January 2016

Cyber Security Challenge

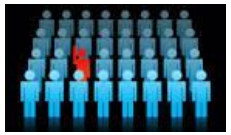
TJ Harrington
Managing Director & Chief Information Security Officer

Cyber Security Key Assumptions for 2016

- The **frequency, speed, and effectiveness** of sophisticated cyber attacks will continue to increase
- Our adversaries represent an **asymmetrical threat**, which includes sophisticated criminal syndicates, nation-states, terrorists, activists and insiders
- **Cyber Security Defensive Strategies** must have a strong prevention component… but no organization can be 100% successful with only a prevention strategy so our ability to detect and respond are equally critical
  - A "Defense in Depth" approach is required, but informed by an Intelligence-led Strategy
- Being **Intelligence-led** is fundamental to long-term success
  - Business Model and Management Philosophy
    - Know your adversary – their motivations, their tactics, techniques, and procedures (TTPs)
    - Know yourself – strengths, challenges, gaps – understand what you value
    - Create a Learning Organization built on a foundation of Information Sharing
    - Integrate Threat Intelligence and Analysis into Decision-Making
- Our adversaries are networked and to match them in agility, adaptability, creativity and speed, we need to create **trusted networks** with a common purpose, shared awareness and empowerment to act to protect the firm
  - Creating a *Team of Teams*, within the firm and among our Clients, Partners and Government entities to facilitate cross-silo and cross-organization collaboration is necessary
- **Crisis Management Preparation** is key to managing a major intrusion and must be practiced

Recognition of an Asymmetrical Cyber Threat Landscape

Threat Actors

Nation-State Actors 	• Motivation: theft of trade or craft secrets or support of military capabilities and nationalized industries • Methods: advanced operations to establish a foothold into infrastructure
Organized Criminals 	• Motivation: make money • Methods: spear-phishing and other techniques; mature underground economy supporting criminal activity
Cyber Terrorists 	• Motivation: instill fear to have targets comply with demands or ideology • Methods: using Cyber to “enable” their programs (recruit, incite, train, plan and finance)
Hacktivists 	• Motivation: seek publicity for their geopolitical agenda • Methods: disruption (i.e., Distributed Denial of Service) and defacement
Insiders 	• Motivation: emotional or sometimes financial needs • Methods: uses insider knowledge to steal data, conduct fraud, etc.

Methods

Social Engineering	A common tactic, at times even non-technical, that relies on human interaction to trick other people to break normal security procedures, allowing them to gain information that may be useful for exploit efforts.
Phishing and Spear-Phishing	Emails, online posts, or other electronic communications that masquerade as a trustworthy party in an attempt to trick the target into divulging information or download malware.
Destructive Malware	Malware is a category of malicious code that includes viruses, worms and Trojan horses. Destructive malware will utilize popular communication tools to spread, including worms sent through email and virus-infected files downloaded from peer-to-peer connections.
Exploit Kits	Packs containing malicious programs that are mainly used to carry out automated ‘drive-by’ attacks in order to spread malware. These kits are sold on the black market, where prices ranging from several hundred to over a thousand dollars are paid. These kits will seek to exploit existing vulnerabilities on systems making their entry quiet and easy.
Drive by Downloads	A program that is automatically installed on a target’s computer by merely visiting a website. Victims do not have to explicitly click on a link within the page.
Distributed Denial of Service	Through computer programs and/or an increased number of participants, hackers flood the attack target’s website with more traffic than the server can handle. As the site attempts to process the large number of malicious traffic, it denies access from legitimate users. The rush of traffic could also cause servers to crash.

Cyber Security: Strategy Overview

Objective: Protect your firm through an Intelligence-led, Threat Focused Defense Network with strong levels of Prevention, Detection, Response and Recovery capabilities

Defense in Depth Execution

- ID & Access Management
- IS Risk Management
- Infrastructure Defense
- Security Incident Management
- Data Protection
- Privileged User Management Access
- Third Party IS Management
- Application Security Management

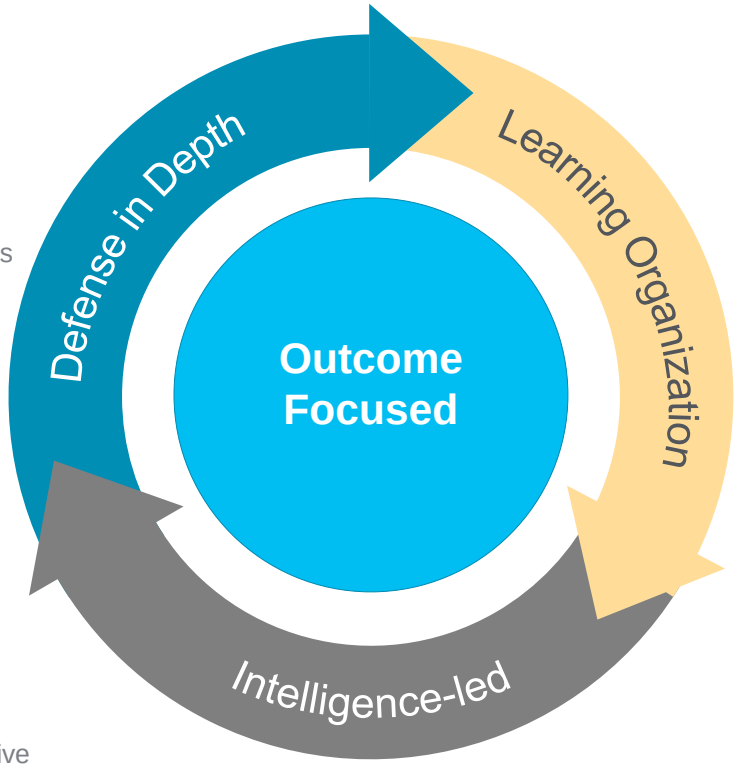
Intelligence-led Methodology

STRATEGIC

- Government Outreach
- Peer and Industry Outreach
- Client Outreach
- Analytical Reports/Studies

TACTICAL

- Forensic Analysis
- Data Analysis is support of preemptive action
- Intelligence Collection (Open Source, Vendor Supported)



Create a Learning Organization

Focus on creating learnings to support:
A) executive decision making B) operator / operations support

TALENT INVESTMENT

- Invest in professional Information Security Officers (ISO) and Analysts
- Professional Training Opportunities – On-the-Job and formal education
- Develop a Network of peers and associates to benchmark

TEAMWORK APPROACH

- Security Operation Centers
  ** Tactical day-to-day management*
- Cyber Fusion Center -- Team of Teams
  ** Situational Awareness, Analysis, Crisis Management*

Potential Key Performance Metrics ???

Citi's Intelligence-Led Information Security Strategy

Have adopted a preemptive posture through the development of threat intelligence that enables Citi to take action in anticipation of, rather than in reaction to, a threat.

Principles of an Intelligence-led organization

1	**Understand the Threat**	Gain knowledge of the adversary and their tradecraft; know ourselves, identify valuable assets and recognize challenges early in the threat cycle
2	**Integrate Threat Intelligence and Analysis Into Decision-Making**	Deliver tactical and strategic intelligence products that create knowledge and insight
3	**Establish a Learning Culture**	Ensure there are management processes and tools that enable key learnings to be raised in a collaborative environment and integrated into how we do business
4	**Build a Foundation of Information Sharing**	Increase internal and external information sharing in a trusted environment One detected event – **shared**, can serve as defense for a sector
5	**Strong Execution of Program Management**	Support an enterprise approach to integrated processes while conducting incident response in a learning cycle environment
6	**Maximize Collaboration**	Promote collaboration and partnerships both internal and external; sharing best practices and benchmarking (Peers, Clients, Government, Vendors)

citi

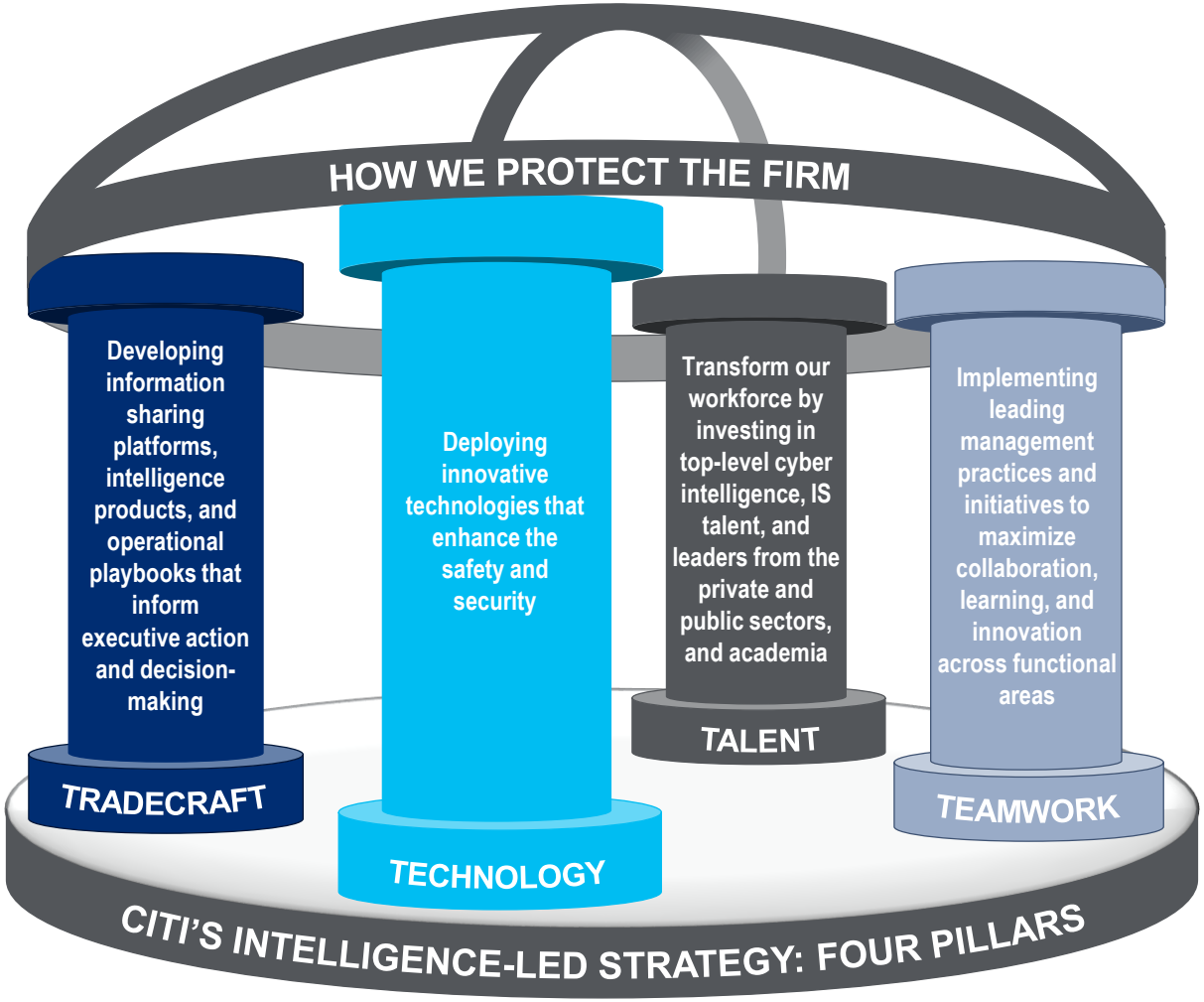
Citi's Intelligence-Led Information Security Investment Pillars

Citi is facing a must-win battle against sophisticated cyber adversaries. The mission of Citi Global Information Security is to prevent, detect, respond to, and recover from cyber attacks. Citi does this by implementing an intelligence-led strategy to protect the firm's data, assets, people, and reputation. Success requires that we consistently execute four components of our strategy: talent, teamwork, tradecraft, and technology.

Intelligence-led Information Security

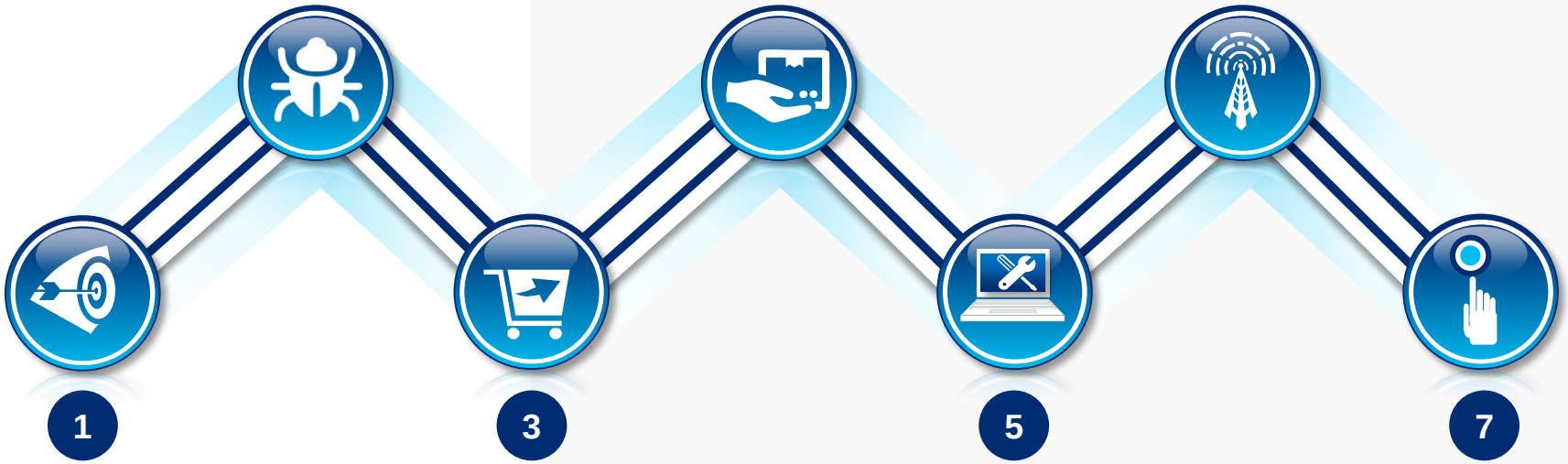
A business model and managerial philosophy where analysis and intelligence are pivotal to an objective, decision-making framework that facilitates information protection through effective implementation of IS strategies that target prolific and serious threat actors and threat methods.

**Adapted from Dr. Jerry Ratcliffe, Author of "Intelligence-led Policing"*



The Cyber Kill Chain

- Citi has adopted the 'Cyber Kill Chain' as a foundational component of our Cyber Intelligence and Security Strategy
- Our goal is to take advantage of the fact the attacker must expose tools, techniques and processes (TTPs) as they move through each phase of the intrusion chain



The Cyber Kill Chain is a Trademark of Lockheed Martin