaction protocol was carried out. For all purposes, the transfer was valid. After a short period time when the team was certain the transfer had worked, they conducted two more wire transfers via the exact same method. The second transfer was for $19.75 million from an account of the Brown Forman Corp., and the third(final) transfer was for $25 million from an account of United Airlines[45] [46].

In essence, the operation was a success for about a day, or until the financial personnel at each companies checked their account statements the following morning[44] [45]. According to all 3 companies, all of them noticed the large overdraft of their accounts first thing in the morning[44] [45] [46]. The attack itself occurred on a Sunday, thus the reason why they did not notice the transfers until the following morning. Once the bank was notified, so were appropriate authorities (FBI). Securing the money was trivial as the New York banks were notified immediately and just froze the accounts; to eventually be returned[45]. When it came to determining and locating the attackers, the attackers made a crucial mistake. When, in the original plan where Gabriel Taylor made the transfer verification phone call, the call was made to Herschel Bailey's house. As per protocol, all calls involving wire transfers are recorded, and without trouble the phone number of Herschel Bailey's residence was determined rather quickly[45].

It is worth to note that the attackers also had another major flaw in the operational plan (besides the phone number one of the attackers on record), the value of the wire transfers. Three transfers, no less than $19.75 million each is and was likely to be noticeable by parties at the bank and the clients themselves[46]. It’s hard to retroactively determine at what value level would have been more successful, but it was not seven figure transfers.

Conclusion:

An example of an insider attack is this attempted heist highlight the very common insider threat. The only aspect of this attack utilizing a cyber or ICT component was the action of a wire transfer that electronically moved digital account balances from one system to another. While, given more details of the attack, one could argue the attack was primarily an effort in social engineering. However, given the available details, this truly was an insider attack made possible by the utilization of information technology. At the time, the attack was titled a “High Tech Heist” by some media[47], but by any standards was not of the sort. This was an attempted attack on a financial institution by methods that were just sophisticated enough to complete it; or almost.

[46] Secter, B. (1988, May 18). 7 Charged in $70 Million Chicago Bank Embezzlement Scheme   Los Angeles Times. Retrieved from http://articles.latimes.com/1988 05 19/news/mn 4838_1_embezzlement scheme

[47] Possley, M., & Cohen, L. (1988, May 19). $70 Million Bank Theft Foiled   Chicago Tribune. Retrieved from http://articles.chicago tribune.com/1988 05 19/news/8803180387_1_chase manhattan bank wire transfers sources

In depth Case Study #3

1994 Citibank Heist

In short:
There are many rumors and conflicting stories about how this attack was carried out. Essentially there are two versions, one produced by media sources and another by questioning security practitioners and underground hacking collective[48] [49] [50]. The media produced a story that a very intelligent Russian hacker and engineer Vladimir Levin had hacked into CitiCorp Citibank's account information systems, extracting account numbers and passwords of customers[48] [49]. Then at a later time, Levin and his associates made about 40 wire transfers from these accounts to their accounts in banks all over the world[48] [49]. At some point, internal warnings triggered as to possible fraudulent transfers and the scheme was brought to light[48].

The other story, believed and propagated by the hacker culture is that the attack did occur but Vladimir Levin was far from being the infamous hacker he was publicized to be[49]. Simply put, the alternate series of events was that a hacker group had found flaws in Citibank's telecommunication systems and had taken customer account data and "played around" with the system but did so just as a proof of feasibility[50]. Eventually the hacker group, who no interest in exploiting the customer information they had, gave it away. They happened to give it away to Vladimir Levin, a systems administrator working in St. Petersburg. Levin then used the valid information to make wire transfers to his accounts[50].

Target:
Citibank, the consumer banking division of the financial services multinational Citigroup, and more specifically, customers of Citibank.

Source:
Vladimir Levin, either the infamous savvy hacker and software engineer or the little less than superstar systems administrator at AO Saturn from St. Petersburg, Russia. Levin was also stated to have accomplices but all of them were not disclosed publicly[48,49,51]. Katerina Korolkov and Vladamir Voronin were two accomplices caught while trying to withdraw transferred stolen funds from targeted accounts[51].If one takes the latter story of events that the hacker culture has followed, the original source of the attack is the hacker group affiliated with an online persona Akranoid. Assuming this timeline , the aforementioned hacker group was the entity to obtain the customer information, and then Levin is the one who utilized it

.

Attack Details:
First, it must be noted that the details of this attack are questionable at best, regardless of what version one takes to be correct. No entity beyond a media source did a publicly disclosed analysis of the attack.

[48] Harmon, A. (1995, August 19). Hacking Theft of $10 Million From Citibank Revealed   Los Angeles Times. Retrieved from http://articles.latimes.com/1995 08 19/business/fi 36656_1_citibank system

[49] Wall Street Journal (1998, February 24). Russian Hacker Is SentencedTo 3 Years in Citibank Heist   WSJ.com. Re rieved from http://online.wsj.com/news/articles/SB888360434859498000

[49]Akranoid (2005, November 2). Äåëî Ëåâèíà: íåäîñòàþùåå çâåíî | Àâòîðñêèå ñòàòüè | Íåçàâèñèìûé îáçîð ïðîâàéäåðîâ. Retrieved from http://www.providernet.ru/article.37.php

[50] PBS (2001). Who Are Hackers   Notable Hacks | Hackers | FRONTLINE | PBS. Retrieved from http://www.pbs.org/wgbh/pages /frontline/shows/hackers/whoare/notable.html

[51] Denning, D. E. (1999). Information Warfare and Security (1st ed.). New York: ACM Press.

Continued

Nevertheless, the stated events are as follows: Between June and October in 1994, Vladimir Levin and his accomplices utilized the wire transfer service of Citibank to make about 40 transfers to their own accounts distributed in Finland, Russia, Germany, Netherlands and United States .The wire transfers were done over the phone through a dial up service[52] [53] . Levin had the account numbers and credentials to carry out the transfers as if he was the account owner. Thus no social engineering or cleverness was necessitated for the operational aspect. The total amount of the attempted heist was $10 million.

After making a few wire transfers, Citibank noticed and immediately brought in the FBI. As well, Investment Capital SA in Buenos Aires signed on to their account and witnessed a $200,000 transfer being made to an unknown account in San Francisco[56]. The FBI monitored the accounts where the money was transferred to[55]. With some amount of time, the accounts attracted the accomplices of Levin and they went to withdraw the money[55]. The FBI arrested Katerina Korolkov and her husband when she tried to withdraw the funds from the San Francisco account[56]. Intelligence extracted from these accomplices led to the arrest Vladamir Voronin when he tried to withdraw $1 million from an account in Rotterdam, Netherlands[56]. Voronin also gave up information on money mules that he had incorporated into the operation[56].

It was also never explained how Levin got the account numbers and credentials in order to make the transfers to begin with. That is where the support for the alternative story that was produced by an online posting site by someone with the moniker Akranoid[55]. This story states that Levin merely was given the credentials by a “real” hacking collective who were originally obtained the credentials via the perspective of a challenge[55]. Exact details of the method were also not given in the online post by Akranoid[54].

Conclusion:

This financial attack, like the previous case study of the First National Bank of Chicago, targeted the functionality brought upon by wire transfer services. An individual came across active accounts and credentials and decided to use them. Unfortunately there are no details on how the account information was obtained originally. However, this attack is important as it highlights the possibility of attackers who came to be by chance and who normally wouldn't have the opportunity to do so. Additionally, one may argue that the advent if ICT (remote wire transfers) in this case encouraged the attackers to conduct the operation whereas otherwise they wouldn't have physically gone to the bank to do so. However, it is certain that Levin and his accomplices did experience and believe they had a sense of immunity and safety operating in remote parts of the world (comparatively); which is noteworthy trend of crime executed over ICT components and infrastructure.

[52] Harmon, A. (1995, August 19). Hacking Theft of $10 Million From Citibank Revealed   Los Angeles Times. Retrieved rom http://articles.latimes.com/1995 08 19/business/fi 36656_1_citibank system

[53] Wall Street Journal (1998, February 24). Russian Hacker Is SentencedTo 3 Years in Citibank Heist   WSJ.com. Re rieved from http://online.wsj.com/news/articles/SB888360434859498000

[54] PBS (2001). Who Are Hackers   Notable Hacks | Hackers | FRONTLINE | PBS. Retrieved from http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/notable.html

[55] Akranoid (2005, November 2). Äåëî Ëåâèíà: íåäîñòàþùåå çâåíî | Àâòîðñêèå ñòàòüè | Íåçàâèñèìûé îáçîð ïðîâàéäåðîâ. Retrieved from http://www.providernet.ru/article.37.php

[56] Denning, D. E. (1999). Information Warfare and Security (1st ed.). New York: ACM Press.

2008 2012 Project Blitzkrieg

In Short:
On September 9 2012, a forum post was made by the self prescribed notorious hacker called vorVzakone. The post appeared to be a fully outlined call out to other botmasters willing to sign up for an upcoming operation on 30 US banks and financial institutions in Spring 2013. The posting highlighted the basic operational questions, process for qualifying to be in the operation, tech requirements and general information. The post also stated that the malware to be used had been created and further developed since 2008; and that the use of the malware in a "case study" operation had been a success concluding in a $5 million total theft. The hacker, vorVzakone, also posted a video of himself and his house on YouTube[57 58].

Many on both sides wondered if this call out was real, a ruse, or a Russian sting operation. McAfee Labs among other sources claimed that the call out was real and that the sponsoring hacker, vorVzakone, appeared to be legit. However, after the media blew the relative cover of the operation, all sources went dark and it has never been confirmed if the attack occurred. The exposure did lead to an investigation, most notably by McAfee and RSA, into the previous test operation that vorVzakone proudly refers to in the post. After which, McAfee and RSA found those claims by vorVzakone to be plausible and mapped out an operation that appeared to match the profile.

Target:
The initial target was 30 U.S. banks. The target was revealed via the original public post made by vorVzakone, where the specific number 30 was listed twice in regards to how transfers work for said financial institution[59]. RSA and McAfee initially knew the proposed institutions were US institutions because this was also spelled out in the post as well as in an online video of the suspected hacker. vorVzakone appeared to target US institutions for 2 reasons; first, he believed that as long as operations were done solely in the US, he and others were at no risk operating out of Russia and Eastern Europe, and 2) reduced transfer security mechanisms as US institutions did not require 2 factor authentication as is commonly found in Europe[57 58]. The latter point is supported by the fact that vorVzakone had had previous success with US financial institutions[57 60] .

According to the post, the information and details regarding the financial institutions alluded to would only be revealed for those that answered the call out and passed the interview for admittance to the project. In other words, the "30 banks" mentioned were purposely vague but intended to demonstrate that vorVzakone and his team had sufficient attack intelligence on a large subset of banks nonetheless.

After security analysts publicized the attack there were no more public forum posts or communications about the project. Nor was it ever confirmed if the operation was carried out or if the suspected targets experienced such attacks.

[57] Sherstobitoff, R. (2012). Analyzing Project Blitzkrieg, Credible Threat. McAfee Labs

[58] Krebs, B. (n.d.). Project Blitzkrieg: Promises more Aggressive Cyberheists Against U.S. Banks. Retrieved from Krebs on Security website: krebsonsecurity.com/2012/10/project blitzkrieg promises more aggressive cyberheists against u s banks/

[59] Krebs, B. (n.d.). Transcript of hacker vorVzakon forum post for Project Blitzkrieg. Retrieved from Krebs on Security website: krebsonsecurity.com/wp content/uploads/2012/10/VorVzakonePostxlated.txt

[60] Ahuvia, M. (n.d.). Cyber Gang Seeks Botmasters to Wage Massive Wave of Trojan Attacks Against U.S. Banks » Speaking of Security The RSA Blog and Podcast. Retrieved from RSA website: http://blogs.rsa.com/cyber gang seeks botmasters to wage massive wave of trojan attacks against u s banks/

RSA and McAfee did research and discover evidence for the previous "test run" operation that vorVzakone used as evidence of past success. From analyzing control servers belonging to the malicious actors, McAfee traced command and control communication channels to 60+ target hosts in the US. They also determined, via URL trigger values in the malware, over 30 targeted US banks; most of which were national and investment banks[61].

Source:
vorVzakone was viewed as one of, if not the primary, operational leaders of this proposed operation; as he was the only person to openly reveal himself. A unique addition to this operation was that vorVzakone, or the man claiming to be vorVzakone, posted a video on YouTube of his house, neighborhood and two cars. The implication in the message was that vorVzakone was living a normal life with no fear of prosecution or conviction. If indeed this was vorVzakone, this supports the notion that he felt he had complete operational security operating out of Russia.

However, the original forum post as well as conclusions from analysis of McAfee highlight that the operation was expected to have many parties and accomplices. The post itself mentions users, lawyers, tech support, contacts, organizers, curators, callers and verifiers[62]. It's hard to tell if the level of personnel and organization implied to in the original post was accurate, as vorVzakone could and would probably say anything to attract potential team mates. Control servers for the malware kit that vorVzakone was suspected of using were geo located to the Netherlands, Ukraine, Russia, and Romania. This operational detail by itself has little bearing on attributing the actual attackers. However, these locations did match where vorVzakone has been found to operate out of; hence it becomes another supporting detail to the profile.

Attack Details:
The forum post by vorVzakone highlights primarily a financial operation to come as well as a past, similar, financial attack as proof of feasibility for the upcoming operation. Since the upcoming attack, Operation Blitzkrieg, was never confirmed to occur via available evidence, the analysis by McAfee Labs was done on confirming the past attack that vorVzakone claimed to have successfully been conducted. vorVzakone states that the previous "prototype" operation already occurred where the same tactics and strategy was utilized that was being proposed for the upcoming phases. McAfee Labs used this assertion as the premise and started digging.

McAfee and RSA stated that the first hints came from screen shots (also provided by vorVzakone in a post) of the administration tool for the back end of the command and control structure. This along with other undisclosed intelligence allowed researchers to identify the root control server. It should be noted that in the images (screen shots) that McAfee provide in the report are indiscernible so it's hard to provide to further details as to what administration tool was in use. Nevertheless, researchers were able to discover a root IP address corresponding to the control server; again this was for the previous, proof of concept attack that vorVzakone alludes to as evidence/motivation for others join in the

[61] Sherstobitoff, R. (2012). Analyzing Project Blitzkrieg, Credible Threat. McAfee Labs
[62] Krebs, B. (n.d.). Transcript of hacker vorVzakon forum post for Project Blitzkrieg. Retrieved from Krebs on Security website: krebsonsecurity.com/wp content/uploads/2012/10/VorVzakonePostxlated.txt

upcoming operation . Additionally the screen shots provided a list of IPs of what one could only suspect are victims. Essentially McAfee states that through further intelligence gleaned from their proprietary intelligence system, McAfee Global Intelligence System, they confirmed that the other IPs found do in fact correspond to systems infected with a unique malware variant around the time that vorVzakone claims to have conducted his initial pilot run[63].

The unique malware that McAfee and RSA were looking for on these systems was titled Gozi Prinimalka. RSA came to the name by combining two factors: the software resembles another malware kit called Gozi, and the term "Prinimalka" was the name of a file folder used as a dropping point that was found in every instance of the malware seen. "Prinimalka" means "to receive" in Russian; fitting given the file's role in the malware. The Gozi Prinimalka malware kit also had variants of its own, so it identification efforts are axiomatically a little more complex. When analyzing the malware images on these compromised systems though, McAfee states they obtained further confirmation of these attacks being linked to information obtained from the screen shots[61]. McAfee doesn't explicitly state but implies that certain hard coded IP addresses found in the malware images correspond to control server addresses found previously for Gozi Prinimalka[63].

Initially, neither McAfee nor RSA was certain that the malware tool kit being used by vorVzakone (and his affiliates) was in fact Gozi Prinimalka. The forum post only claimed that a new malware rootkit superior to SpyEye and Zeus was chosen for the operation. Specifically, vorVzakone mentioned that new tool they were to use had "richer functionality" than the two aforementioned kits and proceeded to mention the following as improvements associated with this new malware kit[64]:

- Automatic tracking of the acquired accounts balances and activity
- Back connect socks
- Ability to synchronize settings with the holder's machines, for creating a clone of his machine on your VM
- Useful admin panel for processing the accounts (all the fields necessary for transfers and calls are filled)
- Module for telephone flooding from the admin panel when using the running Skype instances Downloading of the files into admin panel for each account that is being processed (for down loading screenshots, background and credit reports)
- Highlighting in yellow the accounts that have associated socks server online
- SMS notification that the needed socks server is online
- GeoIP of SOCKS servers acquired from the loads
- Information on the blacklist status of the socks servers
- Sorting of the socks servers by uptime (for checking the accounts through socks servers withlow uptime and transferring funds using socks servers with high uptime)
- Task management admin panel (useful for managing tasks among the team)
- Ability to work with 3rd party logs using our system
- Hiding from AV products

[63] Sherstobitoff, R. (2012). Analyzing Project Blitzkrieg, Credible Threat. McAfee Labs

[64] Krebs, B. (n.d.). Transcript of hacker vorVzakon forum post for Project Blitzkrieg. Retrieved from Krebs on Security website: krebsonsecurity.com/wp content/uploads/2012/10/VorVzakonePostxlated.txt

Continued

Many of the advantages listed focus on operational organization and information awareness that would make an operation more successful. vorVzakone lists features that can be considered to be technically advanced, such as virtual machine victim cloning. One can also note the inherent operational jargon. The intended audience of the post is expected to know what the SOCKS proxy protocol is, AV sandboxes and what back connecting entails.

Whether or not the above mentioned features were found as functionality in the images obtained and analyzed by RSA and McAfee was not disclosed. The only explicit assertion that is made is again that McAfee matched victims who had Gozi Prinimalka on their system to those IP addresses found to be associated with vorVzakone.

McAfee and RSA were nevertheless determined that a specific variant of Gozi Prinimalka was utilized. Any specific variant doesn't hold any immense value but it shows the level of development and evolution of the malware over time. The Gozi Prinimalka was not created by vorVzakone or his affiliates according to McAfee, who say intelligence obtained through monitoring underground web chats points to another third party as being the creator. What's interesting is that given the level of variants and wide use of Gozi Prinimalka seen by RSA and McAfee, the malware toolkit is relatively private compared to other malware kits on the underground market. For instance, SpyEye and Zeus are both kits that are sold publicly, while Gozi Prinimalka is not[65]. It is likely that in cases where Gozi Prinimalka is used, the actors are likely linked to the same group.

Once establishing the specific variant of Gozi Prinimalka that was associated(or most suspected to be) with vorVzakone, McAfee also determined that other variants appeared to occur in 2 other distinct campaigns63. The other 2 campaigns were identified as the “Ukrainian” and “Romanian” campaigns. The Ukrainian campaign occurred from 2008 2011 and the Romanian campaign occurred from August October 2012[65]. Operation Blitzkrieg started in March 2012. It essentially appeared alongside (in time perspective) with the Romanian Campaign. It was found that the Romanian campaign was also dedicated to targeting US citizens who were customers of US banks. This profile is exactly the same as the proposed Operation Blitzkrieg. Thus the immediate question that arose was, was what McAfee termed as the Romanian campaign the actual precursor operation that vorVzakone was referring to.

A conclusive answer will likely never be known. However, researchers did discover more operational intelligence of the Romanian campaign, which at the very least make it a strong candidate to indeed be the pilot operation that vorVzakone was referring to. McAfee, after having discovered the command and control servers for the variant of Gozi Prinimalka that was associated with the Romanian campaign, tracked the servers connections to US target hosts. The control servers were found to be in communication channels with at least 60 victim hosts scattered across cities in the US[66].

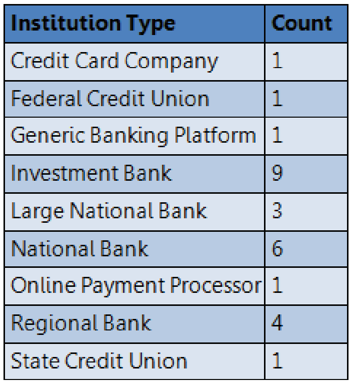
[65] Sherstobitoff, R. (2012). Analyzing Project Blitzkrieg, Credible Threat. McAfee Labs
[66] Sherstobitoff, R. (2012). Analyzing Project Blitzkrieg, Credible Threat. McAfee Labs

According to McAfee labs, this is very typical and matches that of a test run operation. Primarily because the attackers want to remain unnoticed for the future operation, as well as the fact that this initial campaign, according to vorVzakone's post, stole a few million dollars. A large sum such as this would either have to be stolen quickly via a quick execution point and retrieval or pilfered over time though unnoticed sum retrievals. The strategy in this case was the latter with initially only attacking a small amount of targets, limiting possible exposure and being patient. If at any point, the attackers strategy and malware kit were discovered and analyzed, additional defenses could destroy the campaign in its current form[67].

Given the background on the campaigns and modes of operation of the actors, McAfee and RSA were also able to reverse engineer the Gozi Prinimalka malware variant utilized in the Romanian campaign (or possible pilot phase of Operation Blitzkrieg). Essentially this revealed many technical tactics as well the bank institutions to be targeted, and further confirmation of the command and control servers the malware was beaconing out to. First, one of the primary methods the malware utilized to get target information once it was on the target machine/host was what are called "webinjects". Webinjects are content that is injected into a browser when victims connect to their banking institution's websites for the purposes of obtaining account and user information; for the given customer account and corresponding banking institution. Essentially, once a webinject is created, it set to trigger when a certain URL is seen in the browser of a victim's host. For instance, the URL "https://www.purduefed.com/" would be matched to a pre coded list of trigger URLs and then the webinject would occur on the browser.

Since the URLs act as triggers for the malware webinjects, the axiomatic assumption that can be made is that the URL identifiers also act as confirmation of the target banking institutions. In McAfee's report, they provide a set of target URLs (or rather what type of institution the URL is for) extracted from a Gozi Prinimalka malware variant image that was recovered from a victim's host. The URLs were either extracted from the specific malware variant of Gozi Prinimalka that was a part of the pilot campaign/ Romanian campaign or the other identified Ukrainian campaign. The semantics of the report don't make it explicit as to which the set is from. The set contained those of 27 US banking institutions[67]. McAfee doesn't disclose the exact institutions but provides the general count[67]:

Table 1: McAfee Institution Type Targeting



Institution Type	Count
Credit Card Company	1
Federal Credit Union	1
Generic Banking Platform	1
Investment Bank	9
Large National Bank	3
National Bank	6
Online Payment Processor	1
Regional Bank	4
State Credit Union	1

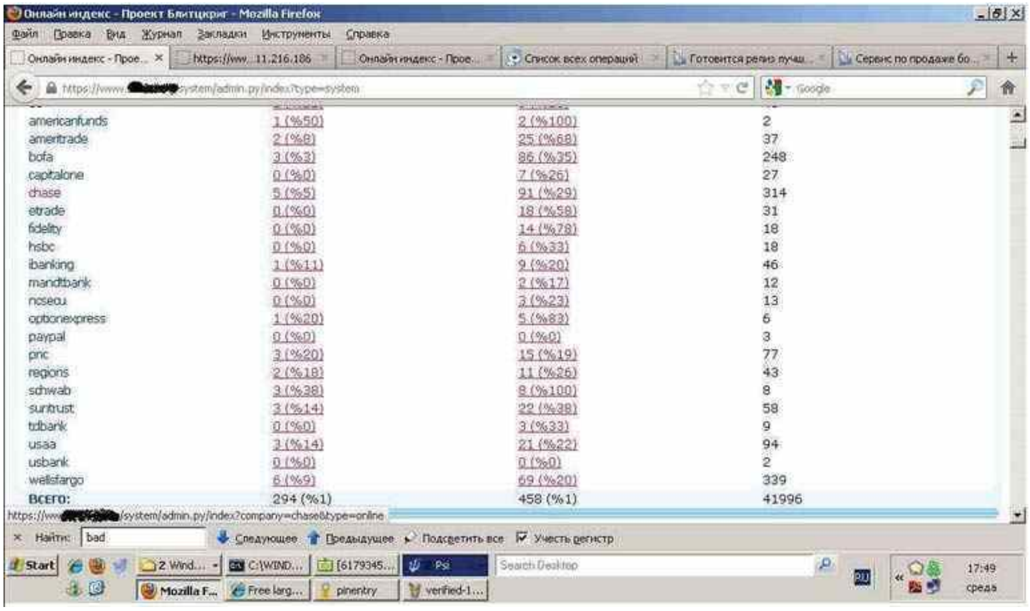
[67] Sherstobitoff, R. (2012). Analyzing Project Blitzkrieg, Credible Threat. McAfee Labs

The majority of targets are either investment banks or national banks. This is not surprising as those can be considered the most lucrative; especially investment banks as the customer's account balance tends to be greater than non investment banks.

The last technical detail is what McAfee describes as sets of mangled string found in the malware images of the Gozi Prinimalka. Researchers' best guesses are that these strings correspond to directory/registry/function names, that are either obfuscated or erroneous. They only reason why it was determined that these string were directory/registry/function names was that when running the malware in a monitored environment, the strings were used as paths to opened and accessed. The malware however did not include any functionality to alter the mangled strings into a human recognizable form[68]. So ultimately, it's unclear what the intended purpose of the suspected obfuscated strings was.

Motivation:
The motivation of Project Blitzkrieg and derivative campaigns were financial gain. Every detail about the attack, especially vorVzakone's personal post, overwhelmingly implied and confirmed the goal and motivation for the operation. In this case study one lingering question is: why did the target space consist of only US citizens and US banking institutions? vorVzakone himself answers that question; attacking targets in the US offers relative safety when operating in eastern Europe and Russia, and reduced security mechanisms[69]. Plus the fact, that the reasons vorVzakone states for targeting US entities are legitimate assertions. In other words, if vorVzakone instead was stating some other, possibly questionable assertions about why the operation is aimed at US citizens and institutions, one could then reasonably re evaluate the motivations. This is not the case here; the motivation is quite overt and evident throughout the analysis done by McAfee and RSA.

A screen shot posted by vorVzakone, showing his Project Blitzkrieg malware server listing the number of online victims by bank[69]



americanfunds	1 (%50)	2 (%100)	2
ameritrade	2 (%8)	25 (%68)	37
bofa	3 (%3)	86 (%35)	248
capitalone	0 (%0)	7 (%26)	27
chase	5 (%5)	91 (%29)	314
etrade	0 (%0)	18 (%58)	31
fidelity	0 (%0)	14 (%78)	18
hsbc	0 (%0)	6 (%33)	18
ibanking	1 (%11)	9 (%20)	46
mandtbank	0 (%0)	2 (%17)	12
ncseou	0 (%0)	3 (%23)	13
optionexpress	1 (%20)	5 (%83)	6
paypal	0 (%0)	0 (%0)	3
pnc	3 (%20)	15 (%19)	77
regions	2 (%18)	11 (%26)	43
schwab	3 (%38)	8 (%100)	8
suntrust	3 (%14)	22 (%38)	58
tdbank	0 (%0)	3 (%33)	9
usaa	3 (%14)	21 (%22)	94
usbank	0 (%0)	0 (%0)	2
wellsfargo	6 (%9)	69 (%20)	339
Всего:	294 (%1)	458 (%1)	41996

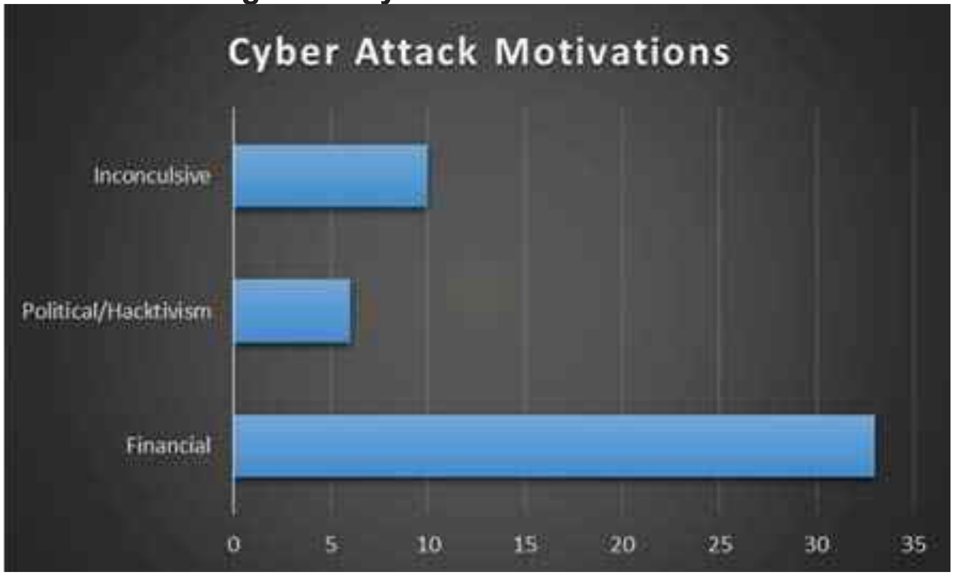
[68] Sherstobitoff, R. (2012). Analyzing Project Blitzkrieg, Credible Threat. McAfee Labs

[69] Krebs, B. (n.d.). Transcript of hacker vorVzakon forum post for Project Blitzkrieg. Retrieved from Krebs on Security website: krebsonsecurity.com/wp-content/uploads/2012/10/VorVzakonePostxlated.txt

Analysis

According to Figure 1, and unsurprisingly, financial motivations appears as the major reason explaining why people commit cyber attacks within the financial realm. Financial motivations almost doubles political/hacktivism and inconclusive motivations. The second reason why criminals commit cyber attacks is inconclusive. Only a small amount of incidents (6 out of 47) collected are motivated by political/hacktivism ranked the third and last in all three reasons that explain why people commit cyber attacks. The attack type must follow the physical and logical principles the attack must remain unknown until damages cannot be hidden. There will not any heist in cyberspace in the US economic system. Most of the common techniques people can use for financial motivated cyber attack could be theft, intrusion, fraud, and phishing. Financial motivations ranking first also shows that to gain enough money through cyber criminals is the main stream of the cyber attacks in the US economic system only very few incidents are caused by political reasons. Even though very few incidents are caused by political reasons, it does not mean we should pay no attention to this type of attack it could cause little damage but huge impact to the public.

Figure 1: Cyber Attack Motivations



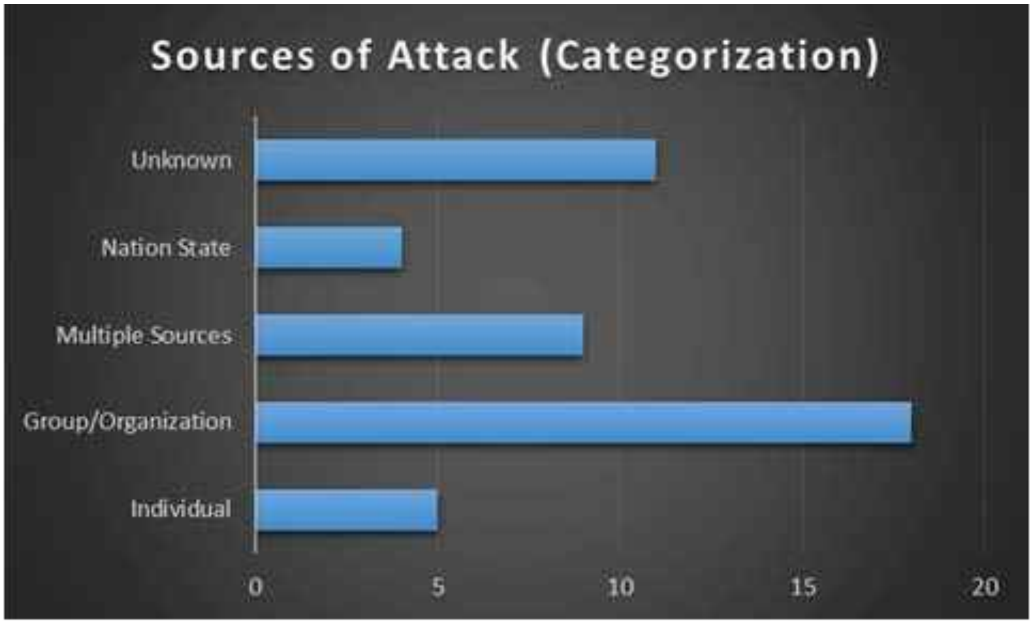
There is another thing that we should also take into consideration: almost 1/4 of the incidents are motivated by inconclusive reasons. This is partly because they are caused by unknown actors. It is difficult to track back to the criminals based on our current techniques, but this does not mean we should pay no attention to this filed: when enemies of the country are trying to attack the US, it is highly possible for them to choose unexpected target. The fact that incidents are inconclusive can reflect the bad condition of the public awareness among the cyber security issues or ability to track cyber criminals. The reasons why some of the details about the attack could not be provided are: the attacks are hidden by the attacked organizations   a release of the details can result in a immediately lost in money; police or organizations cannot track the criminals because of the anti forensics techniques in the cyberspace; and there might be no accurate reason proving the motivation.

Analysis Cont.

According to Figure 2, most of the attacks are committed by groups or organizations from the data gathered. Excluding the unknown attackers, the second ranked attackers are multiple sources. Only 5 of the attacks are committed by the individuals, and 4 of the attacks are committed by the nation state. All of the data shows that among all of the attacks focused in this research, at least a group of criminals were involved. This is because most of the attacks towards the financial industry is financially motivated and to gain enough profit the criminals have to work and cooperate in a group to ensure their success.

An example of this could be the ATM attacks: some of criminals are responsible for finding partners, some of them are responsible for hacking into the system, and some of them are responsible for sharing out the money from the ATM. Other examples are the phishing website, and identity theft. It is unlikely to have only one person finish such a phishing website or theft because of the lacking of techniques such as thousands of code lines have to be implemented before such a crime could be committed. It takes so much time and effort to do this kind of work and no benefit could be retrieved until such attack really happens. So from our data, most of the attacks towards the financial system are committed by groups or organizations and not by the individual.

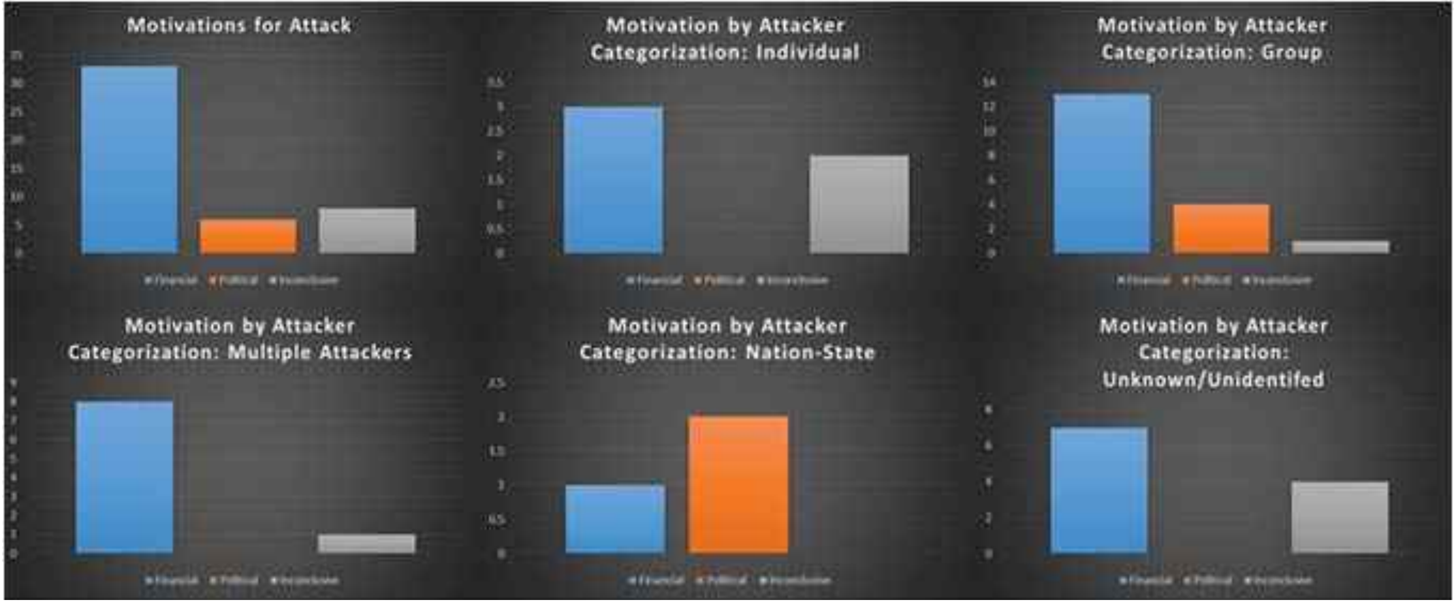
Figure 2: Sources of Attacks



After gathering data for the timeline we then analyzed the different attacks. Of the 47 attacks, 33 (70%) where financial motivated, 6 (13%) were politically motivated, and 8 (17%) of the attacks a motivation could not be attributed. These numbers were charted in the "Motivations for Attack"(top left) graph within Figure 3. The motivations for attack were broken down to the specific categorization of attackers: financial, political, and inconclusive.

Analysis Cont.

Figure 3: Motivation for Attacks



For the categorization of “Individual” (top center graph) in Figure 3, attackers of the 5 attacks attributed to that category. Of those attacks, 3 (60%) of the attacks were financially motivated, and 2 (40%) of the attacks the motivations were found to be inconclusive. For individuals it seems that a political motivation seems to be low in their priorities and personal financial gain is moderate. The total in this area was only up to 5 so with the 2 inconclusive attacks it is difficult to conclude which motivation is the popular pattern for individuals attacking the financial industry as the inconclusive results could be associated with either category making the results very different.

For the categorization of “Group” (top right graph) in Figure 3, attackers there were 18 total attacks attributed to this category. Of those attacks 13 (72.22%) of the attacks were financially motivated, 4 (22.22%) of the attacks were politically motivated and only 1 (5.56%) of the attacks had a motivation that could not be attributed. We begin to see a better idea as to what kind of motivations a group might go after at first glance but within the digital realm it is very easy to make a single person look like an entire group. The data being explored within this area was attributed to known attack groups.

For the categorization “Multiple Attackers” (bottom left graph) in Figure 3 there were 9 attacks attributed. Of the 9 attacks, 8 (88.89%) of the attacks were financially motivated, 1 (11.11%) of theattacks a motivation could not be attributed, and zero (0) political motivations were found. This category denotes the types of motivations for multiple groups attempting a cyber attack upon the financial industry.

For the category “Nation State” (bottom center) in Figure 3 there were a total of 3 attacks attributed. Of the 3, 2 (66.67%) of the attacks were politically motivated, 1 (33.33%) of the attacks were financially motivated and zero of the attacks were inconclusive. The nation state category is perhaps the most difficult of the areas to look into fully as nation states can be very careful in their attacks and rarely will announce to the world that the originating attack was for a political reason. To announce and claim responsibility for an attack against another country’s financial industry could cause political tension and lead to escalated actions.

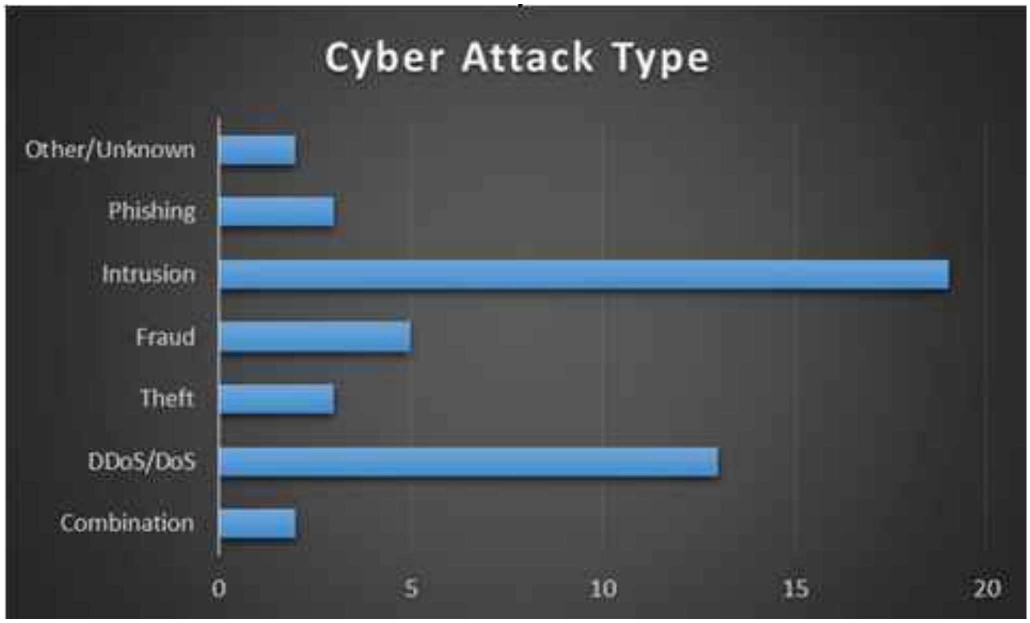
Analysis Cont.

For the category "Unknown/Unidentified" (bottom right) in Figure 3 there were 11 attacks for this category. Of the 11 attacks 7 (63.63%) attacks were financially motivated, and 4 (36.36%) attacks the motivation could not be attributed and zero (0) attacks were politically motivated. These attacks being unknown/unidentified might not show if they were executed by an individual, group, multiples, or nation state but that is not to say it holds no value. By seeing that out of 47 total attacks, 11 (23.4%) of the attacks were unable to result in a definite culprit. This is not to say that 23.4% of the time a cybercriminal will get away with a deed but it does reflect on the difficulties in which investigators deal with when attempting to track a suspect.

According to Figure 3, people commit cyber attack mostly because of financial reasons. From Figure 3 we can also find that a group of actors and nation states tend to commit cybercrime towards the financial industry for political reasons. No known individuals or multiple attackers are found to commit the attack because of political reasons. We also found that the major reason for nation state to commit the cyber attack towards the financial industry is from political aspect. Only 1 nation state attacked the cyberspace of the U.S. financial industry because of financial reasons. Another finding is that all the attacks for political reasons can be attributed. This shows that the US public system is concerned and paying attention to the political attacks from the other countries and such attacks could easily lead to public concern towards the cyberspace security. Even though Figures 3 reflects some important information, there is one limitation of this figure. Sampling data is too little. In the table nation state category, only 3 cases are collected. In the individual category, only 5 cases are collected. This cannot show clearly why nation state and the individuals commit the cyber attack.

According to Figure 4, most of the cyber attack types are: phishing, intrusion, fraud, theft, DDOS/DOS, and a combination of the above. The first and second ranked types are intrusion and DDOS. Fraud ranked third among all of the cyber attack types. Less than 5 phishing or theft cases were collected in our source.

Figure 4: Cyber Attack Type



Analysis Cont.

What we can learn from the Cyber Attack Type is that about 70% of the attacks are from network aspects: 32 out of 47 of the attacks are intrusion and DDOS attacks. Data from the 2013 Data Breach Investigations Report also supports our research[67]. According to the report, which has been published for 10 years and be one of the most respected reports in the financial system, 75% of the attack are committed by three major technologies: web application invasion, DDOS and card scanning .

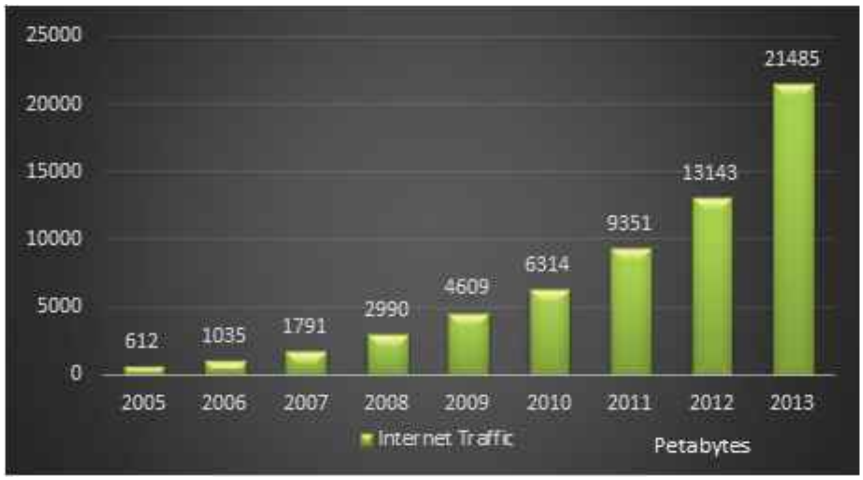
According to Figure 4, fraud, theft and phishing do not seem to be as large of a problem: only 3 phishing cases, 5 fraud cases, and 3 theft cases are reported in our research. It does however seem to be misleading. There is one thing we should take into consideration: people tend not to prosecute fraud or phishing when they are not the victims. According to one of the authors experience's, he has received three phishing emails during only one year, but has never replied to these emails and never prosecuted this to the public. This kind of attack does not cause certain damage to the public and they are not collected as cyberattacks towards the financial industry. We can infer that there are a huge number of cyber phishing and fraud cases unknown to the public. We therefore have to consider phishing and fraud as a serious problem towards the financial industry that is not getting enough recognition in major reports or daily media.

Additional Analysis:

By looking at the Verizon reports as well as ustelecom.org, and dataloss.db.org we were able to extract data that shows us overall attacks. When using this information we are also making a distinction between a "breach" and an "attack"; see the Definitions section at the beginning of the paper for distinction[70] [71].

In Figure 5 we see that internet traffic has increased drastically from 2005 to 2013 from data seen from ustelecom.org. We began to wonder if the amount of breaches throughout the years has a similar pattern so we graphed out the data side by side in Figure 6. When putting internet traffic next to the number of breaches reported throughout 2005 2013 we saw that the pattern wasn't nearly as obvious as the growth in internet traffic. There was a spike in 2008 as well as slight growth up to 2012 but then a decrease in 2013. We then looked at the breaches a litter closer[71].

Figure 5: USTelecom Reported Internet Traffic Growth

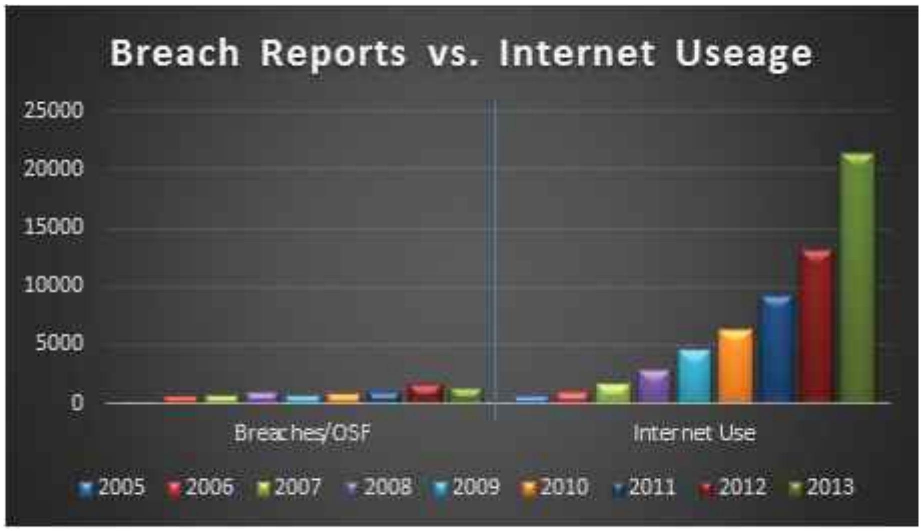


[70] Verizon RISK Team (2013). The 2013 Data Breach Investigations Report. Retrieved on April 22, 2014, from http://www.verizonenterprise.com/DBIR/2013/

[71] US Telecom Report (2013)

Analysis Cont.

Figure 6 Breaches vs. Internet Use



The Verizon Data Breach Reports data represented by Figure 7 show that the amount of breaches between 2005 2013 is increasing in reports but is slightly inconsistent between the years[69]. (Looking through the reports we could not extract the total number of breaches for 2005 2008.) Notice the drop in 2012 and then the acute jump in breach reports to 2013. Grabbing breach data from the Open Security Foundation also showed an increase but also with specific varying results in Figure 8[70]. Looking at Figure 7 and Figure 8, both graphs do show an overall increase in cyber breaches from their reports but their specific data points are varied. This could point out how the reporting process of a breach can vary between organizations and research and the willingness to share this information with other organizations, let alone the public.

Figure 7: Verizon DBIR[72]

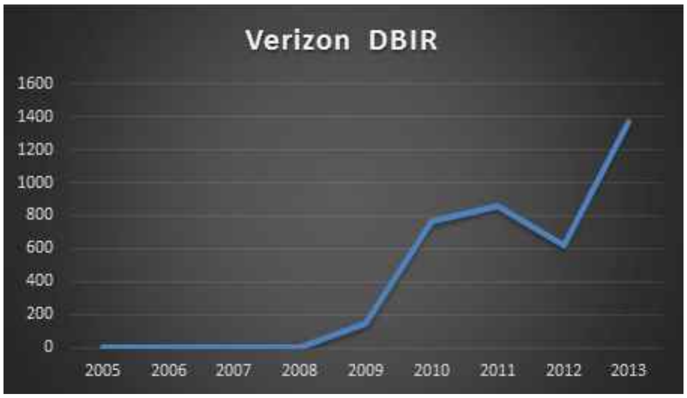
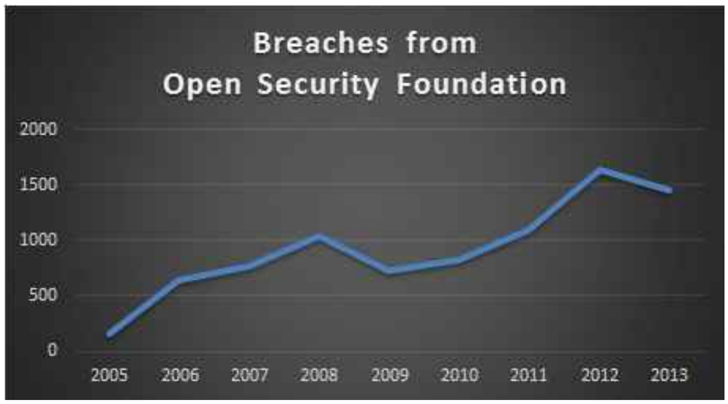


Figure 8: OSF Breaches[73]



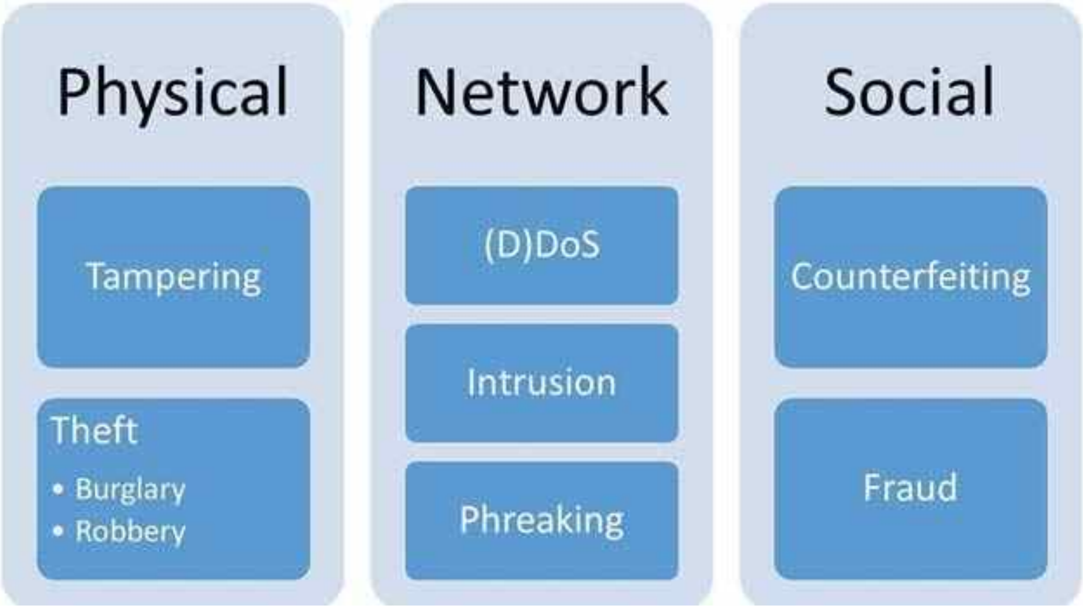
[72] Verizon RISK Team (2013). The 2013 Data Breach Investigations Report. Retrieved on April 22, 2014, from http://www.verizonenterprise.com/DBIR/2013/

[73] Open Security Foundation, 2013

Attack Taxonomy

The taxonomy of attack types used in this paper roughly correspond to the OSI network model. At the bottom layer we have the physical attacks that require access to the physical assets of a financial institution. On top of the physical layer is the network layer where attackers can remotely interact with computing resources. Finally on top of the first two layers is the social layer which utilizes human interaction. Figure 9 shows the taxonomy attack types developed for this paper.

Figure 9: Attack Types



Physical attacks against financial targets are some of the oldest forms of attacks. Before modern technology, money existed as physical currency. The large collections of currency (banks, mints, etc.) provided attackers concentrated targets from which they could steal a large amount of money in a single theft. One of the reasons behind the founding of the Federal Bureau of Investigation (FBI) was the rash of bank robberies in the 1920's that occurred during the Great Depression. Since that time societies began shifting towards cashless interactions via electronic payments. These networked systems still run upon physical machines and wires, and these physical elements continue to provide an attack surface:

Attack Taxonomy

Theft: Stealing the machines used by financial institutions is a direct way to gain access to their stored information.

Tampering: Sometimes the goal of an attacker is to leave a machine in place but alter its functionality.

Network Attacks: Are receiving large amounts of public attention due to an increase in the sophistication of attacks. The early Internet did not design and build security in because of the limited number of connections and users. It was assumed that anyone with access to the Internet was inherently trustworthy. Early network attacks of the 1960s and 1970s were largely a case of individuals with access to network terminals. Modern network attacks need to circumvent protection mechanisms established since those early halcyon days. Increased security is not deterring attackers.

Intrusions: Computer network intrusions are when an attacker is successful in penetrating the security of a target network and executing software of their own design on the target's computers

Phreaking: The term "phreaking" is a portmanteau of "phone" and "hacking". Phreaking is exploiting a telephone system. In the heyday of Captain Crunch and the blue box it was possible to attack phone systems by transmitting signaling information through the voice channel. Newer systems that segregate signal and voice data such as Signaling System Number 7 (SS7) make phreaking attacks more difficult to execute on modern telephony systems.

Remote exploitation: When a software flaw is deployed into a production environment it becomes a vulnerability. Sophisticated attackers are willing to spend the time to identity these vulnerabilities and developing the exploits needed to leverage the vulnerabilities into arbitrary software execution.

(Spear) phishing: Exploiting the human user of a computer is the goal of a phishing attack. The more focused spear phishing differs only in the higher level of customization against a specific target that is involved. In both cases the attacker tries to trick a user into starting execution of the malicious software. Variants on this technique include whaling (attacking high value targets) and water holing.

Availability: Some attackers are content with denying access to legitimate users. These attacks are less technically sophisticated because they use quantity of traffic to overload bandwidth of the servers and network connections (cite Anonymous' use of the Low Orbit Ion Cannon software).

Counterfeiting: Creating false currency for circulation exploits the web of trust built around the targeted currency. This is done for financial gain as a crime, and/or to undermine the confidence in a currency as an attack (cite DPRK superbills paper). Fraud Fraud attacks rely on confidence for their success. Nigerian scammers are the archetypical example of email aided fraudsters. Other attackers leverage stolen user credentials for fraudulent transactions.

Money laundering: The goal of laundering money is to obscure its origins. Enterprises like selling drugs generate a large amount of physical currency but this can be traced back to its source. Illicit gains are in turn funneled into a common fund or source and then extracted again later as profits or sales of the resource.

S.W.O.T. Analysis Case Study: Heartland Payment Systems Modified to Cyber Security Capabilities

This is a Strengths, Weaknesses, Opportunities and Threats (S.W.O.T.) analysis of the Heartland Payment Systems (HPS) cyber security and capabilities. This financial entity was chosen for many reasons: HPS represents a key entity type with the financial industry as a payment processing company, HPS experienced one of the largest data breaches ever publicized, and lastly as a result of the attack HPS has improved their cyber security substantially.

A little background on Heartland Payment Systems (HPS): HPS is a consumer payment processing firm at its core; its primary business objective is to provide services to merchants and companies that must take electronic payment systems from their own customers[74] . In other words they are a third party middleman that process payments for merchants by taking care of the burdensome process of managing the required process with the customer's bank and the merchants bank. HPS began in 1997 and has quickly grown to handling more than 11 million transactions per day, $120 billion in transaction value per year and have over 250,000 client/merchant locations[75].

In 2008 and 2009, HPS corporate network was penetrated due to a software vulnerability. The vulnerability was an SQL injection attack that was known (publicly) for several years but nevertheless remained undetected for years by HPS and their security mechanisms[74]. HPS reported that during this time they had conducted internal and external security audits[74]. After getting into the network, the attackers then spent 6 months attempting to break into the processing network of HPS; their ultimate target. The attackers succeeded and now had a presence on HPS's payment processing network. Their strategy was not to capture all the payment data being sent over the network with network capture tools[74]; this is alternative to trying to get the payment data from fixed location such as a database. It was not stated exactly how many accounts were compromised the media reported 130 million total accounts compromised among HPS and other companies who experienced similar breaches at the time[76].

Format for the SWOT components as they are applied to cyber security:

- **Strengths:** components or factors of HPS cyber security mechanisms, technologies and strategies that give it an advantage in cyber security capabilities.
- **Weaknesses:** components or factors of HPS cyber security mechanisms, technologies and strategies that give it a disadvantage in cyber security capabilities.
- **Opportunities:** elements of cyber security mechanisms, technology, strategy and characteristics that HPS could exploit to its benefit.
- **Threats:** elements of cyber security mechanisms, technology, strategy and characteristics that could cause damage, harm, or less benefit to HPS.

[74] Cheney, J. (2010). Heartland Payment Systems: Lessons Learned from a Data Breach. Payment Cards Center.

[75] Brian Krebs (January 20, 2009). "Payment Processor Breach May Be Largest Ever". Washington Post.

[76] BDO (2013, April). The Heartland Payment Systems Data Breach – what lessons can retailers learn? George Quigley BDO UK BDO. Retrieved from http://www.bdo.co.uk/talk shop/the heartland payment systems data breach what lessons can retailers learn george quigley

S.W.O.T Cont.

Table 2: S.W.O.T. Table

	Strengths	Weaknesses
Internal	(1) Awareness, Priority (2)End to End encryption is standard(Identity Based Encryption (3) Expected security level (4) Experience	(7)Resources for implementing cyber security (8)Resources for dealing with aftermath of attack
	Opportunities	**Threats**
External	(5)Create and follow better standards (6)Update and upgrade security audits	(9)Lucrative Target (10)Insider attack

Strengths

(1) Awareness/Priority : due to the 2008 breach , HPS now treats cyber security as a priority if it wasn't already one. This includes having company employees who are experts in the field, staying current in the field, sharing information with other entities, and update security audits. (this is a common theme after a company has a major attack)

(2) End to End Encryption: all data in transit over HPS networks is encrypted now, after the attack, as well as when data is at rest(on a database). HPS also uses a newer encryption method called Identity Based Encryption for some of its customer communications. Identity Based encryption removes the need for a public key infrastructure and operational costs of doing so. HPS uses Identity Based Encryption technologies from a company called Voltage.

(3) Expected Security Level: This may seem like a threat to HPS but these authors would argue its actually a strength. Given HPS is in the financial industry, they are a lucrative target regardless of how strong their cyber security defense is. However, due to public/societal/industry expectations, financial entities are expected to especially maintain and continually develop a high level of cyber security. In other words, HPS is forced to maintain a high level security standard or at least attempt to. The consequence, regardless of the reason, is a better cyber security defense.

(4) Experience: HPS has experienced a major data breach that led to a reaction and response plan that included containing the breach, patching the network, upgrading technologies, notifying customers, working with customers and dealing with the public. The experience and direct involvement with that process is arguably invaluable. HPS has learned numerous lessons that will guide their future cyber security and response strategies and mechanisms. Also, HPS will always be reminded of how serious the threat is to their cyber and ICT components that maintain their data; this will keep cyber security a top priority.

S.W.O.T Cont.

Opportunities:

(5)Create and follow better standards: There is always room for improvement of security standards when it comes to cyber and ICT components. HPS will need to continually improve their security standards (as they appear to be doing). Of course, this task will be balanced out with the perceived benefit/cost of such standards. However, again given HPS's nature in that it is in the financial realm and experienced a major data breach, one can arguably assume HPS will be more diligent in regards to maintaining appropriate standards than many other entities.

(6) Update and upgrade security audits: this is really an extension of the previous opportunity but is worth noting explicitly.

Weaknesses:

(7)Resources for implementing cyber security: HPS doesn't have unlimited resources to implement cyber security mechanisms, measures, standards, audits, tests, and technologies. This is true for any organization. At some point, there is a bound for cyber security resources. Most likely, HPS will not even reach this bound; they will devote as much resources to cyber security as long as it makes sense in a cost/benefit analysis. In addition, information and cyber security is not an absolute quality, HPS (as well as everyone else) is just raising the costs of possible adversaries.

(8) Resources for dealing with aftermath of attack: After HPS breach in 2008, they faced $12.6 million in expenses including fees and litigations with MasterCard and Visa[77]. HPS also faces class action lawsuits. Aftermath costs also entail new cyber security technologies, upgrading systems, customer fallout, reissuing customer side mechanisms etc... In a future, very damaging breach, HPS may go belly up with the financial consequences required, as they are not a mega corporation with substantial financial resources.

Threats:

(9)Lucrative Target: HPS as a business, processes financial transactions that includes financial information that can be exploited for significant financial gain. In other words, HPS will always be axiomatically an intriguing target to possible adversaries and criminals.

(10)Insider Attacks: Insider attacks are an ever present threat to entities, regardless of their domain or the technologies used. But for HPS and their business domain , the motivation for insiders is arguably higher. Also, from an historical view, one can assert that there is still no solution to insider threats. The same plays for cyber security components, where they are left mute if an authorized individual is malicious. It was stated that investigators considered the possibility of an insider in the 2008 breach[78].

[77] King, R. (2009, July 6). Lessons from the Data Breach at Heartland Businessweek. Retrieved from http://www.businessweek.com/stories/2009 07 06/lessons from the data breach at heartlandbusinessweek business news stock market and financial advice

[78] Claburn, T. (2009, January 20). Heartland Payment Systems Hit By Data Security Breach. Retrieved from http://www.darkreading.com/attacks and breaches/heartland payment systems hit by data security breach/d/d id/1075770?page_number=2

Conclusion

The U.S. financial infrastructure is evolving along with the cyber capabilities it utilizes. Analyzing the statistics of cyber attacks on the United States financial industry and their origins gives insight into patterns of attack, sources and motivation of various nationally significant attacks, and the possibility of continued, increasing cyber threat against the nation's financial sector of its critical infrastructure. Analyzing individual cases of financial cyber crime has allowed for greater understanding of the history and continuing threat the US financial system faces from individuals, hackitivists, groups and nation states. While the motivation for the attacks may vary, the trend of cyber crime is exponentially rising due to increased internet access and usage by individuals, businesses, and government agencies alike.

The financial industry is a direct target for individuals seeking to profit due to the potential for large financial gains. Cyber is a dynamic environment that can easily facilitate these types of financial crimes remotely, quickly, and without leaving obvious signs or evidence of a breach. A significant cyber attack led by a nation state or its actors versus another nation state could be considered an act of war, as defined in this paper. Protecting the framework of the US financial system is essential to the health and survival of the national and global economies. Identifying patterns of compromise and potential attackers is a crucial step in determining if the financial industry is indeed under attack and if so, who the perpetrators may be.

The U.S. financial infrastructure is evolving along with the cyber capabilities it utilizes and travels through. Protecting this framework is essential to the health and survival of the national and global economies. Identifying patterns of compromise and potential attackers is a crucial step in determining if the financial industry is indeed under attack and if so, who the perpetrators may be. The previous work analyzes past cyber attacks to determine if the U.S. financial industry is under attack by individuals, group and nation states. This paper defined key terms and presented a theory and paradigm of cyber attacks. This paper examined case studies, both in summary and in depth, to examine the aggressors and any origination or motivation. Additionally, this paper proposes a taxonomy created by the researchers concerning types of cyber attacks seen in the financial sector. This paper also demonstrated a SWOT analysis on a case study.

This paper provided an overview and timeline of nationally and internationally significant cyber attacks that affected the US financial system. An analysis of attack types and case studies on unique types of breaches were presented. This paper found that there is indeed an upward trend in financial cyber crime; as the number of internet users has grown exponentially over the last decade, the number of reported cyber attacks has increased as well. As more individuals, businesses, institutions, and government agencies continue to use cyber for more and more, the trend of cyber crime will also continue to increase.

Conclusion Cont.

The analysis shows primary motivations for financial cyber attacks as well as possible reasons for undetermined attack origins. The analysis then presents various entities involved in financial attacks as well as various types of methods and attacks utilized. The analysis in this paper was found to correspond with other published reports of frequent attack types and methods. The taxonomy was created to demonstrate and categorize various types of attacks. It classified multiple methods according to attack types and numerous examples and histories of each type. This paper found that intrusion and DDoS/Dos types of attack were the most common cyber attacks seen in the financial industry. Finally, a SWOT analysis was performed on a specific case study involving Heartland Payment Systems, to determine and categorize strengths, weaknesses, opportunities, and threats, both internal and external.

Studying the history of cyber attacks on the U.S. financial system allowed for a greater understanding of the origins, motives, and patterns of significant breaches. This information should be used to strengthen cyber security and help financial institutions and government personnel understand the risks associated with cyber and the U.S. banking system. While cyber crime will continue to be a threat, research, awareness, and understanding of the problem will potentially prevent an attack significant enough to permanently damage or destroy the U.S financial infrastructure.

PURDUE
UNIVERSITY

CYBERFORENSICS LABORATORY

Bibliography

Acohido, B. (2009). Hackers breach Heartland Payment credit card system. Retrieved *October,18*(2011), 2009-0.

Albanesius, C. (2013). Feds Charge Three Over 'Gozi' Banking Virus. Retrieved March 15th, 2014, from http://www.pcmag.com/article2/0,2817,2414604,00.asp

Akamai (2012, October). *Increasing Size of Individual DDoS Attacks Define 3rd Qrt, According to Prolexic*. Retrieved March 2014, from www.prolexic.com/news-events-pr-increasing-size-of-individual-ddos-attacks-20-gbps-is-the-new-norm-2012-q3.html

Arbor Networks (2013). *2.64 Gbps: Average Size of DDOS Attacks Launched in 2013*. Retrieved 2014, from http://news.softpedia.com/news/2-64-Gbps-Average-Size-of-DDOS-Attacks-Launched-in-2013-391974.shtml

Ashford, W. (September 27th, 2013). Top 10 cyber crime stories of 2013. Retrieved from http://www.computerweekly.com/news/2240210681/Top-10-cyber-crime-stories-of-2013

Associated Press. (2009). W. Pa. school district among targets of cyber-attacks, many originating in Europe. Retrieved March 15th, 2014, from http://triblive.com/x/pittsburghtrib/business/s_640015.html#axzz2w5W6xpzA

BBC News (2011, March). *BBC News - South Korea hit by cyber attacks*. Retrieved March 2014, from http://www.bbc.co.uk/news/technology-12646052

BBC News (2013, March).*BBC News - China IP address link to South Korea cyber-attack*. Retrieved from http://www.bbc.com/news/world-asia-21873017

BBC News (2011, March). *BBC News - South Korea hit by cyber attacks*. Retrieved March 2014, from http://www.bbc.co.uk/news/technology-12646052

Booton, J. (2011). Hackers Gain Data Access to 200,000 Citi Bank Cards.

Booton, J. (2013). 'White Hat' Hackers Expose Flaws of U.S. Stock Market. Retrieved March 15th, 2014, from http://www.foxbusiness.com/technology/2013/10/22/white-hat-hackers-expose-cyber-flaws-us-stock-market/

Botnet Operation Disabled FBI Seizes Servers to Stop Cyber Fraud. (April, 2011). Retrieved from http://www.fbi.gov/news/stories/2011/april/botnet_041411

Bull, A. & Finkle, J. (2013, February 5). Fed says internal site breached by hackers, no critical functions affected. Retrieved from http://articles.chicagotribune.com/2013-02-05/business/chi-federal-reserve-hacked-20130205_1_hackers-personal-information-central-bank

Burton, M. (2010). Government Spying for Commerical Gain. *Studies in Intelligence, 37*(2), 17-23. Retrieved March 19, 2014, from https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol37no2/pdf/v37i2a02p.pdf

Carter, S. (March, 2014). How sanctions against Russia could signal the beginning of 'World War III'. Retrieved from http://www.theblaze.com/stories/2014/03/18/how-sanctions
-against-russia-could-signal-the-beginning-of-world-war-iii/

Clearfield, C. (2013, November 15). *Finance Industry Grapples with Cyber Threats*. Retrieved March 17, 2014, from Forbes: http://www.forbes.com/sites/chrisclearfield/2013/11/15/finance-industry-grapples-with-cyber-threats/

Cluley, G. (2013). Hackers hit the NASDAQ community forum, email addresses and passwords compromised. Retrieved March 16th, 2014, from http://grahamcluley.com/2013/07/nasdaq-hackers/

Cutler, K. (2014, March). *Mt.Gox Posts New Statement On Alleged Bitcoin Theft, Bankruptcy Filing | TechCrunch*. Retrieved March 2014, from http://techcrunch.com/2014/03/03/mt-gox-posts-new-statement-on-alleged-theft-bankruptcy-filing/

Cyber Conflict Studies Association. (2012). Addressing cyber instability. *Executive Summary.*

Cyber crime. (n.d.) Retrieved from http://www.fbi.gov/about-us/investigate/cyber

Davidson, P., (2013). Banks, regulators moving to thwart cyberattacks. *USA Today.* Retrieved from: http://www.usatoday.com/story/money/business/2013/12/09/financial-institutions-cybersecurity/3929969/.

'Dark Market' Takedown exclusive cyber club for Crooks Exposed. (October, 2008). Retrieved from http://www.fbi.gov/news/stories/2008/october/darkmarket_102008

Delevingne, L. (December, 2009). The decade's 10 biggest financial crimes. Retrieved from http://www.businessinsider.com/the-decades-10-biggest-financial-crimes-2009-12?op=1

DeLuca, C.D. (2013). The need for international laws of war to include cyber attacks involving state and non-state actors. *Pace International Review Online Companion 278*. Retrieved from http://digitalcommons.pace.edu/cgi/viewcontent.cgi?

Denning, D. E. (1999). Information Warfare and Security (1st ed.). New York: ACM Press.

Dictionary. (2014). *Cyber*. Retrieved March 17, 2014, from Dictonary: http://dictionary.reference.com/browse/cyber

Dixon, H. (2013, September). *Barclays hacking attack gang stole £1.3 million, police say - Telegraph*. Retrieved March 2014, from http://www.telegraph.co.uk/news/uknews/crime/10322536/Barclays-hacking-attack-gang-stole-1.3-million-police-say.html

DTCC. (2013). *Beyond the Horizon: A White Paper to the Industry on Systemic Risk.* DTCC.

Dunn, J. (2013, July). *DDoS attack sizes rise above 2Gbps for first time - Techworld.com*. Retrieved March 2014, from http://news.techworld.com/security/3461365/ddos-attack-sizes-rise-above-2gbps-for-first-time/

Egan, M. (2013, May).*Financial Exchange Blitzed by Massive Memorial Day Cyber Attack | Fox Business*. Retrieved March 2014, from http://www.foxbusiness.com/technology/2013/05/30/financial-exchange-blitzed-by-massive-memorial-day-cyber-attack/

FBI Cyber Most Wanted. (2013, 11/05/2013). FBI Cyber Most Wanted List. Retrieved March 16th, 2014, from http://www.fbi.gov/news/stories/2013/november/new-subjects-added-to-cybers-most-wanted-list/new-subjects-added-to-cybers-most-wanted-list

FBI Testimony (2011) Testimony on The Cyber Threat to the Financial Sector United State House of Representatives.

Federal Bureau of Investigation (FBI). (n.d.) *Computer Intrusions*. Retrieved from: http://www.fbi.gov/about-us/investigate/cyber/computer-intrusions

Federal Bureau of Investigation. (2014, March 17). Bank Crime Statistics (BCS). Retrieved March 17,2014,from FBI.gov: http://www.fbi.gov/stats-services/publications/bankcrime-statistics2011/bankcrime-statistics-2011

Federal Reserve Board, (2013, March). Consumers and Mobile Financial Services 2013. Retrieved from *www.federalreserve.gov/.../consumers-and-mobile*

Finkle,J. (2012, September).*Exclusive: Iranian hackers target Bank of America, JP Morgan, Citi*| *Reuters*. Retrieved March 2014, from http://www.reuters.com/article/2012/09/21/us-iran-cyberattacks-idUSBRE88K12H20120921

Freeman, K. D. (2014). World War III: The Coming Cyber-Financial Attack that will Shock America. Retrieved from http://www.theblaze.com/contributions/world-war-iii-the
-coming-cyber-financial-attack-that-will-shock-america/

Geers, K., Kindlund, D., Moran, N., Rachwald, R. (2013). *World war c: Understanding nation-state motives behind today's advanced cyber attacks.* Retrieved from http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf

Gertz, B., (2012). Iran Stikes Back: Iranians used University of Michigan Network to Launch Cyber Attack on U.S. Financial System. Retrieved March 20, 2014, from http://freebeacon.com/iran-strikes-back/

Google. (2014). *Define*. Retrieved March 18, 2014, from Google: www.google.com

Goldman,D. (2012, September).*Major banks hit with biggest cyberattacks in history - Sep. 27, 2012*. Retrieved2014, from http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/

Government Accountability Office. (2011). *GAO-11-695R Defense Cyber Efforts.* Retrieved from http://www.gao.gov/assets/100/97674.pdf

Greenberg, A. (2014, February 25). *Bitcoin's Price Plummets as Mt. Gox Goes Dark with Massive Hack Rumored*. Retrieved March 21, 2014, from Forbes: http://www.forbes.com/sites/andygreenberg/2014/02/25/bitcoins-price-plummets-as-mt-gox-goes-dark-with-massive-hack-rumored/

Gurusamy, S. (2008). Financial Services and Systems 2nd edition, p. 3. Tata McGraw-Hill Education. ISBN 0-07-015335-3

HacknMod. (2013). *Top 10 Internet Hacks of all Time*. Retrieved March 21, 2014, from Hack n Mod: http://hacknmod.com/hack/top-10-internet-hacks-of-all-time/

Hale, J., (2013). Bank on it: attacks on financial institutions. *SC Magazine.* Retrieved from: http://www.scmagazine.com/bank-on-it-attacks-on-financial-institutions/article/316380/3/.

Hannas, W. C., Mulvenon, J., & Puglisi, A. B. (2013). *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation.* Routledge.

Harnden, T. (2011, June 12). *IMF hit by major cyber attack*. Retrieved March 19, 2014, from The Telegraph: http://www.telegraph.co.uk/finance/financialcrisis/8571306/IMF-hit-by-major-cyber-attack.html

Hathaway, O., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel J. (2012) *The Law of Cyber-Attack*. California Law Review, vol. 100, pp. 817-886. Retrieved from http://www.californialawreview.org/assets/pdfs/100-4/02-Hathaway.pdf

Higgins, K. (2013, July). *Feds Indict 5 in massive Credit Card Data Breach Scheme*. Retrieved March 2014, from ttp://www.darkreading.com/attacks-breaches/feds-indict-five-in-massive-credit-card/240158980

High-Tech Heist 2,100 ATMs Worldwide Hit at Once. (November, 2009). Retrieved from http://www.fbi.gov/news/stories/2009/november/atm_111609

Hua, J., & Bapna, S. (2013). *The economic impact of cyber terrorism.* Retrieved from www.sciencedirect.com

(ISC)^2 Congress 2013: Financial Market Manipulation Poised as Next Wave in Cybercrime. (2013). Retrieved from http://www.infosecurity-magazine.com/view/34766/isc -congress-2013-financial-market-manipulation-poised-as-next-wave-in-cybercrime/

International Monetary Fund. (2012). *Annual Report of the Executive Board: Appendix II: Financial operations and transactions.* Retrieved March 19, 2014, from http://www.imf.org/external/pubs/ft/ar/2012/eng/pdf/a2.pdf

International Telecommunication Union. (2009). *Understanding Cybercrime: A Guide for Developing Countries.*

Internet Crime Complaint Center. (2011). 2011 Internet Crime Report.

Internet Crime Complaint Center. (2012). 2012 Internet Crime Report.

Jeffries,A. (2013). *Cyber caper: behind the scenes of the $45 million global ATM heist | The Verge*. Retrieved from The Verge website: http://www.theverge.com/2013/5/13/4326336/cyber-caper-behind-the-scenes-of-the-45-million-atm-heist

Kallberg, J. & Thuraisgham, B. (2013, May/June). State actors' offensive cyber operations: The disruptive power of a systematic cyberattack. *ITPro*.

Kaspersky. (2014) *Spear Phishing*. Retrieved from: http://usa.kaspersky.com/internet-security-center/definitions/spear-phishing#.U1lHBlf0kWZ

Kelson, R., Paganin, P., Martin, F., Pace, D., & Gittins, B. (2012). Who is attacking the financial world, and why? Retrieved fromhttp://securityaffairs.co/wordpress/9346/cybercrime/who is-attacking-the-financial-world-and-why.html

Kitten, T., (2014). Banking cyber-attack trends to watch. *Bank Info Security.* Retrieved from: http://www.bankinfosecurity.com/banking-cyber-attack-trends-to-watch-a-6482/op-1.

Kitten,T. (2012, December).*DDoS Attacks: PNC Struck Again - BankInfoSecurity*. Retrieved March 2014, from http://www.bankinfosecurity.com/ddos-attacks-pnc-struck-again-a-5356/op-1

KnowBe4. (2011). Cybercrime Extracts $399,000 from Florida Dentist’s Account; Internet Security Awareness Could Have Thwarted Attack Retrieved March 16th, 2014, from http://www.prweb.com/releases/2011/4/prweb8338409.htm

Kovacs, E. (2013). Thousands of Sites Hacked for OpUSA, but Not All Hacktivists Support the Campaign. Retrieved March 16th, 2014, from http://news.softpedia.com/news/Thousands-of-Sites-Hacked-for-OpUSA-but-Not-All-Hacktivists-Support-the-Campaign-351197.shtml

Krebs, B. (2012). New Findings Lend Credence to Project Blitzkrieg. Retrieved March 15th, 2014, from http://krebsonsecurity.com/2012/12/new-findings-lend-credence-to-project-blitzkrieg/

Kshteri, N. (2010). Diffusion and effects of cyber-crime in developing economies. *Third World Quarterly, 31*(7) 1057-1079.

Kumar, M. (2012, December 23). *Stabuniq Trojan Rapidly Stealing Data from US Banks*. Retrieved March 19, 2014, from The Hacker News: http://thehackernews.com/2012/12/stabuniq-trojan-rapidly-stealing-data.html

Lee, T. B. (February 28, 2014). Bitcoin Exchanges hit by hackers. Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/28/hackers-allegedly-stole-400-million-in-bitcoins-heres-how-to-catch-them/

Legal Information Insitute. (n.d.). Wex Legal Dictionary: Fraud. Retrieved from: http://www.law.cornell.edu/wex/fraud

Lewis, J. A. (2006). Cybersecurity and critical infrastructure protection. *Center for Strategic and International Studies*.

Lewis, J. A. (2009). The" Korean" Cyber Attacks and Their Implications for Cyber Conflict.

Liles, S., (2012). The cyber force matrix. Retrieved from: http://selil.com/archives/3148.

Liles, S., (2013). Research note: defining attacker knowledge, skill, and ability. Retrieved from: http://selil.com/archives/4912.

Malkin, L. (2006). *Krueger's Men: The Secret Nazi Counterfeit Plot and the Prisoners of Block 19.*

Mandiant. (2013). *APT1: Exposing One of China's Cyber Espionage Units.* Retrieved March 12, 2014, from http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Markoff, J. (2008, August 13). Before the Gunfire, Cyberattacks. *The New York Times*, p. A1. Retrieved March 20, 2014, from http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0

Markoff, J. & Shanker, T. (2009, August 1). Halted ’03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk. Newyorktimes.com Retrieved from: http://www.nytimes.com/2009

McAfee. (July, 2013). The economic impact of cybercrime and cyber espionage. *Center for Strategic and International Studies.* Retrieved from http://www.mcafee.com/us /resources/reports/rp-economic-impact-cybercrime.pdf

McAfee & Guardian Analytics (2013).*Dissecting Operation High Roller*. McAfee.

McCormick, T. (2013, April 29). *Hacktivism: A Short History*. Foreign Policy. Retrieved from: http://www.foreignpolicy.com/articles/2013/04/29/hacktivism

McMillan, R. (2009). ACH Fraud: Cyber Attackers Empty Business Accounts in Minutes. Retrieved March 16th, 2014, from http://www.csoonline.com/article/499189/ach-fraud-cyber-attackers-empty-business-accounts-in-minutes

Meen, J. (2013). FBI warns Syrian group may increase cyber-attacks. Retrieved March 15th, 2014, from http://www.nbcnews.com/technology/fbi-warns-syrian-group-may-increase-cyberattacks-8C11095844

Menn, J., (2013). Cyber-attack against banks more severe than most realize. Retrieved from: http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518

Merriam-Webster. (2014). *Cyber*. Retrieved March 17, 2014, from Merriam-Webster: http://www.merriam-webster.com/dictionary/cyber

Merriam-Webster. (ND). Tactics Definition. Retrieved March 19th, 2014, from http://www.merriam-webster.com/dictionary/tactics

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39-53.

Moscaritolo, A. (2011, June 9). *Citibank Cyberattack affects 210,000 Customers*. Retrieved March 21, 2014, from SC Magazine: http://www.scmagazine.com/citibank-cyberattack-affects-210000-customers/article/204857/

Moteff, J., & Parfomak, P. (2004, October). Critical infrastructure and key assets: definition a identification. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE.

Nanto, D. K. (2009). *North Korean Counterfeiting of U.S. Currency.* Congressional Research Service. Retrieved from http://www.fas.org/sgp/crs/row/RL33324.pdf

National Fraud Center, Inc., & The Economic Crime Investigation Institute (December, 2000). The growing global threat of economic and cyber crime. Retrieved from http://www.utica.edu/academic/institutes/ecii/publications/media/global_threat_crime.pdf

NATO Review, Cyber Timeline. Retrieved from: http://www.nato.int/docu/review/2013 /Cyber/timeline/EN/index.htm.

NIJ. (2008). NIJ Special Report Electronic Crime Scene Investigation: A Guide for First Responders (2nd ed.). Washington D.C.: U.S. Department of Justice.

Nishad, S. (2014, January 20). *Vladimir Levin - First ever hacker to pull internet bank robbery*. Retrieved March 21, 2014, from Surfthelist.com: http://surfthelist.com/vladimir-levin-first-ever-hacker-to-pull-internet-bank-robbery/

OICU-IOSCO. (2013). *Cyber-Crime, Securities Markets and Systemic Risk.* IOSCO.

OMB Memorandum M-07-16 dated May 22, 2007, Subject: A Safeguarding Against and Responding to the Breach of Personally Identifiable Information

Operation Ghost Click International Cyber Ring That Infected Millions of Computers Dismantled. (November, 2011). Retrieved from http://www.fbi.gov/news/stories /2011/november/malware_110911/malware_110911

Operation Phish Phry Major Cyber Fraud Takedown. (October, 2009). Retrieved from http://www.fbi.gov/news/stories/2009/october/phishphry_100709

Ott, T.P. (2010). US law enforcement strategies to combat organized crime threats to financial institutions. Retrieved from www.emeraldinsight.com/1359-0790.htm

Oxford Dictionary. (2014, March 19). Cyberwar. Retrieved from www. Oxforddictionaries.com/us/definition/American_english/cyberwar

Passeri, P. (2012). 2012 Cyber Attacks Statistics. Retrieved March 19th, 2014, from http://hackmageddon.com/2012-cyber-attacks-statistics-master-index/

Passeri, P. (2014). 2013 Cyber Attack Statistics. Retrieved March 19th, 2014, from http://hackmageddon.com/category/security/cyber-attacks-statistics/

Peltier, TR. (2001). *Information Security Risk Analysis*. Auerbach.

Perlroth, N. (2012). Attacks on 6 Banks Frustrate Customers. Retrieved March 15th, 2014, from http://www.nytimes.com/2012/10/01/business/cyberattacks-on-6-american-banks-frustrate-customers.html?_r=0

Pras, A., Sperotto, A., Moura, G., Drago, I., Barbosa, R., Sadre, R., ... & Hofstede, R. (2010). Attacks by “Anonymous” WikiLeaks proponents not anonymous.

Puaar, A. (2013, August 8). *Cyber Attacks: drilling down into the financial system's newest threat*. Retrieved March 17, 2014, from Financial News: http://www.efinancialnews.com/story/2013-08-08/cyber-attacks-dtcc-nature-of-the-threat

QASSAMCYBERFIGHTERS. (October, 2012). The 6th Week, Operation Ababil. Retrieved from http://pastebin.com/QWXkfPhG

QASSAMCYBERFIGHTERS. (September, 2012). Bank of America and New York Stock Exchange under attack. Retrieved from http://pastebin.com/mCHia4W5

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2005). *Insider threat study: Illicit cyber activity in the banking and finance sector* (No. CMU/SEI-2004-TR 021). CARNEGIE MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Rantala, R. R. (2008). Cybercrime against Businesses, 2005. (NCJ221943).

Rexrode, C. & Gordon, M. (2013). Quantum Dawn 2: US banks on cyber-attack defense. NBCNews. Retried from v http://www.nbcnews.com/business/business-news/quantum-dawn 2-us-banks-cyber-attack-defense-f6C10648551

Rial, N. (2013). Anonymous announce plans to attack US banks, institutions. Retrieved March 16, 2014, from http://www.neurope.eu/article/anonymous-announce-plans-attack-us-banks-institutions

Riley, C. (February, 2013). Hackers access Federal Reserve website, data. Retrieved from http://money.cnn.com/2013/02/06/technology/federal-reserve-hack/index.html

Rouse, M. (2005, April). *Cyber*. Retrieved March 17, 2014, from SearchSOA: http://searchsoa.techtarget.com/definition/cyber

Rouse, M. (2006). Social Engineering. Retrieved December 10, 2013, from Search Security: http://searchsecurity.techtarget.com/definition/social-engineering

Sahadi, J. (2005, July 27). *40M Credit Cards Hacked*. Retrieved March 21, 2014, from CNN Money: http://money.cnn.com/2005/06/17/news/master_card/

Sanders, C. (2010, March 17). Understanding Man-in-the-Middle Attacks: ARP Cache Poisoning (Part 1). Retrieved December 4, 2013, from Windows Security:http://www.window security.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part1.html

Santora, M. (2013, May). *In Hours, Thieves Took $45 Million in A.T.M. Scheme - NYTimes.com*. Retrieved March 2013, from http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-thefts.html?pagewanted=1&_r=0

Schaffhauser, D. (2010). New York District Faces $500,000 Loss in Cyber Bank Theft. Retrieved March 16th, 2014, from http://thejournal.com/articles/2010/01/12/new-york-district-faces-500000-loss-in-cyber-bank-theft.aspx

Scott, M. (2009). Account take-over fraud. Retrieved from www.stpaul.gov/DocumentView

Shackelford, S. (2012). *Should your firm invest in cyber risk insurance?* Retrieved from www.sciencedirect.com

Shan, Y. (2010). Could China and Russia corporate to have a cyber attack towards the US economic industry? Retrieved from http://blog.tianya.cn/blogger/post_read.asp?BlogID=18597&PostID=21901225

Sherstobitoff, R. (2013). Analyzing Project Blitzkrieg, a Credible Threat (pp. 18). Santa Clara, CA: McAfee Labs.

SIFMA (2013). Cybersecurity Exercise: Quantum Dawn 2. Retrieved from http://www.sifma.org/services/bcp/cybersecurity-exercise--quantum-dawn-2/

Skalak, S., Patel, D., Tan, A., Nestler, C., Burg, D. (2014). Global economic crime survey 2014. *Pwc*. Retrieved from http://www.wm.edu/about/administration/provost /mission/index.php

Smith, G. (2013, October). *Feds Charge 13 Members Of Anonymous In 'Operation Payback' Attacks*. Retrieved March 2014, from http://www.huffingtonpost.com/2013/10/03/anonymous-charges-operation-payback_n_4039887.html

Snow, G. (2011, September 14). Statement before the House of Financial Service Committee. Retrieved from http://www.fbi.gov/news/testimony/cyber-security-threats-to-thefinancial

Snyder, M., (2013). Big banks are being hit with cyberattacks “every minute of every day”. *Infowars.com.* Retrieved from: http://www.infowars.com/big-banks-are-being-hit-with-cyberattacks-every-minute-of-every-day/.

Steiner, C. (2012). *Automate This: How Algorithms Came to Rule Our World.* Portfolio.

Stewart, S. (2011, January 27). *The Moscow Attack and Airport Security*. STRATFOR Global intelligence. Retrieved from: http://www.stratfor.com/weekly/20110126-moscow-attack-airport-security

Stewart, S. (2012, July 26). *The persistent threat to soft targets*. STRATFOR Global Intelligence*.* Retrieved from: http://www.stratfor.com/weekly/persistent-threat-soft-targets.

Strohm, C. Englemann, E. (2012). Capital One Target as Cyber Attacks Resume on U.S. Banks. Retrieved March 15th, 2014, 2014, from http://www.businessweek.com/news/2012-10-09/capital-one-target-as-cyber-attacks-resume-on-u-dot-s-dot-banks

Sverdlove, H. (2011). Cyber Attack at IMF – Why Motivations Matter. Retrieved March 19th, 2014, from https://blog.bit9.com/2011/06/12/cyber-attack-at-imf-why-motivations-matter/

Symantec (2013). *Internet Security Threat Report (*18). Symantec.

TechRepublic (2008, October). *Process 300 million transactions a day*. Retrieved March 2014, from http://www.techrepublic.com/blog/decision-central/process-300-million-transactions-a-day-without-going-crazy/

Tendulkar, R. (2013). Cyber-crime, securities markets and systemic risk (pp. 59): IOSCO.

Thomas, T. (2012). *Three Faces of the Cyber Dragon; Cyber Peace Activist, Spook, Attacker.* Fort Leavenworth, Kansas: Foreign Military Studies Office.

The top 10 biggest financial crimes in history. (n.d.). Retrieved from http://www.safety -security-crazy.com/financial-crimes.html

Top 10 most notorious cyber attacks in history. Retrieved from: http://www.arnnet.com.au/slideshow/341113/top_10_most_notorious_cyber_attacks_history/?image=6

Travis, A. (2001, April 18). *Internet banks 'in denial' on hacking thefts*. Retrieved March 21, 2014, from The Guardian: http://www.theguardian.com/technology/2001/apr/19/security.hacking

Trigaux, R. (2000). *A History of Hacking*. Retrieved March 18, 2014, from St. Petersburg Times online: http://www.sptimes.com/Hackers/history.hacking.html

Tropina, T. (2014). Cyber crime and organized crime. *Freedom from Fear.* Retrieved from http://www.freedomfromfearmagazine.org/

Trustwave.*2013 Global Security Report*. Rep. N.p.: Trustwave, n.d. Print.

Tsukayama, H. (2012). Report warns of cyber threat to US banks Retrieved March 15th, 2014, from http://www.independent.co.uk/news/world/americas/report-warns-of-cyberthreat-to-us-banks-8412295.html

U.S. Army Training and Doctrine Command. (2010). *Cyberspace Operations Concept Capability Plan 2016-2028.* United States Army.

US Attorney's Office. (2013, July 25). *Manhattan U.S. attorney and FBI assistant director in charge announce charges against Russian national for hacking NASDAQ servers*. Retrieved from http://www.fbi.gov/newyork/press-releases/2013/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-charges-against-russian-national-for-hacking-nasdaq-servers

USA Today. (2014, February). Target card breach and what to do: Our view. Retrieved from http://www.usatoday.com/story/opinion/2014/01/02/target-credit-card-debit-card-breach editorials-debates/4295661/

USA Today, (2013, December). Banks, regulators moving to thwart cyber attacks. Retrieved from http://www.usatoday.com/story/money/business/2013/12/09/financial-institutions cybersecurity/3929969/

US-CERT. (2009, November 4). Security Tips (ST04-015): Understanding Denial-of-Service Attacks. Washington D.C.: Retrieved from http://www.us-cert.gov/ncas/tips/ST04-015.

US-CERT. (2013). US-CERT Security Trends Report: 2012 in Retrospect. Washington D.C.: Retrieved from https://www.us-cert.gov/sites/default/files/US-CERT_2012_Trends-In_Retrospect.pdf.

US Telecom (2013). Internet Usage. Retrieved April 29th, 2014 from http://www.ustelecom.org/broadband-industry/broadband-industry-stats/internet-usage

von Clausewitz, C. (1984). *On War.* (M. Howard, P. Paret, Eds., M. Howard, & P. Paret, Trans.) Princeton, New Jersey: Princeton University Press.

Wallace, G. (2013, December 23). *Target Credit Card Hack: What you need to know*. Retrieved March 21, 2014, from CNN Money: http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/

Waterman, S. (2013). Tag team: Jihadist, hackers join forces to launch cyber-attacks on United States. Retrieved March 16th, 2014, from http://www.washingtontimes.com/news/2013/may/6/jihadis-and-hackers-teaming-launch-cyberattacks-us/

Whiteside, T. (1979). *Computer Capers: Tales of Electronic Thievery, Embezzlement and Fraud.* Ty Crowell.

Whittaker, Z. (2013). As NASDAQ's site hit by hackers, report says half of world's exchanges suffered cyber-attacks. Retrieved March 16th, 2014, from http://www.zdnet.com/as-nasdaqs-site-hit-by-hackers-report-says-half-of-worlds-exchanges-suffered-cyberattacks-7000018243/

Wiener, N. (1948). *Cybernetics, or Control and Communication in the Animal and the Machine.* New York: John Wiley & Sons.

Wilmshurst, E. (2008). *Definition of Aggression*. United Nations Audiovisual Library of International Law. Retrieved from: http://legal.un.org/avl/pdf/ha/da/da_e.pdf

Zhan, Y. (August, 2008). Strategic considerations for army transformation. Beijing Zhongguo Junshi Kexue. *China military science*, pp. 86-97.