FIA Webinar -
Cybersecurity Threats: Preparation & Response

June 29, 2015

Moderator:

Gregory Gist, Director, CBCP, Industry Relations, Office of Emergency Management, Citi

Speakers:

William Nelson, President & CEO, Financial Services Information Sharing and Analysis Center (FS-ISAC)

Leo Taddeo, Special Agent in Charge, Cyber/Special Operations, FBI New York Field Office

AMERICAS | EUROPE | ASIA

Cybersecurity Webinar

- The webinar will be recorded and posted to the FIA website following the conclusion of the live webinar.

- A question and answer period will conclude the presentation.
  - Please use the “chat” function on your webinar control panel to ask a question to the moderator or speakers. Questions will be answered at the conclusion of the webinar.

Cybersecurity Webinar

- **Overview of Webinar**
- **Background on Cybersecurity**

- *Speaker: Gregory Gist, Director, CBCP, Industry Relations, Office of Emergency Management, Citi*

New York Office
Cyber/Special Operations Division

Who are the Adversaries?

→ ★ *Sophistication* ★ *Expertise* ★ *Funding* ★ *Patience* ★ *Target Value* →

<u>Threat Level 1</u>

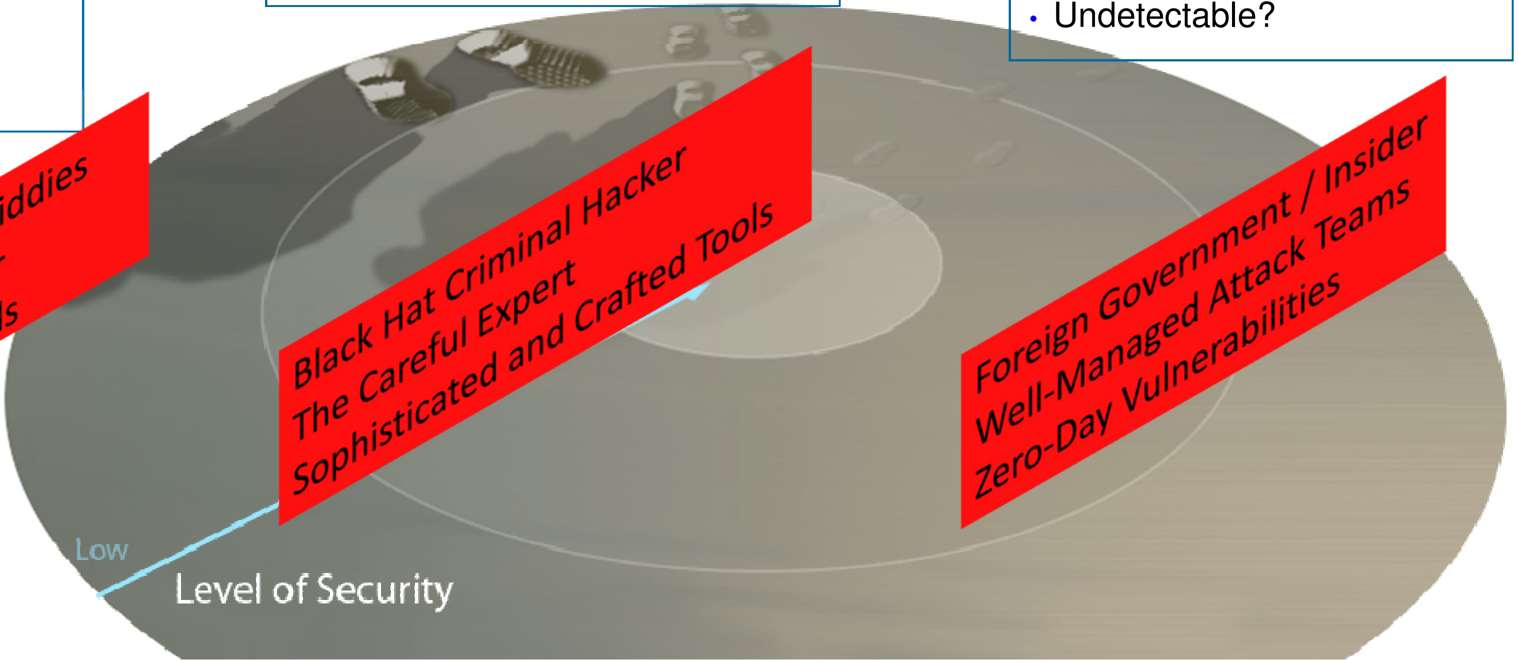
- Inexperienced
- Limited funding
- Opportunistic behavior
- Target known vulnerabilities
- Use viruses, worms, rudimentary trojans, bots
- In it for thrills, bragging rights
- Easily detected

<u>Threat Level 2</u>

- Higher order skills
- Well-financed
- Target known vulnerabilities
- Use viruses, worms, trojans, bots to introduce more sophisticated tools
- Target and exploit valuable data
- Detectable, but hard to attribute

<u>Threat Level 3</u>

- Very sophisticated tradecraft
- Foreign Intel Agencies
- Very well financed
- Target technology as well as info
- Use wide range of tradecraft
- Establish covert presence on sensitive networks
- Undetectable?



Ankle Biters / Script Kiddies
The Careless Beginner
Publicly Available Tools

Black Hat Criminal Hacker
The Careful Expert
Sophisticated and Crafted Tools

Foreign Government / Insider
Well-Managed Attack Teams
Zero-Day Vulnerabilities

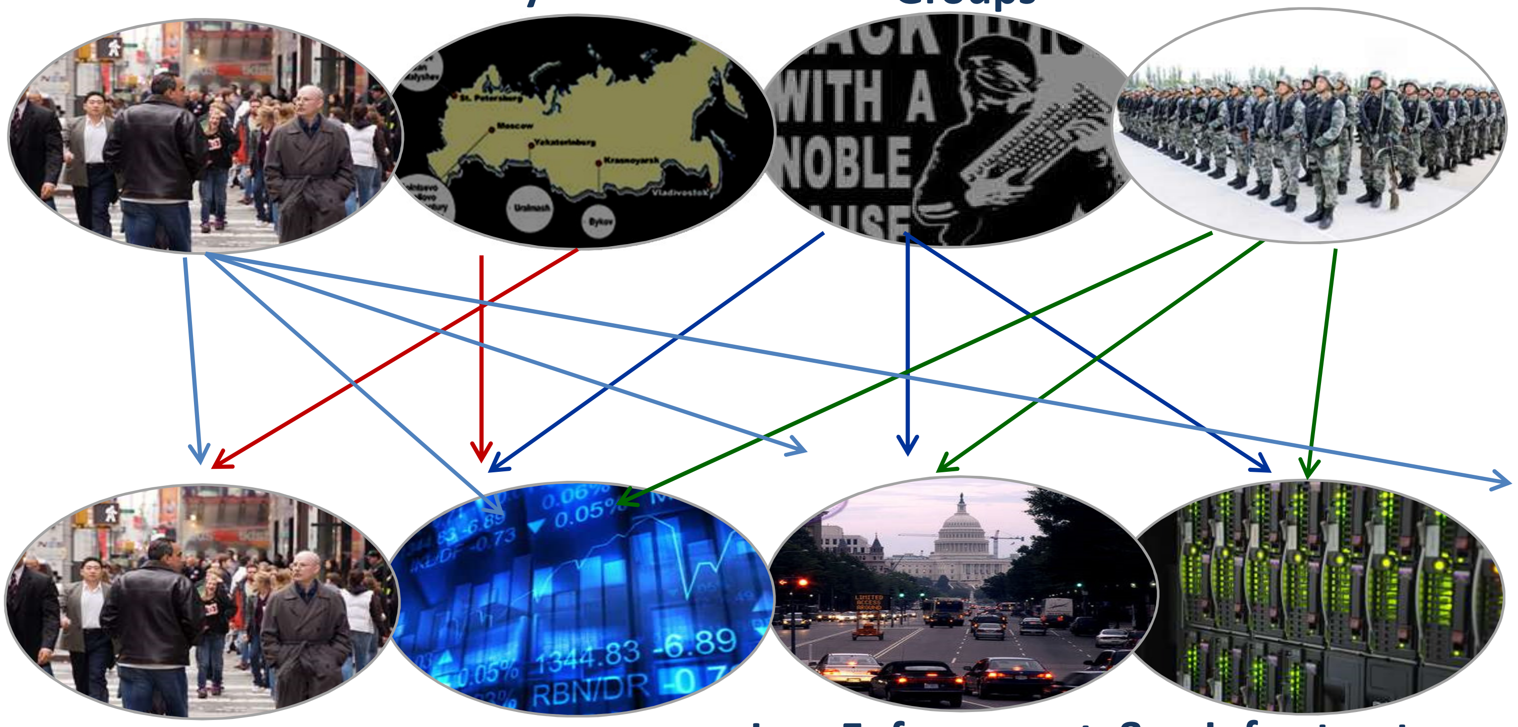
The Cyber Threat Reality

Individuals

Organized Crime Syndicates

Hacktivist Groups

Nation States



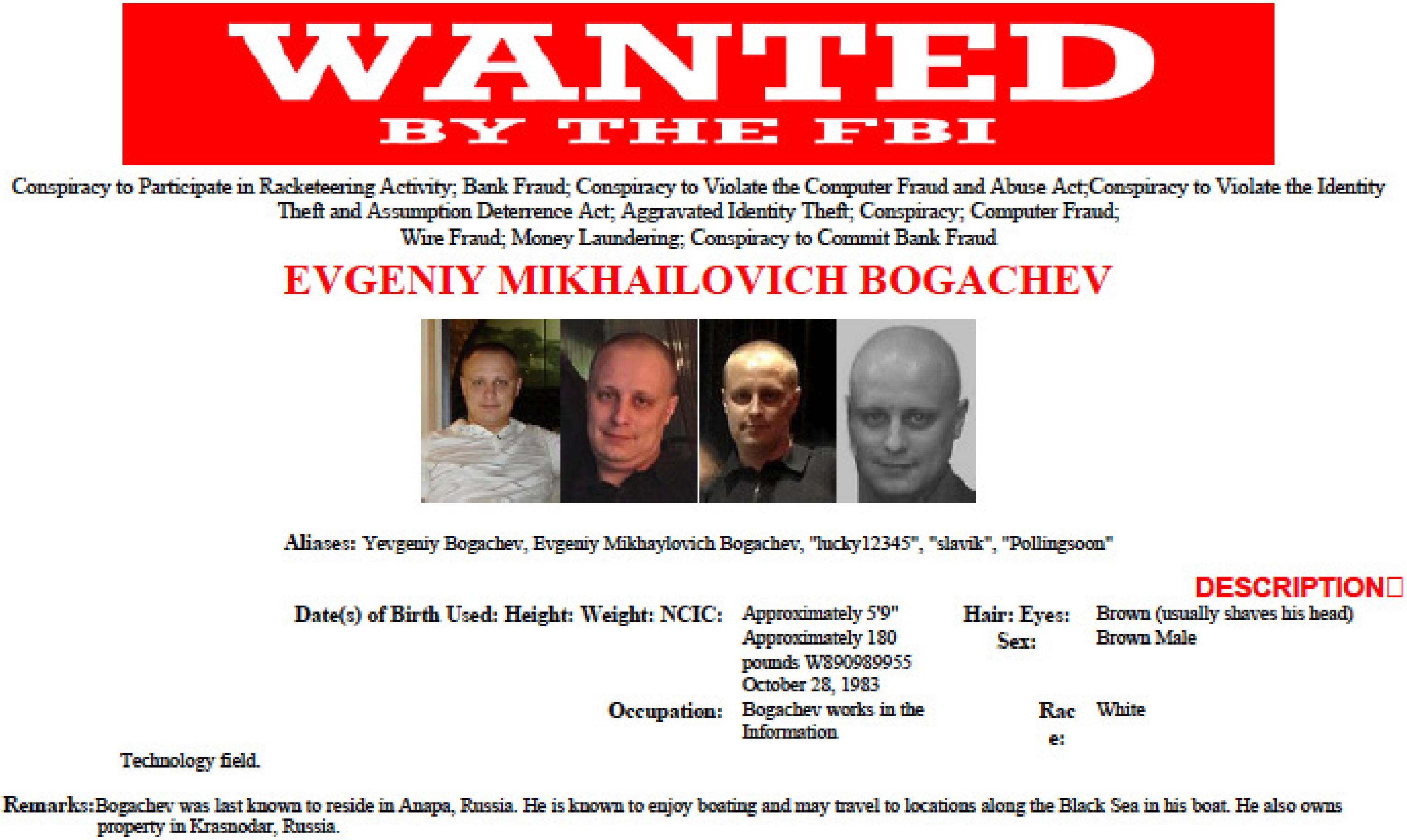
Individuals

Industry

Law Enforcement & Government

Infrastructure

GameOver Zeus



WANTED
BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act;Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

EVGENIY MIKHAILOVICH BOGACHEV

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

DESCRIPTION□

Date(s) of Birth Used: Height: Weight: NCIC: Approximately 5'9" Approximately 180 pounds W890989955 October 28, 1983

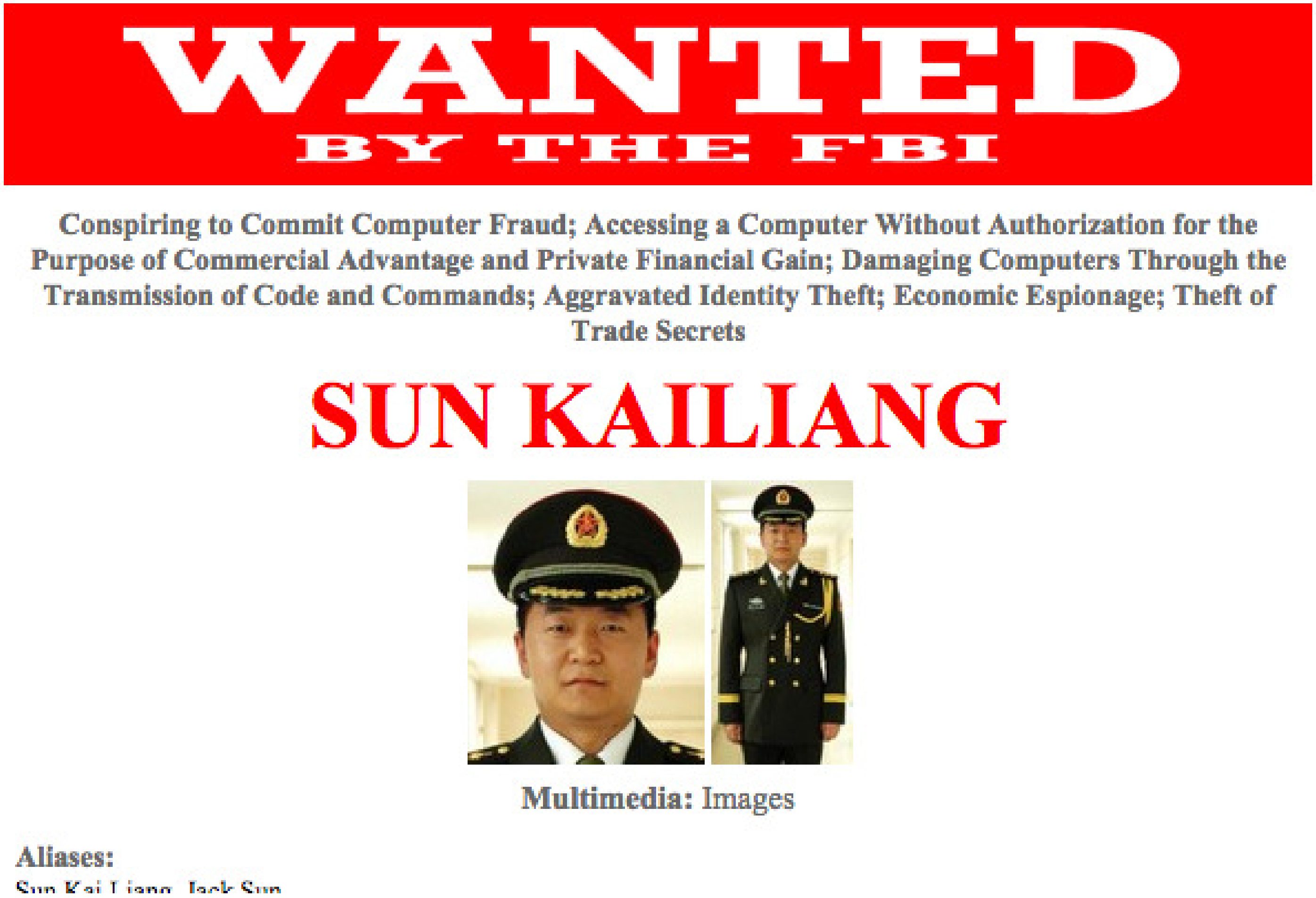
Hair: Eyes: Sex: Brown (usually shaves his head) Brown Male

Occupation: Bogachev works in the Information Technology field.

Rac e: White

Remarks: Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

People’s Liberation Army (PLA)



WANTED

BY THE FBI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

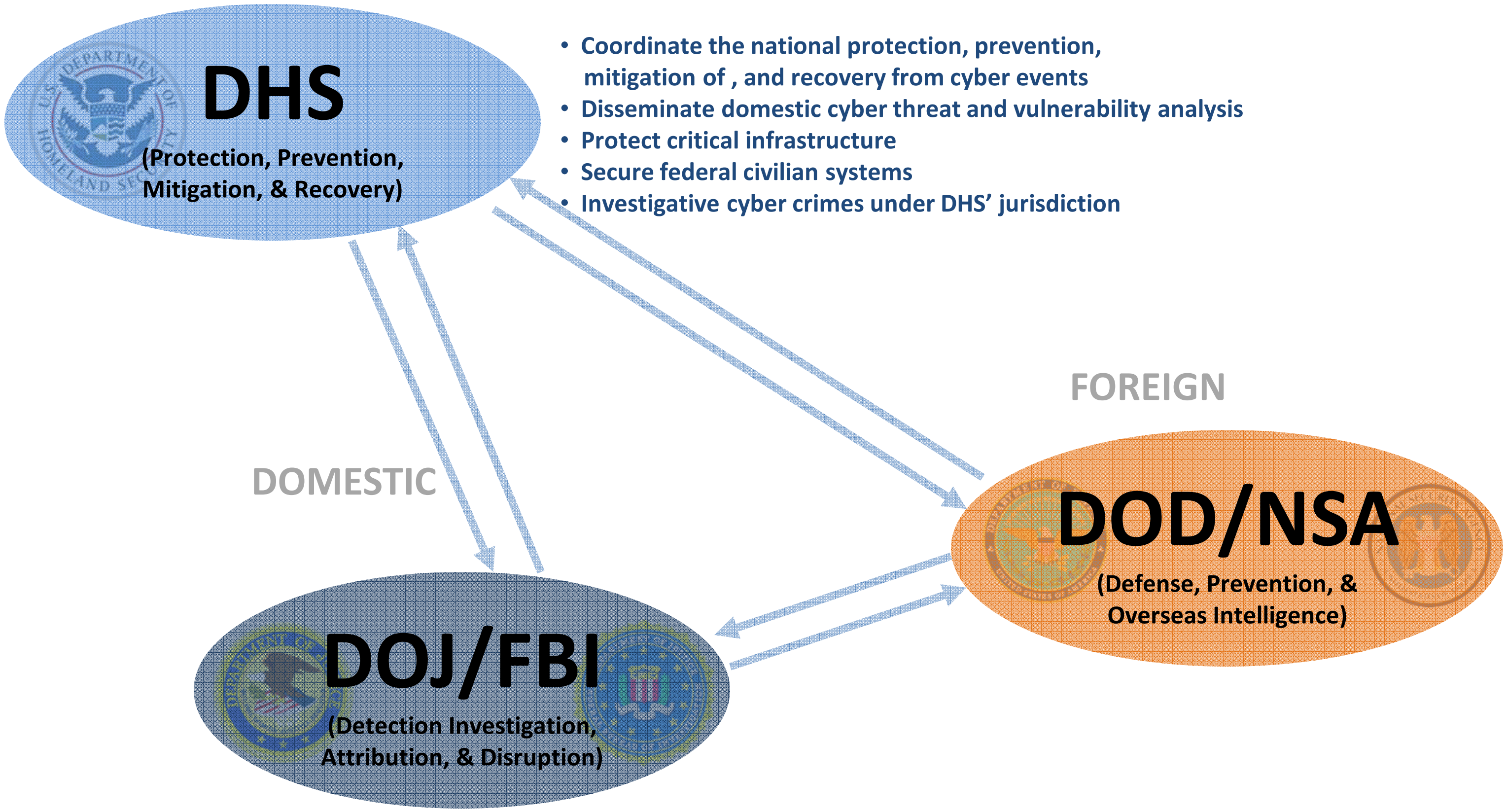
SUN KAILIANG

Multimedia: Images

Aliases:

Sun Kai Liang, Jack Sun

National Cybersecurity Framework



DHS

(Protection, Prevention, Mitigation, & Recovery)

- Coordinate the national protection, prevention, mitigation of , and recovery from cyber events
- Disseminate domestic cyber threat and vulnerability analysis
- Protect critical infrastructure
- Secure federal civilian systems
- Investigative cyber crimes under DHS’ jurisdiction

FOREIGN

DOMESTIC

DOD/NSA

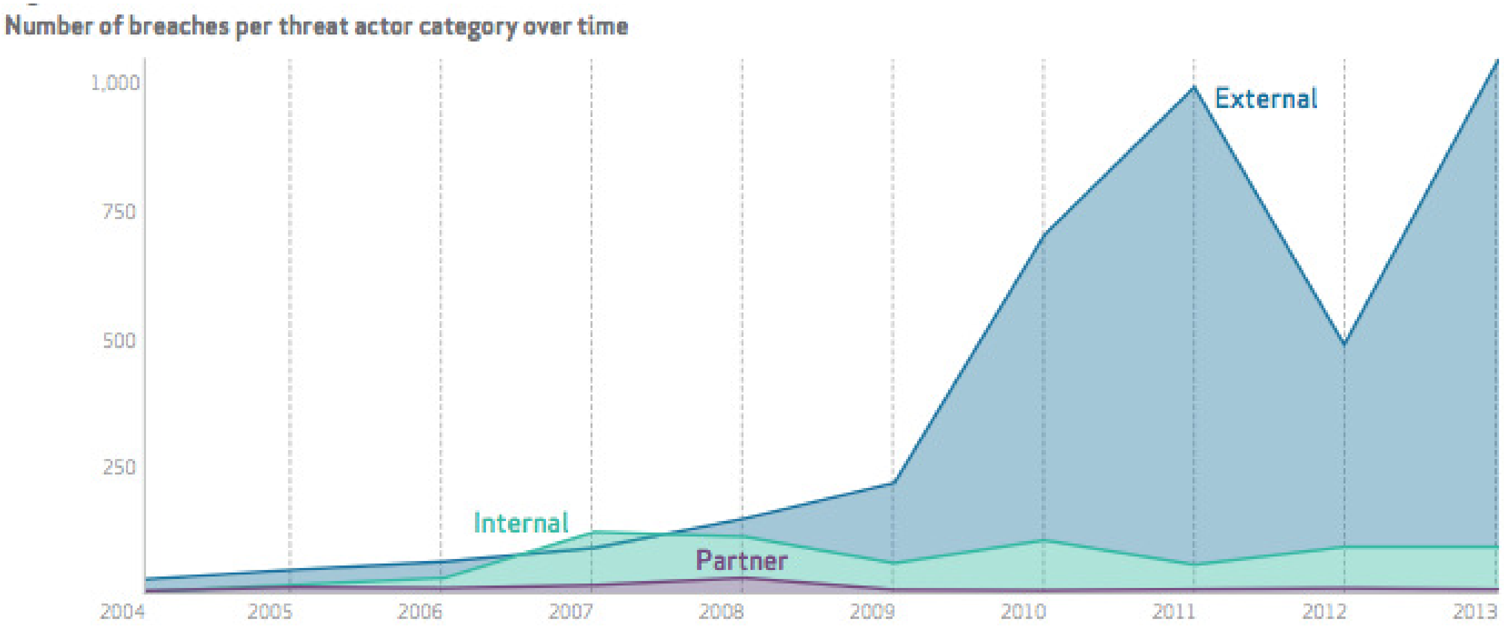
(Defense, Prevention, & Overseas Intelligence)

DOJ/FBI

(Detection Investigation, Attribution, & Disruption)

- Investigate, attribute, disrupt, and prosecute cyber crimes
- Lead domestic national security operations
- Conduct domestic collection, analysis, and dissemination of cyber threat intelligence
- Support the national protection, prevention, mitigation of, and recovery from cyber incidents
- Coordinate cyber threat investigations

External Breaches



- Source: Verizon 2014 Data Breach Investigations Report

When to Call Law Enforcement

- Public Safety
- Potential impact to critical infrastructure
- National security matters
  - Defense contractor
  - Classified databases
  - Origin of attack
- Criminal or nation-state
- Sophistication/Skill level of attacker
- Potential impact to other networks
- Potential financial loss to victim

Capabilities/Skill Sets

Network Traffic Analysis

- Analysis of network traffic (netflow and pcap)

  Router configuration files and other network related log files

Host-Based Forensics

- Collect forensic host images and live memory capture

  Analyze images for indicators of compromise

Malware

- Analyze samples of malicious code

Legal

- Process legal documentation (consent/trespasser)

Intelligence

- Research evidence in FBI/USIC databases and disseminate to partners

FBI Objectives in Responding to Cyber Incident

- Investigate and prosecute Cyber crimes
- Work with victim to →

★ Continue operations

  - System owner retains control of systems
  - System owner (not Special Agent) produces logs, memory images, etc.
  - No crime scene tape around your networks

★ Protect data

  - Not advance team for regulators or plaintiffs lawyers
  - Maintain confidentiality of PII and other protected data
  - Maintain confidentiality of incident

★ Assist in mitigation and recovery

  - Provide signatures, TTPs
  - Provide classified information as needed

Points of Contact

Call your local FBI field office:

- New York
  - Assistant Special Agent in Charge Richard Jacobs
    - Richard.Jacobs@ic.fbi.gov
    - 212-384-2949

- Chicago
  - Assistant Special Agent in Charge John Brown
    - John.Brown@ic.fbi.gov
    - 312-829-5187

FINANCIAL SERVICES ISAC

Cybersecurity Threats, Preparation, and Response

June 29, 2015

Financial Services
Information Sharing & Analysis Center

FINANCIAL SERVICES ISAC

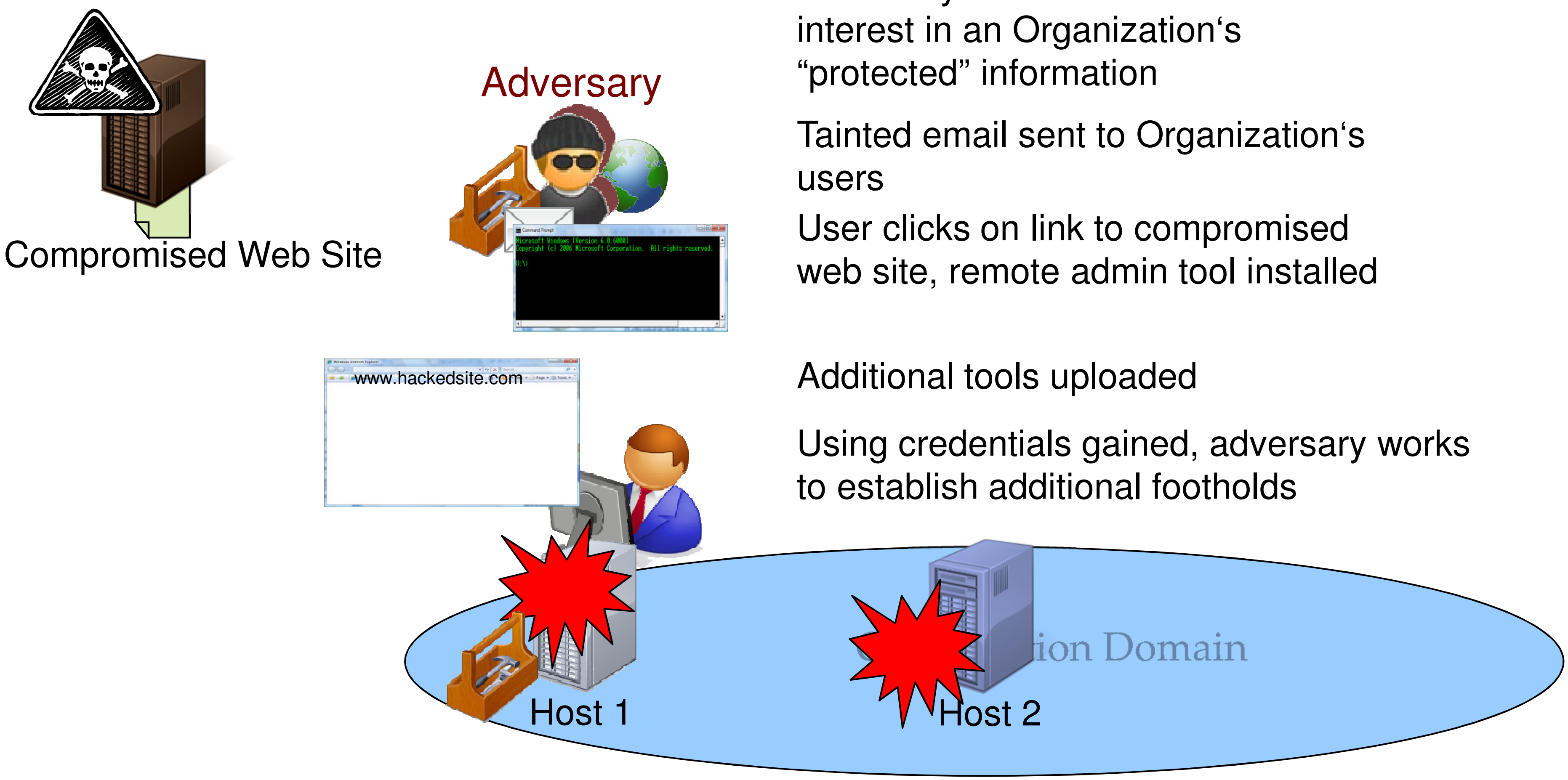
Anatomy of an Attack

Financial Services Information Sharing & Analysis Center

Attacker Mindset

- An adversary will attack the network’s weakest point
  - The User
  - The Supply Chain
- Targeting has become very selective
  - Executives & staff (access to data)
  - System and network administrators (privileged credentials)
  - Third Party vendors
- Open source information gathering allows the adversary to become very familiar with target prior to attack
  - Organizational structure, technologies, research activities
- Attacker will utilize minimum complexity to be successful
  - Simple techniques allow the adversary to leverage more attacks (less training and technology required)

Common Attack Scenario
Adversary Gains Foothold



```
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

U:\>
```

Adversary determines that it has an interest in an Organization‘s “protected” information

Tainted email sent to Organization‘s users

User clicks on link to compromised web site, remote admin tool installed

Additional tools uploaded

Using credentials gained, adversary works to establish additional footholds

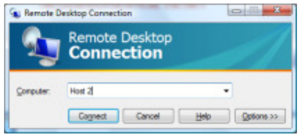
Common Attack Scenario
Data Mining

Adversary frequently will perform data mining through a host (Host 2) other than the initially compromised host (Host 1)

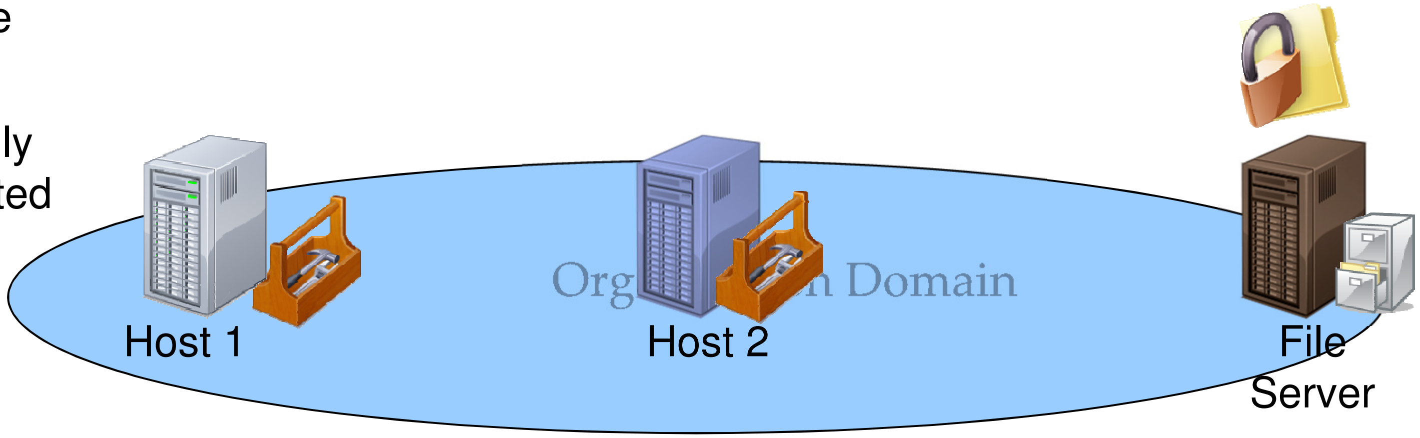
Remote host may or may not be the same IP/Domain as initial attack

Data mining typically occurs on file servers via share permissions

Multiple files are typically extracted as an encrypted bundle


Remote Desktop Connection

Computer: Host 2



FINANCIAL SERVICES | ISAC

Information Sharing

To be forewarned is to be fore-armed

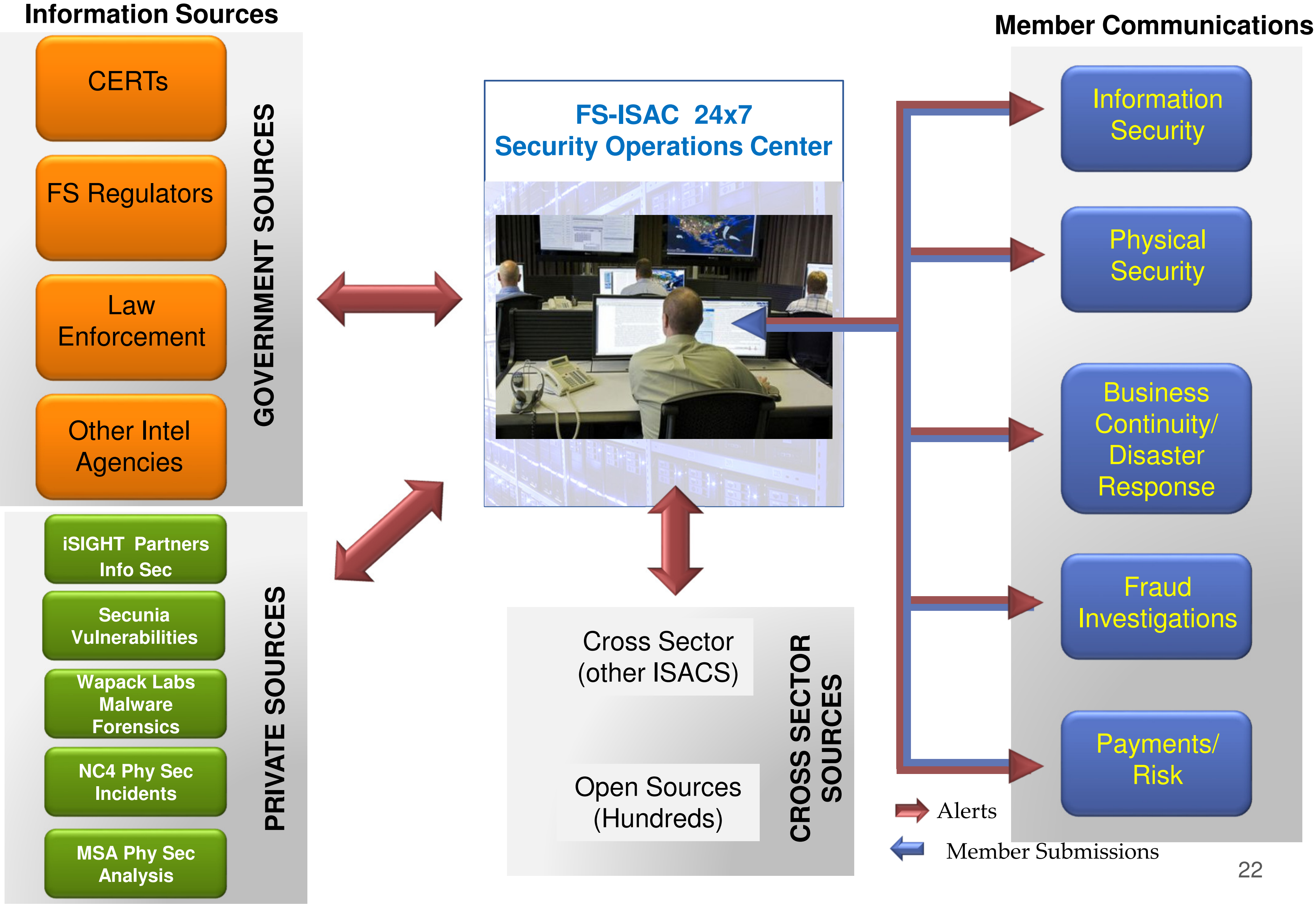
FS-ISAC MISSION:

Sharing Timely, Relevant, Actionable Cyber and Physical Security Information & Analysis

- A nonprofit private sector initiative formed in 1999
- Designed/developed/owned by financial services industry
- Mitigate cybercrime, hactivist, nation state activity
- Process thousands of threat indicators per month
- 2004: 68 members; 2015: 5700+ members
- Sharing information globally

FINANCIAL SERVICES ISAC

FS-ISAC Operations



Information Sources

GOVERNMENT SOURCES

- CERTs
- FS Regulators
- Law Enforcement
- Other Intel Agencies

PRIVATE SOURCES

- iSIGHT Partners Info Sec
- Secunia Vulnerabilities
- Wapack Labs Malware Forensics
- NC4 Phy Sec Incidents
- MSA Phy Sec Analysis

FS-ISAC 24x7 Security Operations Center

CROSS SECTOR SOURCES

- Cross Sector (other ISACS)
- Open Sources (Hundreds)

Member Communications

- Information Security
- Physical Security
- Business Continuity/ Disaster Response
- Fraud Investigations
- Payments/ Risk

→ Alerts

← Member Submissions

Information Sharing & Analysis Tools

Threat Data, Information Sharing

- **Anonymous Submissions**
- **CyberIntel Listserver**
- Relevant/Actionable Cyber & Physical Alerts (Portal)
- **Special Interest Group Email Listservers (Broker-Dealer, Asset Managers)**
- Document Repository
- Member Contact Directory
- Member Surveys
- Risk Mitigation Toolkit
- Threat Viewpoints

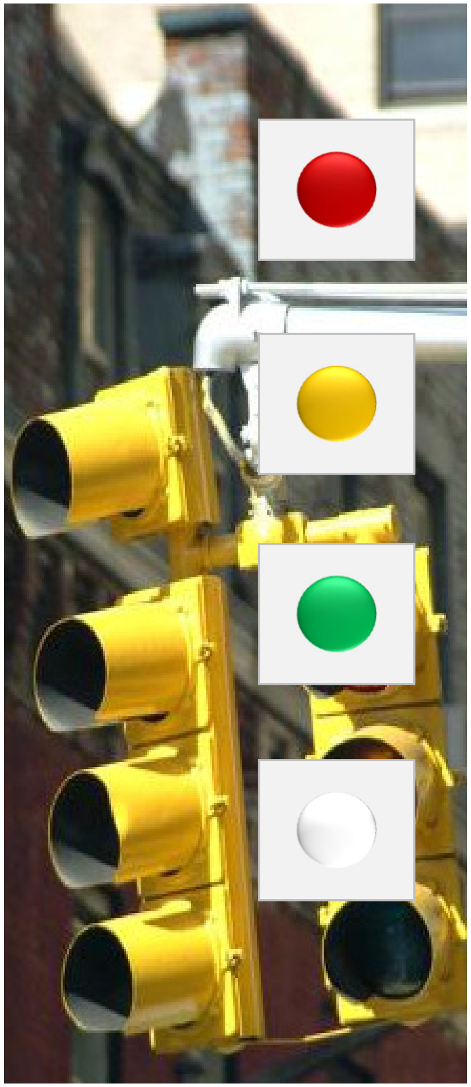
Ongoing Engagement

- Bi-weekly Threat Calls
- Emergency Member Calls
- Semi-Annual Member Meetings and Conferences
- Regional Outreach Program
- Bi-Weekly Educational Webinars

Readiness Exercises

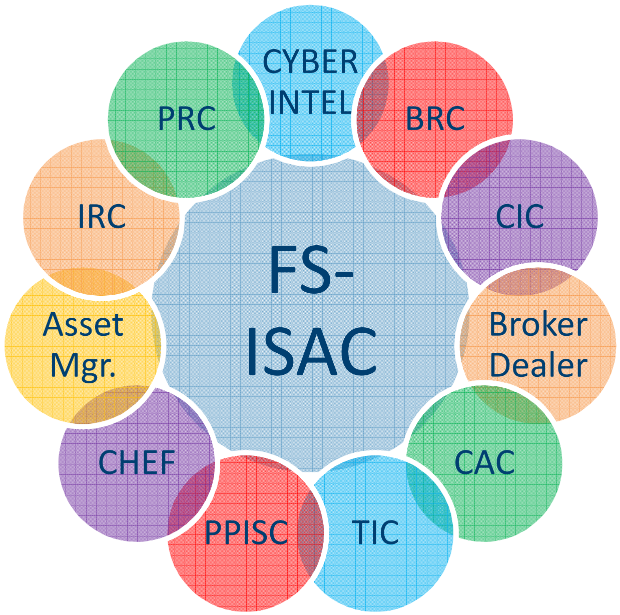
- Government Sponsored Exercises
- Cyber Attack against Payment Processes (CAPP) Exercise
- Advanced Threat/DDoS Exercise
- Industry exercises-Systemic Threat, Quantum Dawn Two, etc.

Information Sharing: Traffic Light Protocol

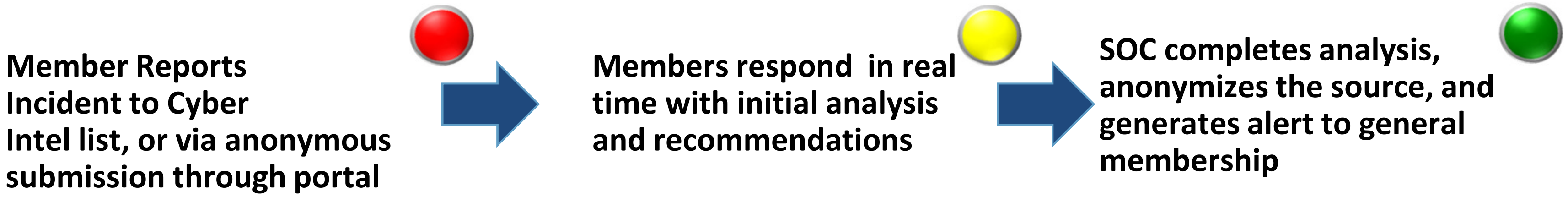


- Restricted to a defined group (e.g., only those present in a meeting.) Information labeled RED should not be shared with anyone outside of the group
- This information may be shared with FS-ISAC members.
- Information may be shared with FS-ISAC members and partners (e.g., vendors, MSSPs, customers). Information in this category is not to be shared in public forums
- This information may be shared freely and is subject to standard copyright rules

FS-ISAC Circles of Trust



- Clearing House and Exchange Forum (CHEF)
- Payments Risk Council (PRC)
- Payments Processor Information Sharing Council (PPISC)
- Business Resilience Committee (BRC)
- Threat Intelligence Committee (TIC)
- Community Institution Council (CIC)
- Insurance Risk Council (IRC)
- Compliance and Audit Council (CAC)
- **Cyber Intelligence Listserv**
- **Asset Manager Council**
- **Broker-Dealer Council**



Member Reports Incident to Cyber Intel list, or via anonymous submission through portal

Members respond in real time with initial analysis and recommendations

SOC completes analysis, anonymizes the source, and generates alert to general membership

FINANCIAL SERVICES ISAC

Types of Information Shared

Cyber Threats, Vulnerabilities, Incidents

- ✓ Malicious Sites
- ✓ Threat Actors, Objectives
- ✓ Threat Indicators
- ✓ Tactics, Techniques, Procedures
- ✓ Courses of Action
- ✓ Exploit Targets
- ✓ Denial of Service Attacks
- ✓ Malicious Emails: Phishing/Spearphishing
- ✓ Software Vulnerabilities
- ✓ Malicious Software
- ✓ Analysis and risk mitigation
- ✓ Incident response

Physical Threats, Incidents

- ✓ Terrorism
- ✓ Active Shooter
- ✓ Hurricanes
- ✓ Earthquakes
- ✓ Other meteorological events
- ✓ Geopolitical impacts
- ✓ Pandemic
- ✓ Type, location, severity
- ✓ Impact analysis and risk mitigation
- ✓ Business resilience preparation and incident response

FINANCIAL SERVICES ISAC

Security Automation

Will Revolutionize Information Sharing

SOLTRA

Soltra Edge

OPEN CYBER INTELLIGENCE PLATFORM

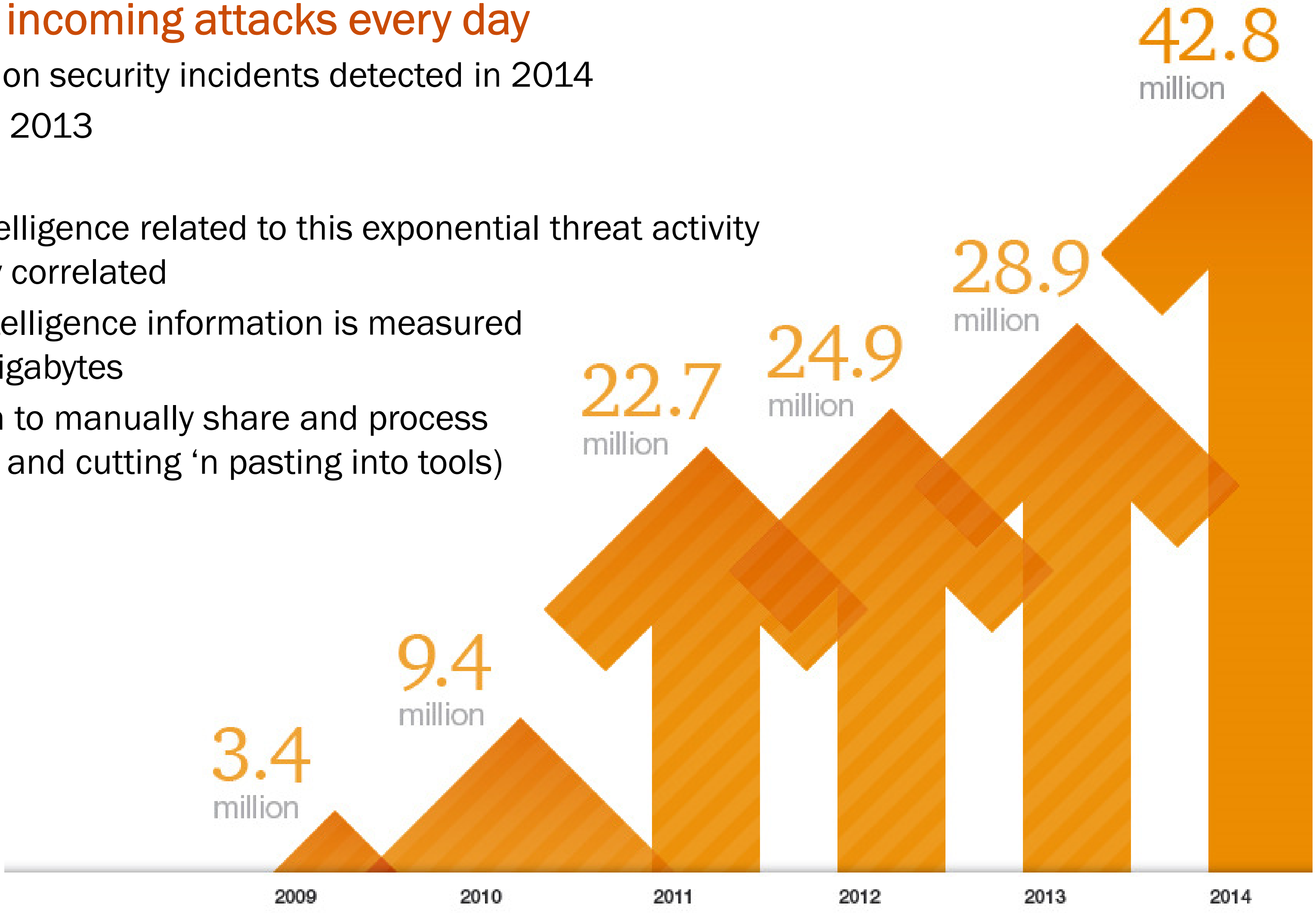
www.soltra.com

THREATS (& INTELLIGENCE) GROWING FAST

117,339 incoming attacks every day

- 42.8 million security incidents detected in 2014
- 48% over 2013

- Cyber Intelligence related to this exponential threat activity is directly correlated
- Today, intelligence information is measured daily in Gigabytes
- Too much to manually share and process (emailing and cutting 'n pasting into tools)



Findings from The Global State of Information Security Survey 2015 Graphic Source: PwC

THE NEED FOR SPEED

Attackers Act 150x Faster Than Victims Respond

- Minutes vs. Weeks/ Months

Attackers have honed their skills to come at you rapidly

Defenders take a long time to feel the impact of an attack

	Seconds	Minutes	Hours	Days	Weeks	Months
Initial Attack to Initial Compromise (Shorter Time Worse)	10%	75%	12%	2%	0%	1%
Initial Compromise to Data Exfiltration (Shorter Time Worse)	8%	38%	14%	25%	8%	8%
Initial Compromise to Discovery (Longer Time Worse)	0%	0%	2%	13%	29%	54%

MACHINES CAN HELP, BUT FIRST…

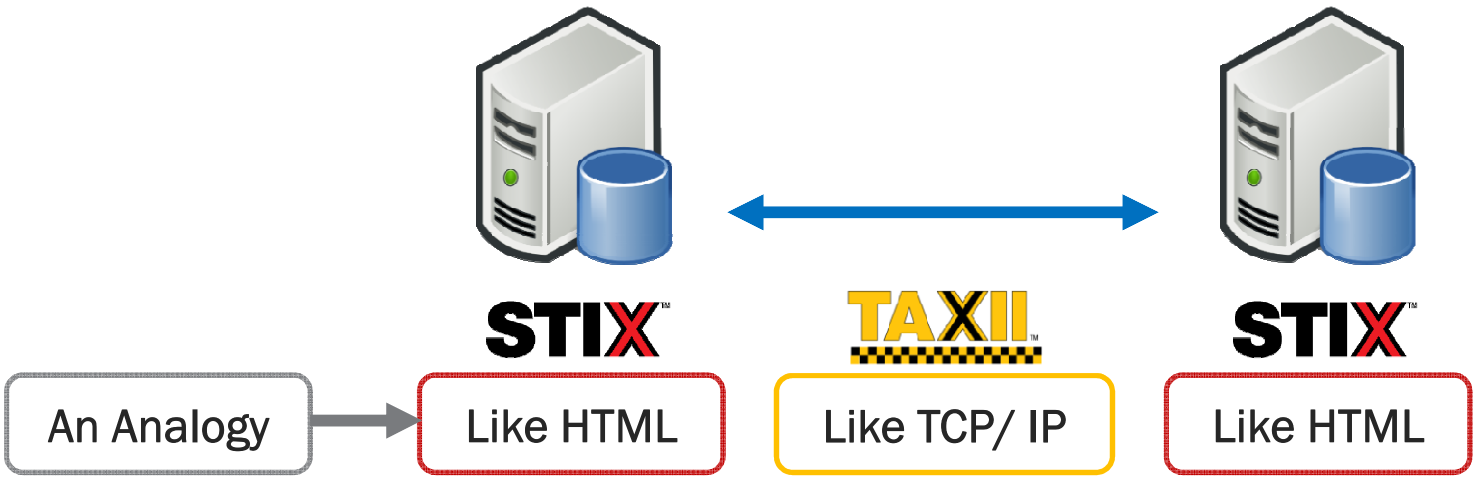
…Machines Need a Language to Talk about Threats

STIX™ - Structured Threat Intelligence eXpression

- Structured language used by machines to describe cyber threats

TAXII™ – Trusted Automated eXchange of Indicator Information

- Transport mechanism for cyber threat information represented in STIX



STIX™

TAXII™

STIX™

An Analogy

Like HTML

Like TCP/ IP

Like HTML

STIX CONSTRUCTS

An open standard to categorize cyber threat intelligence information

Atomic

Observable

What threat activity are we seeing?

Tactical

Indicator

What threats should I look for on my networks and systems and why?

Operational

Incident

Where has this threat been seen?

Course of Action

What can I do about it?

ExploitTarget

What weaknesses does this threat exploit?

Strategic

ThreatActor

Who is responsible for this threat?

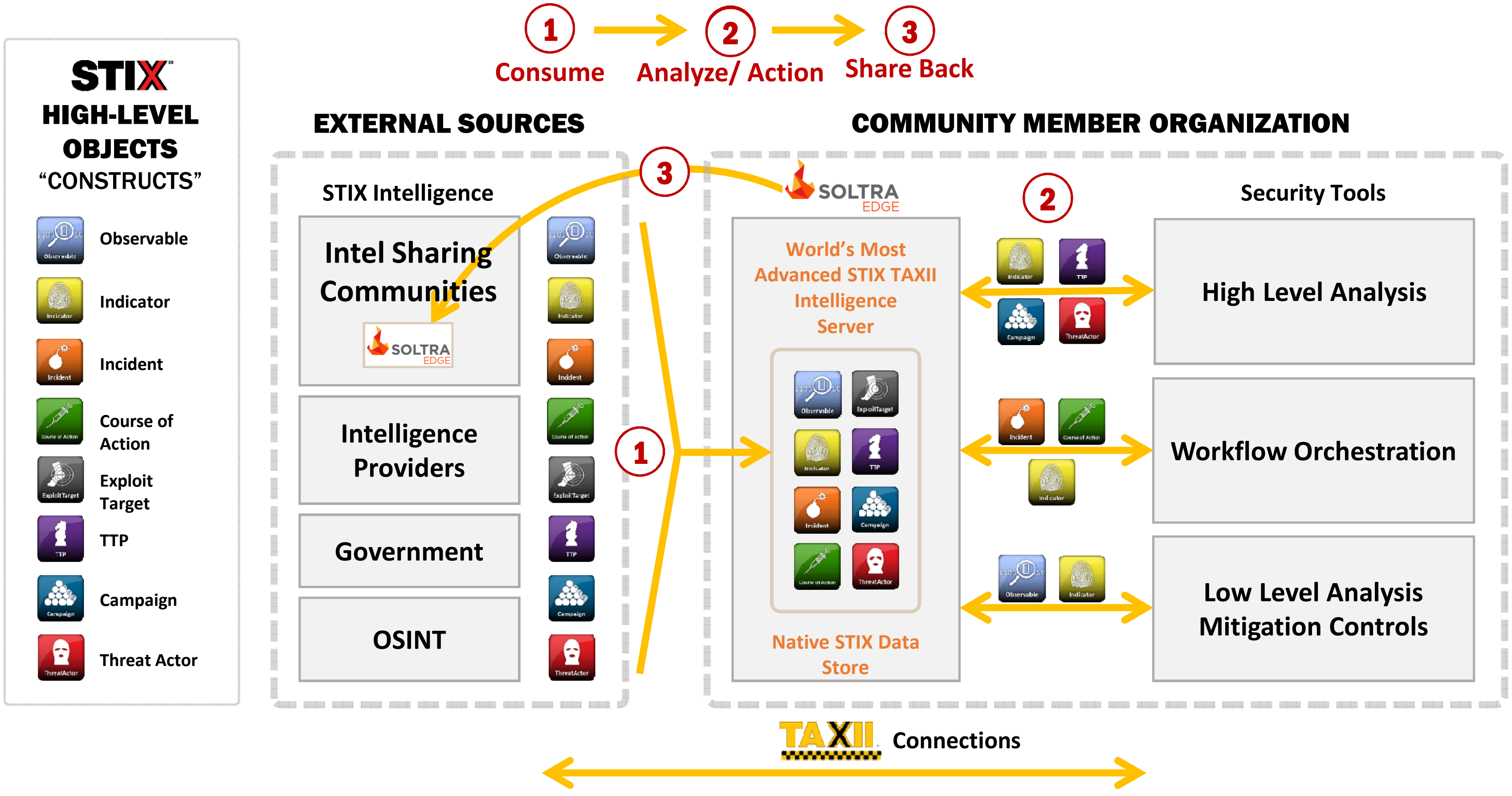
Campaign

Why do they do this?

TTP

What do they do?

OPEN INTELLIGENCE WORKFLOW



STIX™ HIGH-LEVEL OBJECTS "CONSTRUCTS"

- Observable
- Indicator
- Incident
- Course of Action
- Exploit Target
- TTP
- Campaign
- Threat Actor

1 Consume → 2 Analyze/ Action → 3 Share Back

EXTERNAL SOURCES

STIX Intelligence

- Intel Sharing Communities (SOLTRA EDGE)
- Intelligence Providers
- Government
- OSINT

COMMUNITY MEMBER ORGANIZATION

SOLTRA EDGE

World's Most Advanced STIX TAXII Intelligence Server

Native STIX Data Store

Security Tools

- High Level Analysis
- Workflow Orchestration
- Low Level Analysis Mitigation Controls

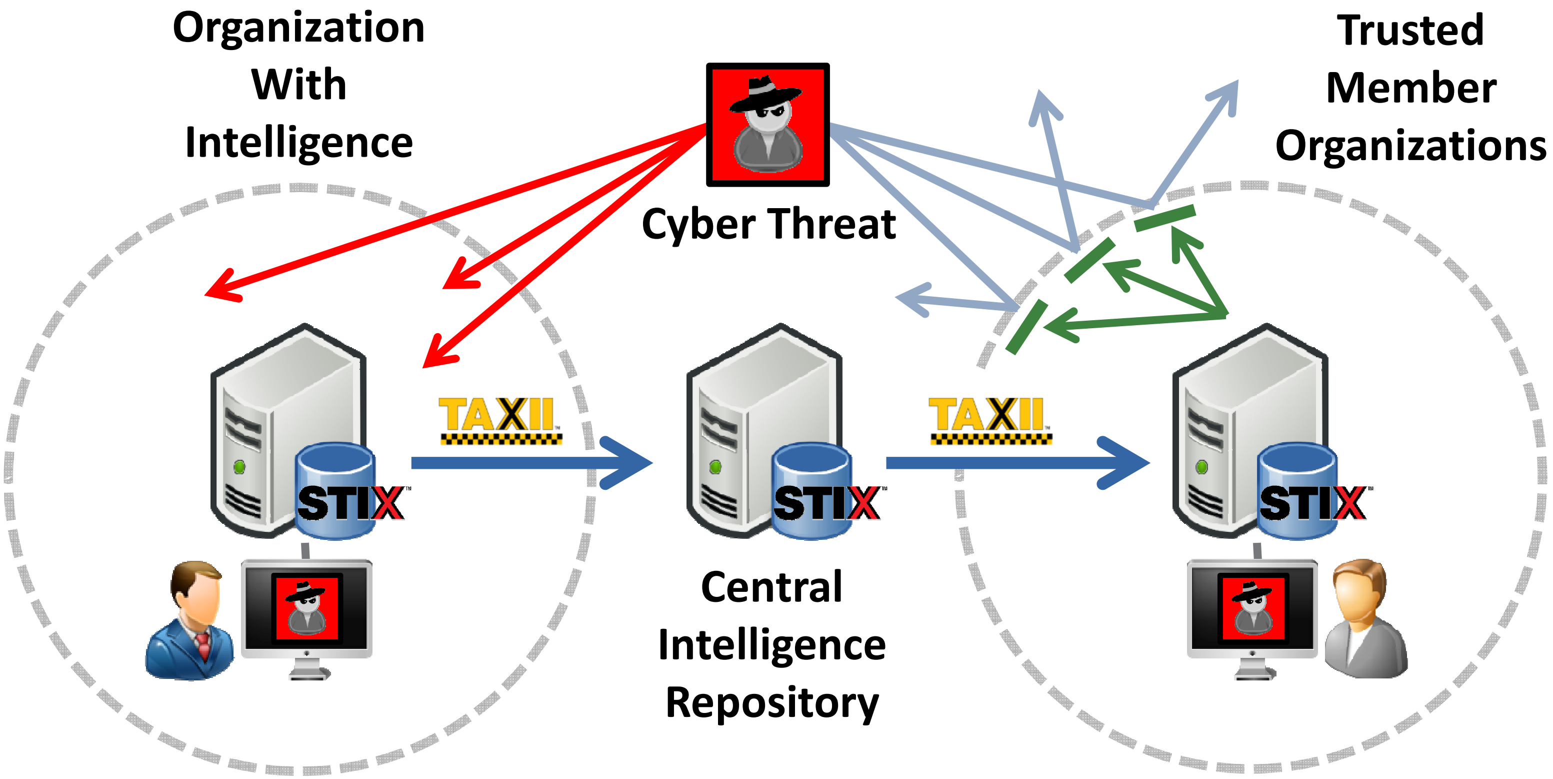
TAXII Connections

FINANCIAL SERVICES | ISAC

INTELLIGENCE-DRIVEN COMMUNITY DEFENSE

Maturing An Intelligence Ecosystem

- Standards-based Machine Speed Communication
- End-to-End (Sensor to Control) Community Defense Model



Organization With Intelligence
Cyber Threat
Trusted Member Organizations
TAXII
TAXII
STIX
STIX
STIX
Central Intelligence Repository

SECURITY AUTOMATION STATUS

- **Soltra– joint venture between FS-ISAC and DTCC**
  - Industry-owned utility to automate threat intelligence sharing
  - DTCC IT & scalability; FS-ISAC community & best practices
  - Funded by the industry, including SIFMA and some of its largest members
  - At-cost model; open standards (STIX, TAXII)
  - Provide platform that can be extended to all sizes of financial services firms, other ISACs and industries
  - Integrate with vendor solutions (firewalls, intrusion detection, anti-virus, threat intelligence, etc.)

- **Soltra Edge**
  - General availability 12/3/2014
  - FS-ISAC instance, January 2015
  - Over 900 downloads of Soltra Edge, less than half from financial services sector
  - Adapter and Network capabilities-- 2015

SOLTRA

FINANCIAL SERVICES ISAC

Information Sharing

One Firm’s Incident becomes the Entire Community’s Response

Trustwave's List of 7 Deadly Employee Sins

1) **Pathetic Passwords**: The most common corporate password is "Password1" because it meets the minimum complexity requirements. 15% of physical security tests, written passwords were found on and around user workstations.
2) **Peeping ROM**: 71% of workers sneak a peek at a co-workers or stranger's workstation. One in three workers leaves their computers logged on when they are away from their desk.
3) **USB Stick Up**: 60% of users who find random USB sticks in a parking lot will plug them into their computers; add those sticks that includes a company logo and the number increases to 90%.
4) **Phish Biting**: 69% of phishing messages past spam filters; 27% of IT organizations have users who have fallen for malicious e-mail attacks.
5) **Reckless Abandon**: 70% of users do not password-protect their smartphones, and 89% of people who find lost cell phones rummage through the digital contents.
6) **Hooking up with Another Man's WiFi**: By 2015, the number of WiFi hotspot deployments will increase 350%, but currently, only 18% of users use a VPN tool when accessing public WiFi
7) **A Little Too Social**: 67% of young workers think corporate social media policies are outdated, and 70% regularly ignore IT policies. Just over half (52%) of enterprises have seen an increase of malware infections due to employees' use of social media

Contact Information

Bill Nelson, President & CEO	bnelson@fsisac.us
Eric Guerrino, EVP Operations	eguerrino@fsisac.us
Peter Falco, Broker Dealer Services	pfalco@fsisac.us
Robin Fantin, VP Marketing	rfantin@fsisac.us
Beth Hubbard, Director of Member Services	bhubbard@fsisac.us

www.fsisac.com

FINANCIAL SERVICES ISAC

Thank You for Your Time Today

Financial Services
Information Sharing & Analysis Center

Q&A

- Please use the “chat” function on your webinar control panel to ask a question to the moderator or speakers.
- If you have additional questions following the conclusion of the webinar, please contact:
  - Barbara Wierzynski, FIA (bwierzynski@fia.org)
    - All content related questions
  - Mary Freeman, FIA (mfreeman@fia.org)
    - All logistical questions pertaining to access of the webinar, webinar recording, and slide deck.
- The recorded webinar will be available on the FIA website within 24 hours following the conclusion of the webinar.