JPMorgan Chase & Co.

SANS Cyber Threat Intelligence Summit

An End User's Perspective on the Threat Intelligence Industry

February 3, 2016

About Me

- JPMorgan Chase Global Chief Information Security Officer
- Financial Services Information Sharing and Analysis Center (FS-ISAC) Board Member
- Lockheed Martin Global Cybersecurity Solutions
- BS/MS University of Pennsylvania
- Doctoral degree in Information Security from George Washington University
- Co-authored the seminal paper on Intelligence Driven Defense and the Cyber Kill Chain

JPMorgan Chase & Co.

	Consumer & Community Bank	Corporate and Investment Bank	Commercial Banking	Asset Management
What We Do	Help people bank, save, invest, make purchases with credit cards and finance homes and cars	Offers a suite of investment banking, market-making, prime brokerage and treasury and security products and services	Provides credit, banking and treasury services to mid-sized businesses, corporations, municipalities, financial institutions nonprofit entities, and real estate owners and investors	Manages money for many of the world's wealthiest individuals and families and institutions
Highlights	■ #1 in ATMs, #2 in branches and #1 online banking portal ■ #1 in deposit growth among the largest 50 U.S. Banks ■ #1 credit card issuer in U.S. based on loans outstanding ■ #1 in total U.S. credit and debit payments volume ■ #2 mortgage originator and servicer ■ # 1 in customer satisfaction amongst the largest US banks for the 3rd consecutive year	■ #1 for Global Investment Banking fees with 8.1% wallet share ■ #1 wallet share in North America and EMEA ■ >80% of Fortune 500 companies do business with us ■ #1 firm in U.S. dollar clearing for clients ■ $20 trillion in assets under custody in 2015 ■ $34.6 billion in net revenue	■ Approximately 59,000 clients in the United States across 119 cities in the United States and 13 major international cities ■ Top 3 traditional middle market syndicated lender ■ #1 U.S. multifamily lender ■ #1 cash management portal in North America	■ Serve more than 3,000 financial intermediaries and 60% of the largest pension and sovereign wealth funds ■ Assets Under Management: $1.7 Trillion

Source: 2014 Annual Report, How We Do Business, 2015 Investor Day Presentation and 2015 4Q Earnings all of which can be found at http://investor.shareholder.com/jpmorganchase/index.cfm

JPMorgan Chase & Co. - By the Numbers

$9B

Annual spend on technology

$500M+

Spent on cyber capabilities in 2015 up from the $250 Million outlay in 2014

~$6T

Payments daily on behalf of the firm and its clients and customers in 2015

66K

Servers in 32 strategic data centers in 2014

318K

Desktops supported for over 200,000 employees in 2014

35M+

Active online and over 19 million active mobile clients and customers in 2015

Source: 2015 4Q Earnings and 2014 Annual Report all of which can be found at http://investor.shareholder.com/jpmorganchase/index.cfm

Agenda

How Large Financial Institutions Use Threat Intelligence

Shortcomings of Threat Intelligence

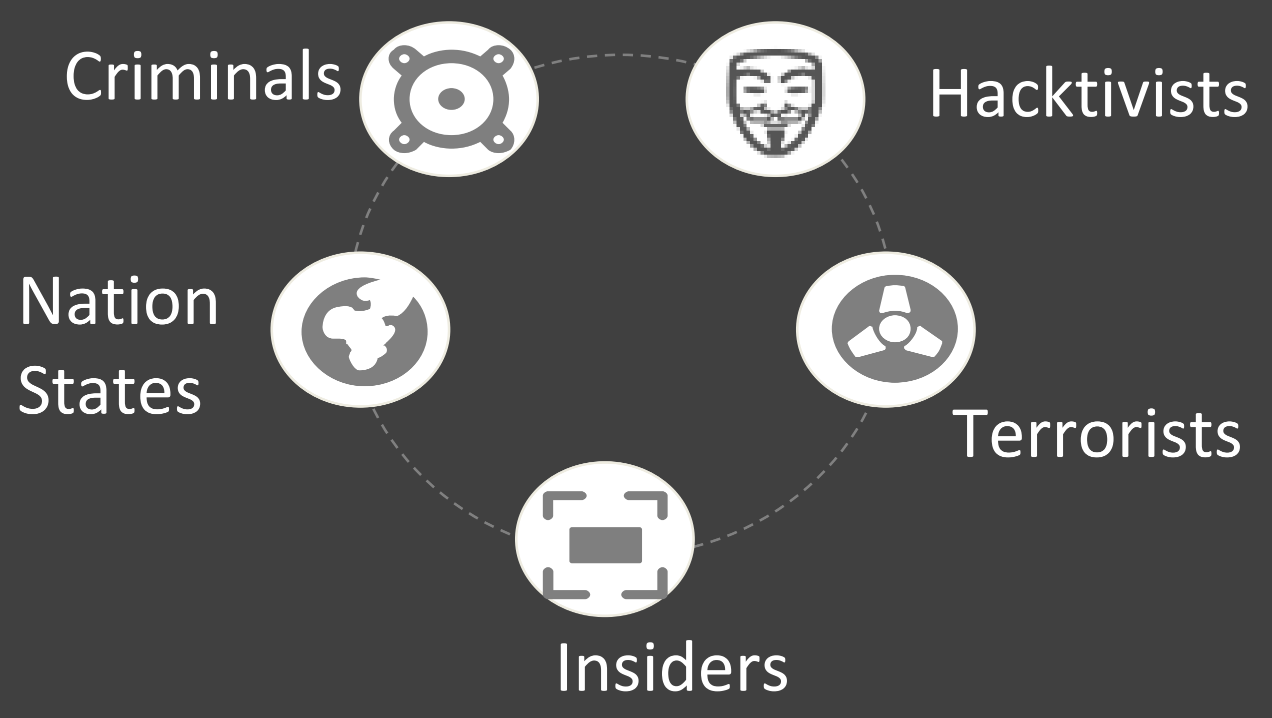
Q&A

How Large Financial Institutions Use Threat Intelligence

Cybersecurity Drivers

A Continuously Changing Operating Environment

Changing Threat Environment



Criminals

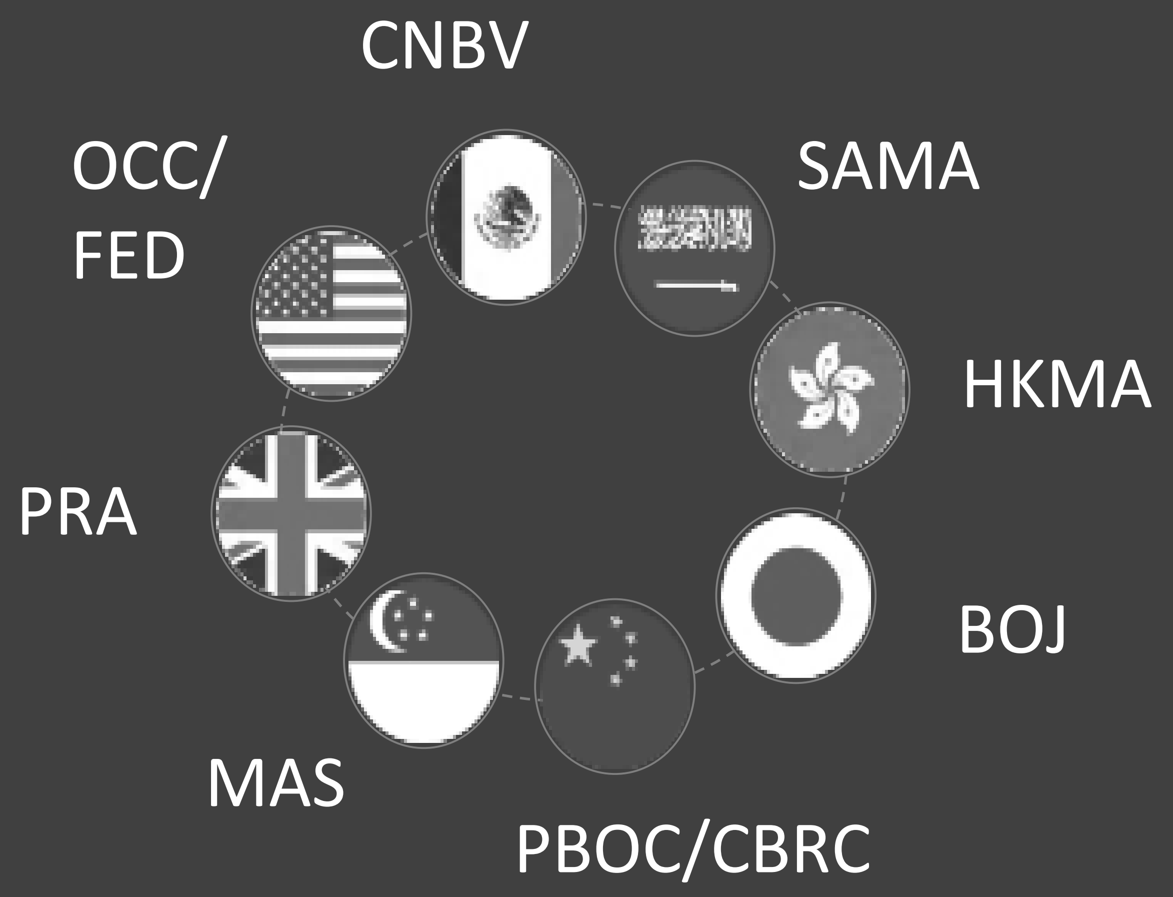
Hacktivists

Nation States

Terrorists

Insiders

Global Regulatory & Government Environment



CNBV

OCC/ FED

SAMA

HKMA

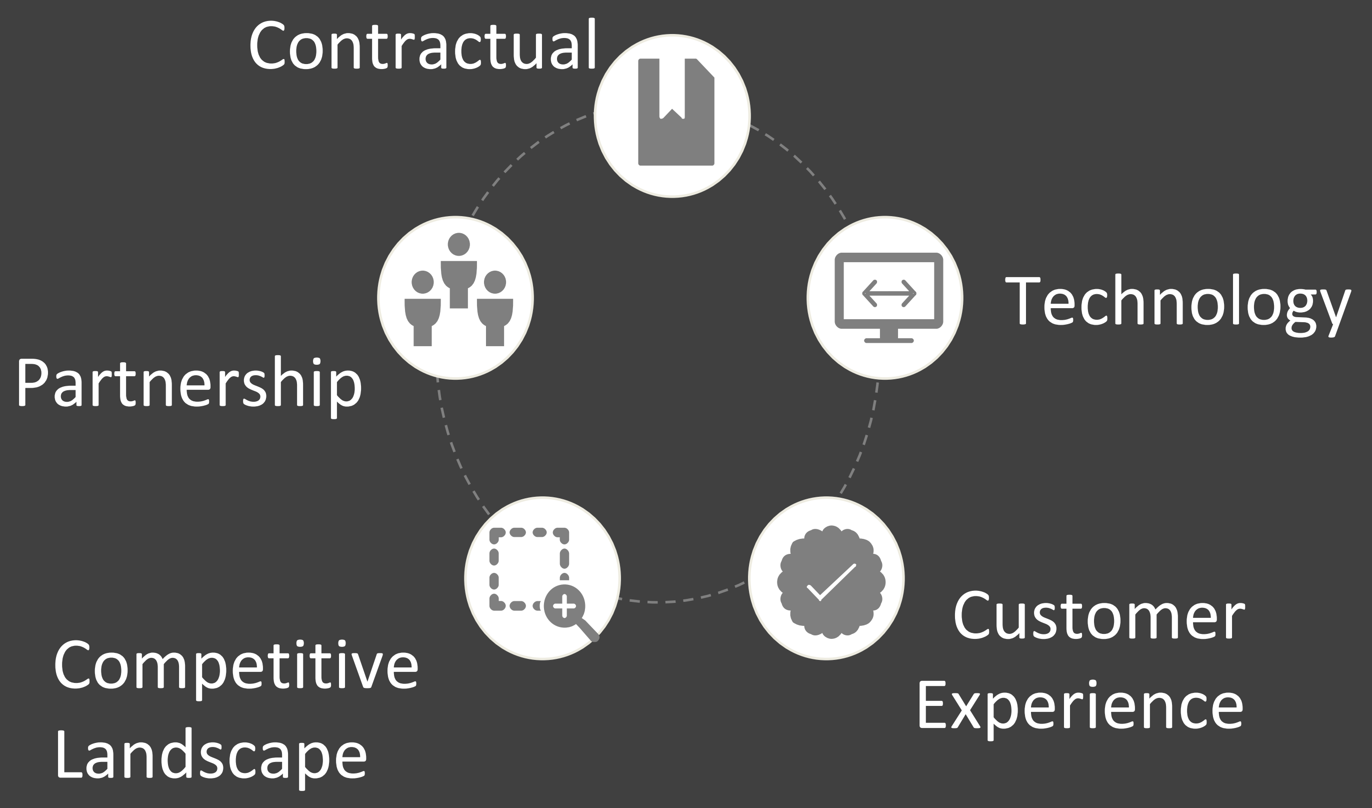
PRA

BOJ

MAS

PBOC/CBRC

Business Agenda



Contractual

Partnership

Technology

Competitive Landscape

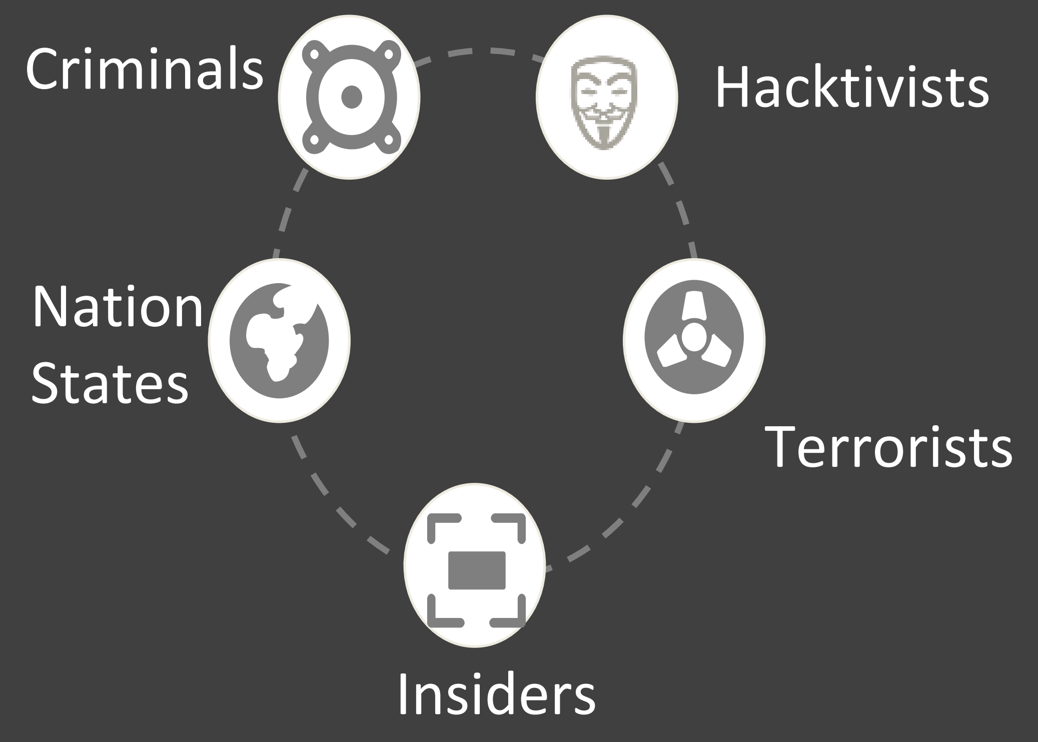
Customer Experience

Operational Risk Framework

Identify

What are the risks?

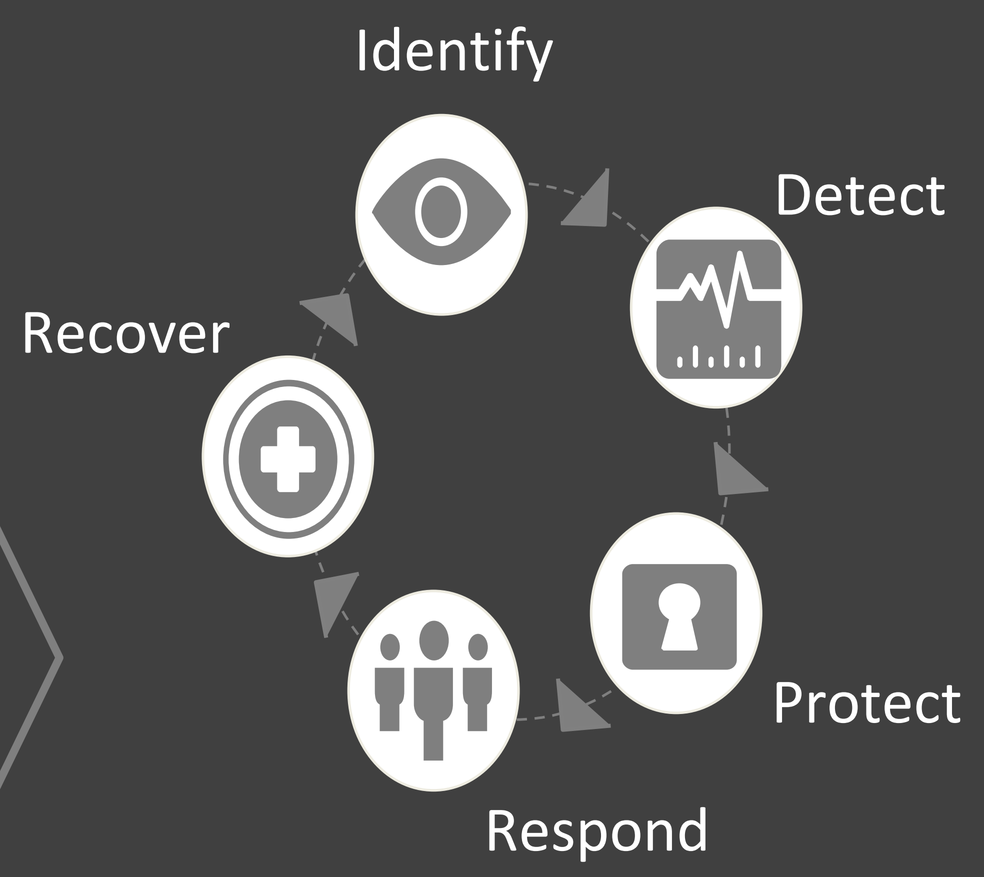
Changing Threat Environment



Threat	Likelihood			Impact			Inherent Risk
	L	M	H	L	M	H	

Control

How do we Protect?



Threats \ Controls			
		R	
		A	R
		G	

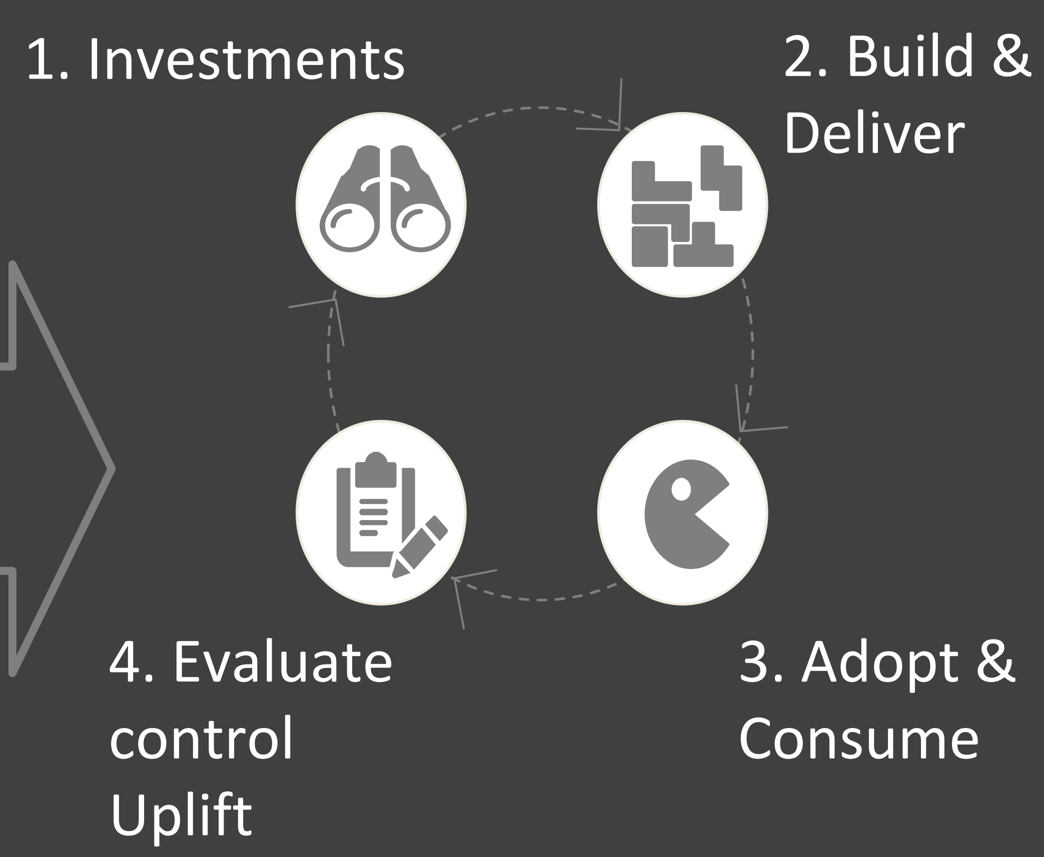
Assess

How effective are the Controls?

Top Threats	Top Controls
1. *Cybercrime & Fraud* 2. *Disruption of IT* 3. *Integrity* …	1.*Continuous Monitoring* 2. *Access Control* 3.*Recovery Planning* …

Treat

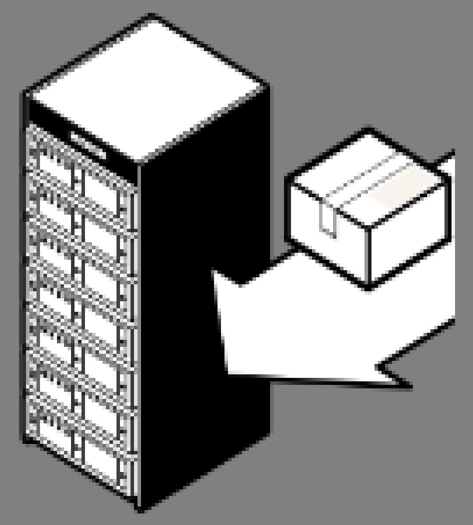
How do we reduce risk exposure?



Reducing the Impact – Fraud Kill Chain

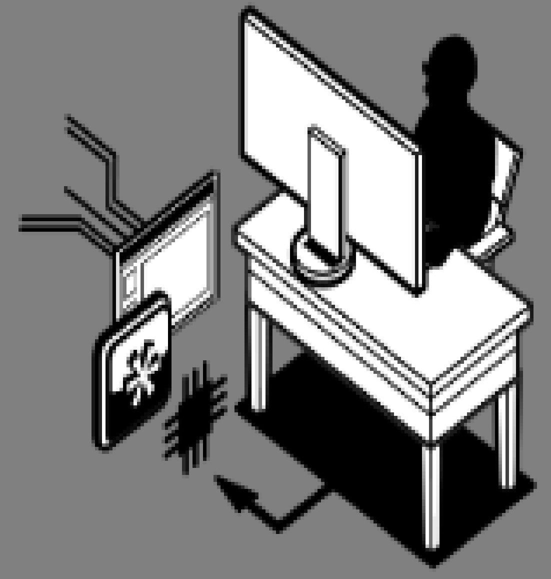
External Reconnaissance

Target research and collection of information on selected targets



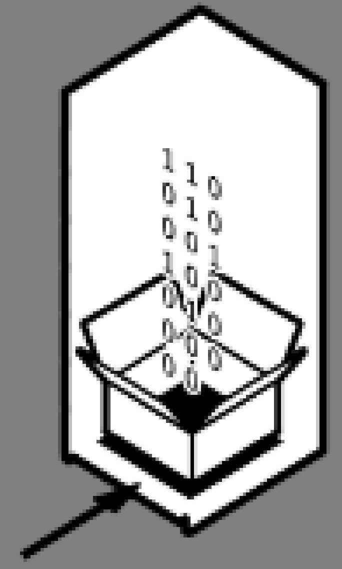
Delivery

Transmission of payload (phish, malware, etc.) to selected targets



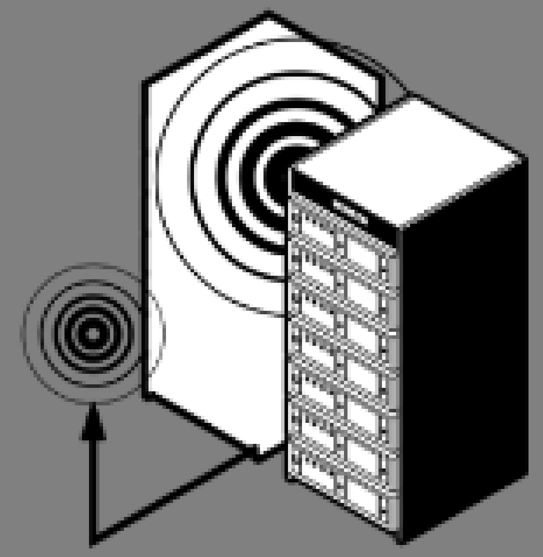
Exploitation

Execution of the delivered payload through system vulnerability, social engineering or both



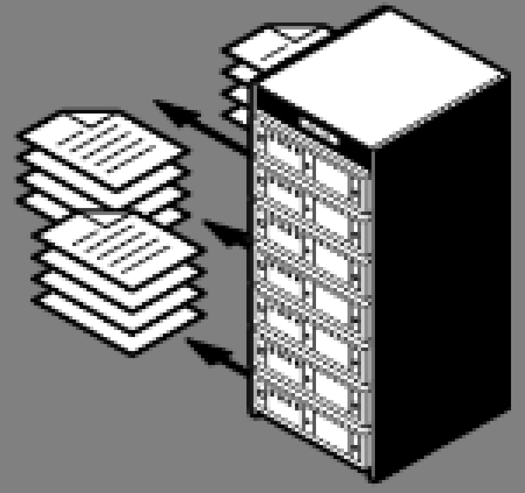
Positioning

Attacker positioning themselves to complete their goals while limiting exposure



Abuse

Attacker takes initial action toward realization



Monetization

Attacker completes goal

Pre-Compromise → Post Compromise/Pre-Abuse → Post Abuse

← Outside JPMC (Limited Visibility) → ← Inside JPMC (Visibility) →

← Cyber Defense Strategy allows a firm to identify attackers earlier in the Kill Chain, reducing the impact of attacks

Review of Regulatory Requirements

FFIEC – Guideline Maturity Level	FFIEC Declarative Statement
Advanced	Threat intelligence is viewed within the context of the institution's risk profile and risk appetite to prioritize mitigating actions in anticipation of threats.
Advanced	Threat intelligence is used to update architecture and configuration standards.
Innovative	The institution uses multiple sources of intelligence, correlated log analysis, alerts, internal traffic flows, and geopolitical events to predict potential future attacks and attack trends.
Innovative	Highest risk scenarios are used to predict threats against specific business targets.
Innovative	IT systems automatically detect configuration weaknesses based on threat intelligence and alert management so actions can be prioritized.
Advanced	Management communicates threat intelligence with business risk context and specific risk management recommendations to the business units.
Innovative	A mechanism is in place for sharing cyber threat intelligence with business units in real time including the potential financial and operational impact of inaction.
Innovative	A system automatically informs management of the level of business risk specific to the institution and the progress of recommended steps taken to mitigate the risks.

Source: FFIEC Cybersecurity Assessment Tool Study

Shortcomings of Threat Intelligence

Indicators of Compromise != Threat Intelligence

Less Important

- Quantity
- Number of Feeds

More Important

- Quality
- Context

News != Threat Intelligence

Less Important

- Daily open source summary of articles

More Important

- Tell me something not in the news

Understand My Business

Less Important

- Generic threat and vulnerability data

More Important

- Understand specific industries and new business models

Requirements are Important

Less Important

- What requirements?

More Important

- Formalized processes for intelligence collection and subsequent tasking

APT is not everything

Less Important

- APT-itis

More Important

- Stronger focus on criminal and non-espionage related threats

Q&A