Financial Services Information Sharing & Analysis Center (FS-ISAC) Overview

FIRST Annual General Meeting

June, 2012

Kevin Thomsen

Citi

FINANCIAL SERVICES ISAC

Sharing Critical, Specific, Meaningful, Accurate, Reliable and Timely Information

Agenda

- FS-ISAC Background
- FS-ISAC Benefits
- Member Benefits
- Features
- Account Takeover in the U.S.
- Microsoft/FS-ISAC Civil Litigation

FS-ISAC Background

The Financial Services Information Sharing and Analysis Center was formed in 1999 and is:

- A nonprofit private sector initiative
- Designed/developed/owned by financial services industry: Banks, Card companies, Payment and Clearing Processors, Brokerage Firms, Insurance companies, Associations
- 2012 Membership criteria change

Goal: share timely, relevant and actionable information and analysis of physical and cyber security information

FS-ISAC Membership

- Before 2012, FS-ISAC members had to have a U.S. presence.
- In 2012, FS-ISAC Board of Directors changed the Operating Rules to allow for Fis to join that do not have a U.S. presence
- Goal: Ability to exchange intelligence and collaborate globally
- Trial Memberships Available

FS-ISAC Benefits

- Dissemination of timely, relevant, and **actionable** information between members, with government agencies and other sectors.
- Find out about a specific threat or incident **as it unfolds: learn** what others are doing tactically to combat this threat along with mitigation strategies.
- Engage CISOs/Heads of IT Risk and security operations and incident response teams along with fraud investigations, business continuity, disaster response physical security, payments risk professionals.
- Facilitates the development of professional and trusted relationships among peers and subject matter experts to protect member firms

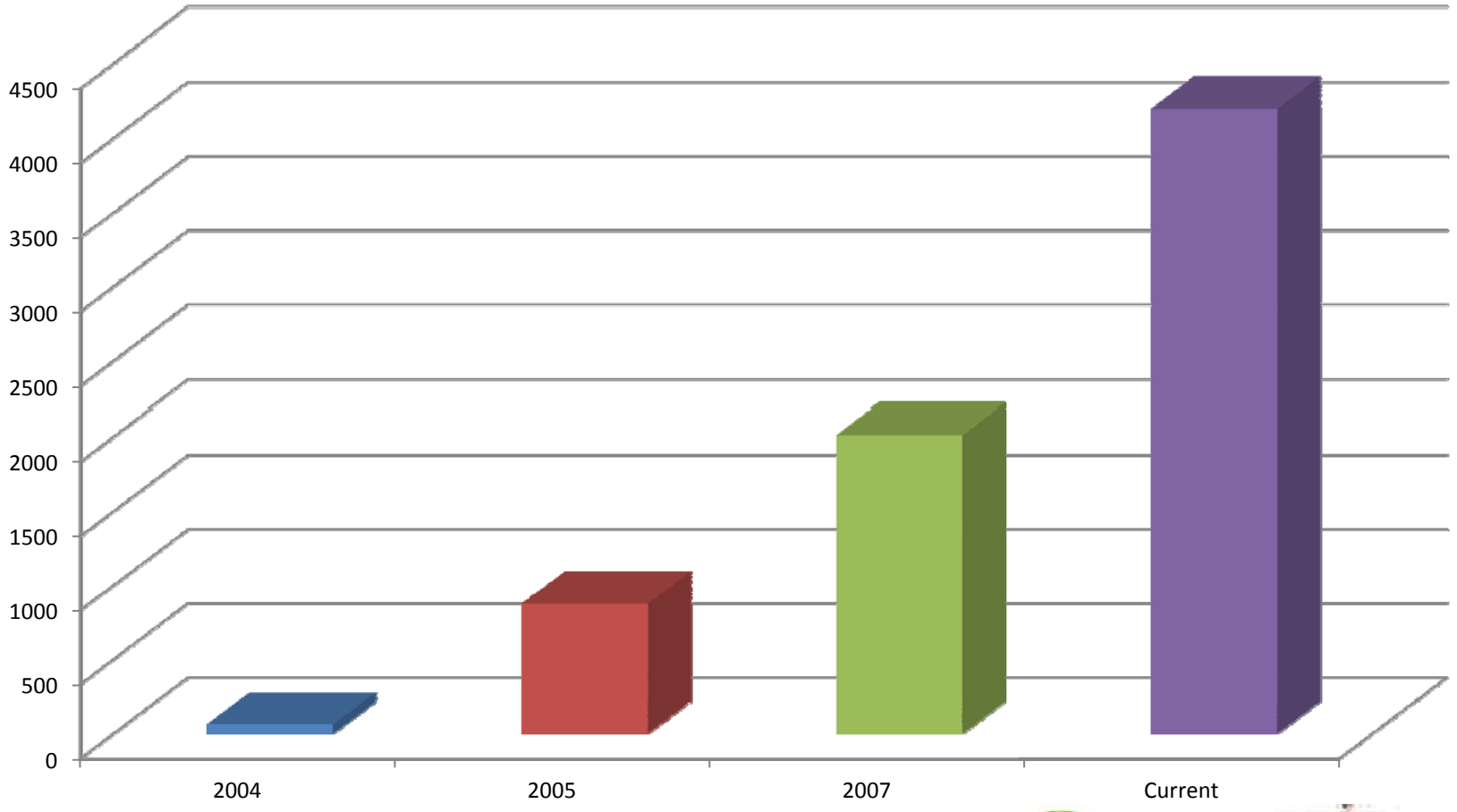
5

Member Benefits

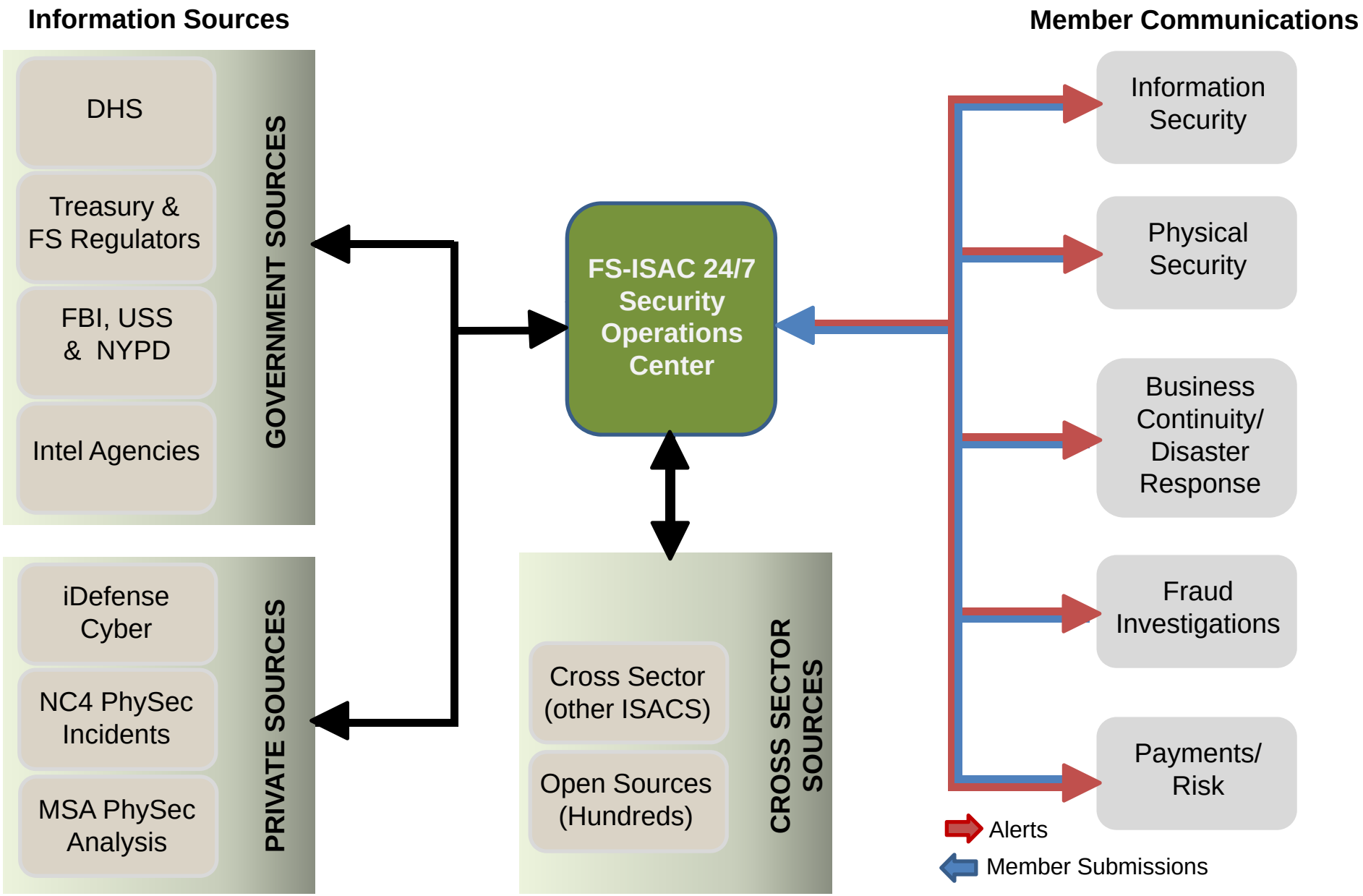
- Learn about the latest threats and vulnerabilities instantly
- Obtain more details about a specific attack
- Find out what others are doing and mitigation strategies in regards to a specific threat
- Learn about the latest trends and technologies
- Protect and secure their enterprise data
- Prevent and respond to customer threats
- Educate their staff

6

FS-ISAC Membership Growth



FS-ISAC 24/7 Security Operations Center



FS-ISAC Information Sharing and Analysis Tools

Phone/in-person

- ✓ Bi-weekly Threat calls
- ✓ **Emergency member calls**
- ✓ Semi-annual conferences
- ✓ Regional Outreach Program
- ✓ **Payments Risk Council**
- ✓ Card Payment Processors
- ✓ **Compliance Audit Council**

Exercises

- ✓ Financial Services sector exercises
- ✓ **Cyber Attack against Payment Processes (CAPP Exercise)**
- ✓ Government exercises

Information Sharing

- ✓ **Relevant/actionable cyber& physical alerts**
- ✓ Member contact directory
- ✓ **Risk Mitigation Toolkits**
- ✓ Document Repository
- ✓ **Anonymous Submissions**
- ✓ Threat Intelligence listserv
- ✓ **Member surveys**
- ✓ Government sharing (DHS, US CERT, FBI, Treasury, USSS)
- ✓ Cross-Sector (Telecommunications, IT, Electricity, etc.)

Analysis and Collaboration

FINANCIAL SERVICES ISAC

Sharing Critical, Specific, Meaningful, Accurate, Reliable and Timely Information

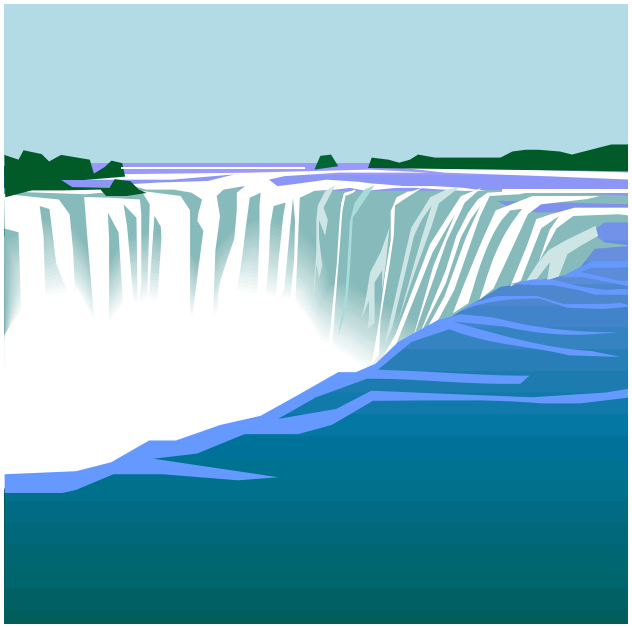
FS-ISAC Traffic Light Protocol (TLP)

Classification	Target Audience
+ **FS-ISAC Red**	+ **Restricted to a defined group (e.g., only those present in a meeting or recipient of defined group.) Information labeled RED should not be shared with anyone outside of the group.**
+ **FS-ISAC Amber**	+ **This information may be shared with FS-ISAC members. Generally, alerts with the FS-ISAC Yellow classification will be kept behind the FS-ISAC secure portal.**
+ **FS-ISAC Green**	+ **Information within this category may be shared with FS-ISAC members and partners (e.g., DHS, Treasury and other government agencies and ISACs). Information in this category is not to be shared in public forums**
+ **FS-ISAC White**	+ **This information may be shared freely and is subject to standard copyright rules**

Information Sharing:
Moving from a Drip to a Torrent

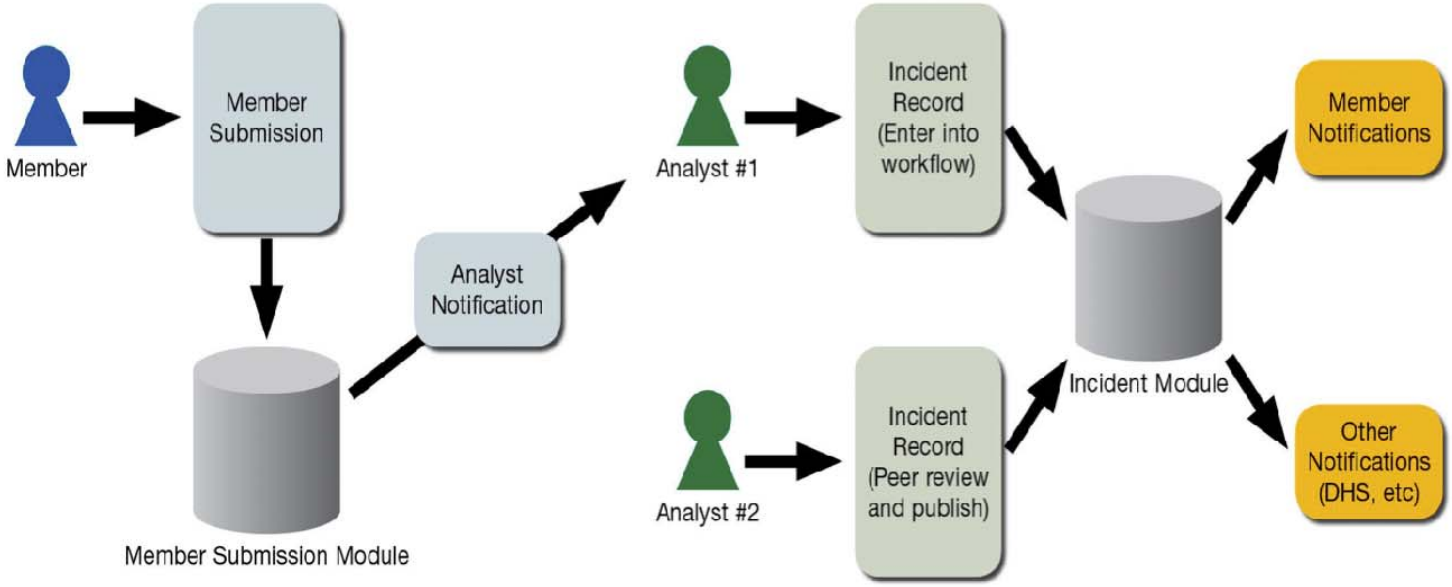
Before TLP

After TLP



Member Submissions

Anonymous or Attributed
Submission Types: Cyber Incident, Physical Incident or Document Upload



FS-ISAC Groups

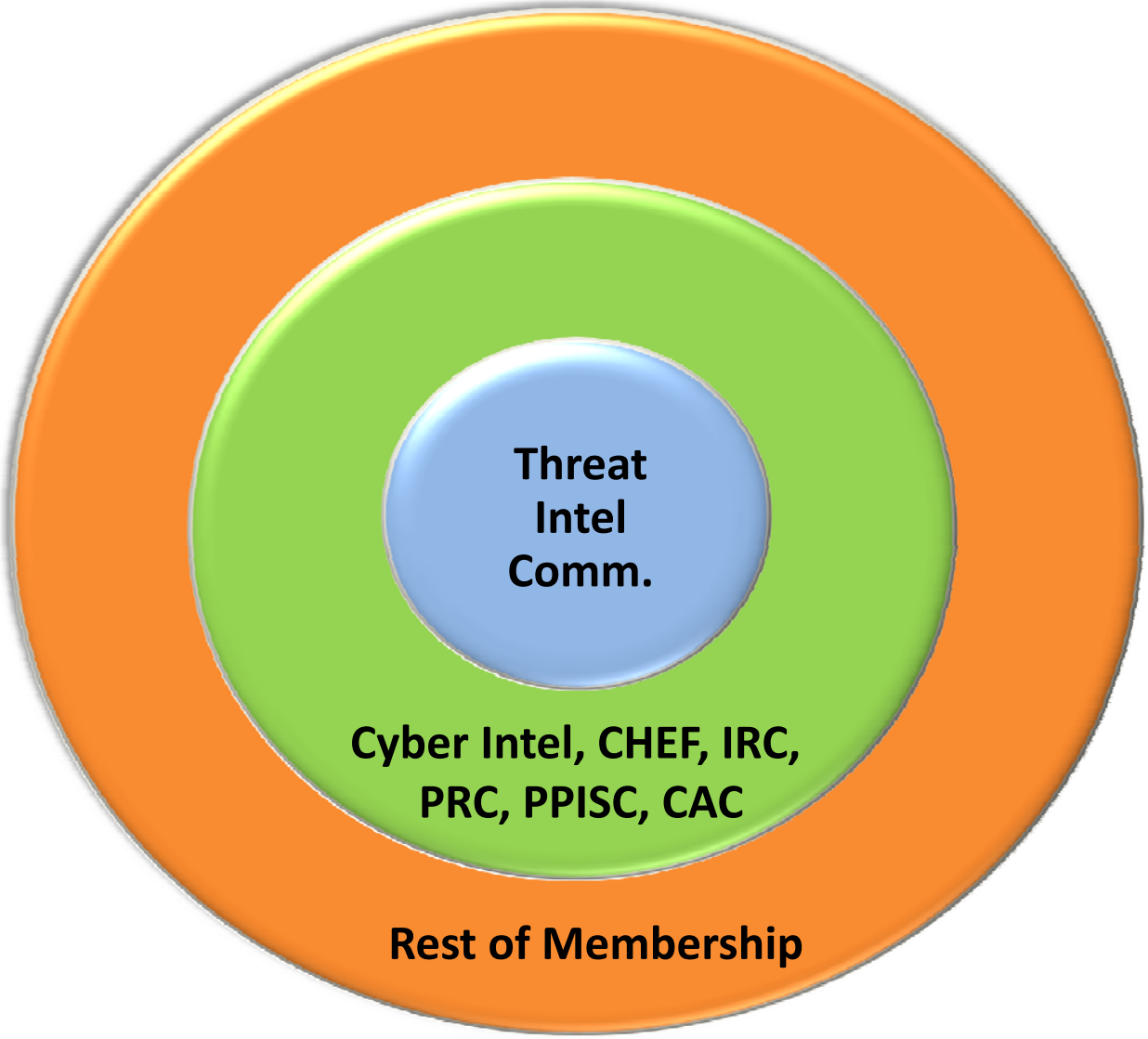
Active Online Special Interest Groups

- ✓ Threat Intelligence Committee (TIC)
- ✓ Cyber Intelligence List– Open to all members
- ✓ Payments Risk Council (PRC)
- ✓ Clearing House and Exchange Forum (CHEF)
- ✓ Payments Processor Information Sharing Council (PPISC)
- ✓ Compliance Audit Council (CAC)
- ✓ Insurance Risk Council (IRC)

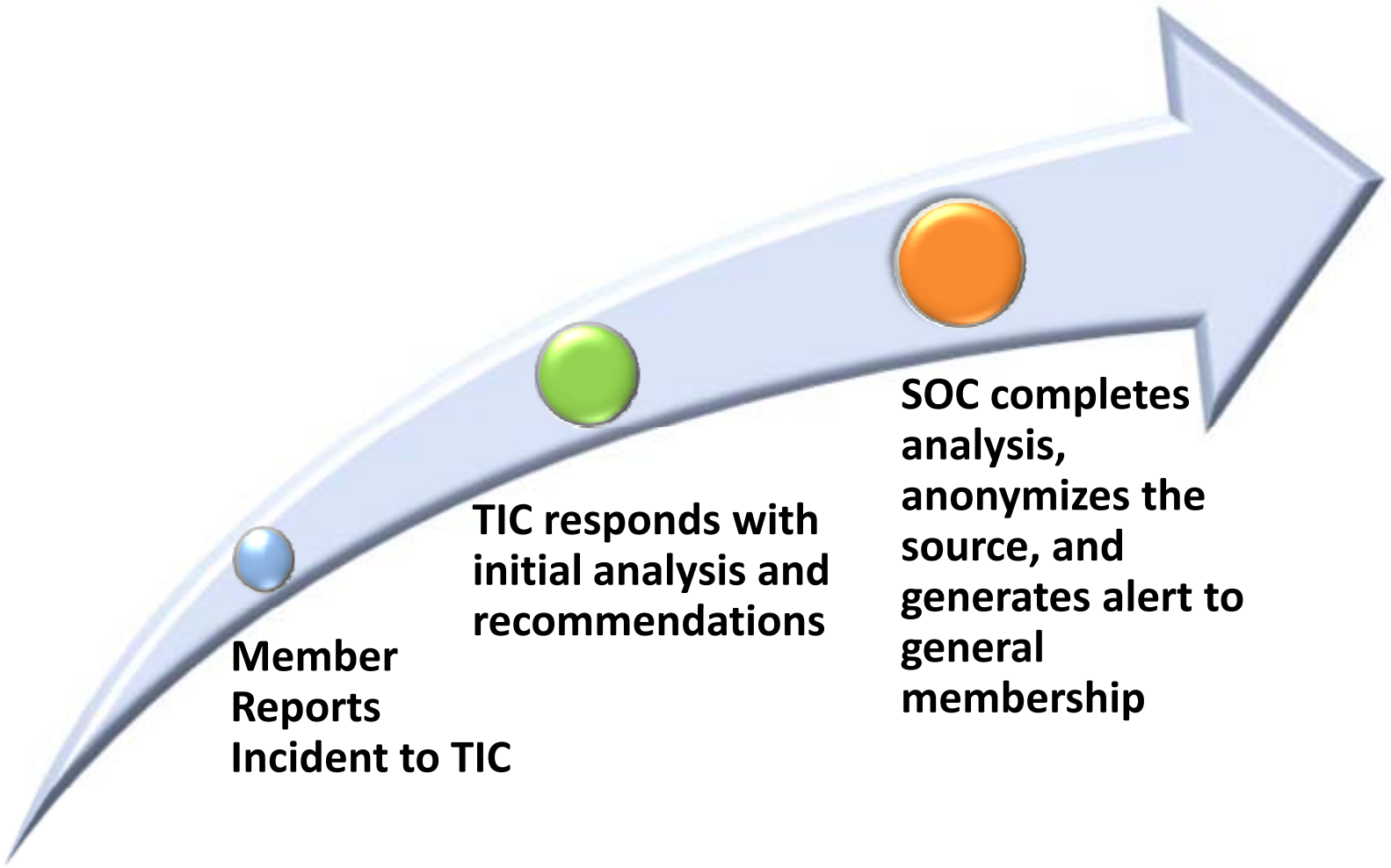
Committees and Task Forces

- ✓ Education Committee
- ✓ Product and Services Committee
- ✓ Business Resilience Committee
- ✓ Survey Review Committee

Circles of Trust



Typical Process Utilizing Circles of Trust

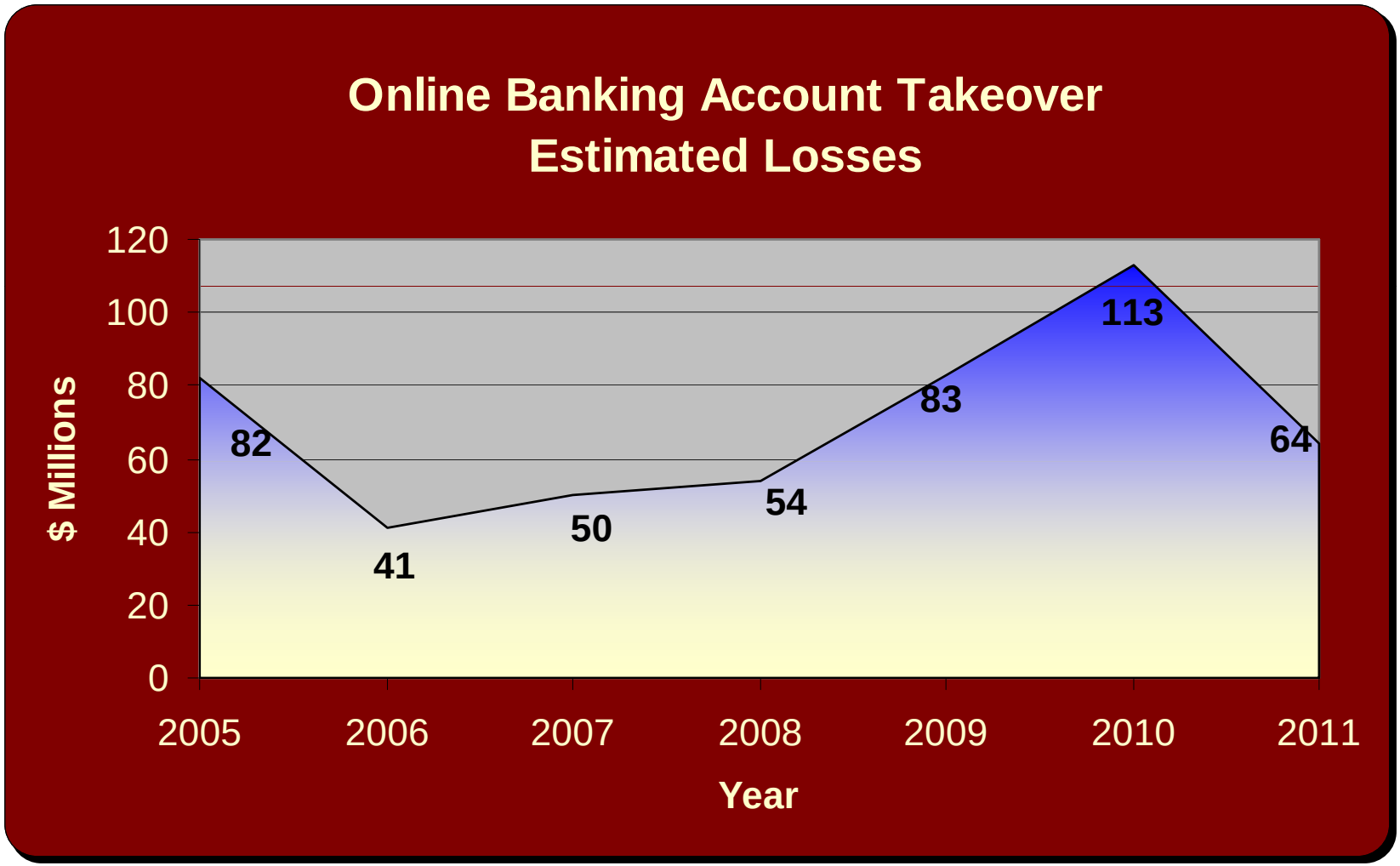


Account Takeover Attacks

FINANCIAL SERVICES ISAC

Sharing Critical, Specific, Meaningful, Accurate, Reliable and Timely Information

Downward Trend During 2011



Source: FDIC

Evolution of Attack and Response: August 2009 Business Account Takeover

- NACHA asked to participate in release of joint FBI/FS-ISAC bulletin
- GREEN and YELLOW bulletins released with detailed risk mitigation recommendations

FS-ISAC YELLOW: The contents of this alert are sensitive, and intended only for the recipients and other FS-ISAC members with a need-to-know.

Corporate Account Takeover Impacts Payment Systems
21 August 2009

This product was created as part of a joint effort between the Federal Bureau of Investigation, the Financial Services Information Sharing and Analysis Center (FS-ISAC) and NACHA - the Electronic Payments Association, in coordination with the U.S. Department of Treasury.

Background

Within the last six months, the FBI has seen a significant increase in fraud involving the exploitation of valid online banking credentials belonging to small and medium sized businesses. In a typical scenario, the attack vector is a "spear phishing"[a] e-mail which contains either an

FS-ISAC, NACHA, FBI Risk Mitigation Recommendations for Business Users

1. Initiate ACH and wire transfer payments under dual control
2. **Online commercial banking customers execute all online banking activities from a dedicated, stand-alone, and completely locked down computer system from where email and web browsing are not possible.**
3. Limiting administrative rights on users' workstations to prevent inadvertent downloading of malware
4. Reconcile all banking transactions on a daily basis.
5. Financial institutions should also implement an awareness communications program to advise customers of current threats and fraud activities

FBI, NACHA, FS-ISAC Recommendations

6. **FIs implement appropriate fraud detection best practices including transaction risk profiling and behavior monitoring**
7. FIs consider using manual or automated Out-Of-Band authentication systems in concert with fraud detection systems.
8. Such OOB solutions many include manual client callback or automated solutions SMS text messaging, Interactive Voice Response system callback to a known phone number with a PIN code and similar solutions.

Fourteen additional in-depth defenses including, …

Additional 14 in-depth recommendations

1. Perimeter router blocking of all unnecessary ports
2. Intrusion Prevention Systems at perimeter and internal network
3. Firewalls with a default deny configuration
4. Layered anti-virus systems with different vendors at key access points and services
5. Web proxy systems with automated malicious site blocking and outgoing activity analysis
6. Perimeter SPAM and malicious content filtering
7. Least Privilege Doctrine for all users to prevent unauthorized software installation and assist in blocking malicious code installation
8. Vulnerability scanning program with patch and mitigation service levels defined
9. Comprehensive patch mgmt program that patches critical and high risk vulnerabilities within a short period of time.
10. Web and email surveillance tools to identify information leakage and compromise.
11. Security Incident Mgmt capability to correlate events
12. **Subscribe to appropriate threat intelligence and information sharing services**
13. Prepare and implement an Incident Response plan
14. Develop a relationship with your local FBI and USSS Field Offices

Microsoft, FS-ISAC,NACHA Civil Litigation against ZeuS botnet infrastructure March 2012

FINANCIAL SERVICES ISAC

Sharing Critical, Specific, Meaningful, Accurate, Reliable and Timely Information

Operation b71

- Building on the successes of its previous botnet takedowns, Microsoft partnered with the financial services sector to execute a coordinated global takedown operation against the ZeuS, SpyEye and Ice IX botnets
- The takedown was accomplished through legal and technical action and disrupted ZeuS, SpyEye and Ice IX botnets, striking a major blow against cybercriminal operations
  - Plaintiffs include Microsoft, FS-ISAC and NACHA
- ZeuS, SpyEye and Ice IX malware infects victims' computers, stealing PII and account login credentials, and are responsible for the vast majority of electronic Account Takeovers

Operation b71

- March 19, 2012– Microsoft, FS-ISAC and NACHA obtained a restraining order from U.S. District Court for the Eastern District of NY
- The order allowed Microsoft and its partners to sever the command and control structures of the Zeus, SpyEye and Ice IX malware
- March 23, 2012-- Microsoft and its co-plaintiffs, escorted by the U.S. Marshals, executed a coordinated physical seizure of command and control servers in multiple hosting locations in the US and separate action in the UK, to preserve evidence for this case

Operation b71

- Firsts—
  - This is the first time FS organizations have joined Microsoft as plaintiffs in the legal case for a botnet takedown
  - First time a well-established law known as the Racketeer Influenced and Corrupt Organizations (RICO) Act has been used as the legal hook to disrupt a botnet
  - This is also the first operation for Microsoft that involved the simultaneous takedown of multiple operating botnets in a single action

Operation b71

- The takedown will disrupt, but is not expected to completely eliminate the ZeuS, SpyEye and Ice IX botnets
- Microsoft working with law enforcement to begin actions against the criminals responsible for creating, selling and using the ZeuS, SpyEye and Ice IX botnets to perpetrate fraud
- Operation b71 will help diminish the threat these botnets pose by reducing the size of each botnet through international cleanup efforts
- Microsoft will use the intelligence gained from this takedown to partner with ISPs and others around the world to help clean computers infected with ZeuS, SpyEye and Ice IX

Top ten ZeuS hosting ISPs (by number of ZeuS C&Cs)

ZeuS C&C count	AS number	AS name
182	8069	MICROSOFT-CORP---MSN-AS-BLOCK - Mic
28	3598	MICROSOFT-CORP-AS - Microsoft Corp
14	25532	MASTERHOST-AS CJSC _MasterHost_
11	14618	AMAZON-AES - Amazon.com, Inc.
9	3595	GNAXNET-AS - Global Net Access, LLC
8	21844	THEPLANET-AS - ThePlanet.com Intern
7	21788	Network Operations Center Inc.
6	24940	HETZNER-AS Hetzner Online AG RZ
6	29873	BIZLAND-SD - The Endurance Internat
6	35415	WEBAZILLA WebaZilla European Networ

As of 3/26/2012, 4:35 pm EDT

210 of 809 (26%)

MS Civil Litigation Results

- Symantec reported on 4/30/2012 that MS's civil action and takedown of the Rustock botnet resulted in elimination of 20 billion spammed email PER DAY
  - 2010– spam represented 88% of all email
  - 2011– spam represented 75% of all email
- Before 3/23/2012, NACHA reported average volume of spoofed NACHA email messages with malware links averaged 11 million per week. After the MS action, the average was less than 1 million per week.

New Paradigm in the Fight Against Cyber Crime

<u>Criminal Action Only</u>:

Continue to let criminals steal from customers while LE builds comprehensive cases against Eastern Europeans which are

1. difficult to prosecute,

2. obtain meaningful convictions, and

3. take months or years of investigation

<u>Civil and Criminal Action</u>:

Disrupt criminals' operations through civil action that

1. identifies the defendants quickly,
2. notifies the customers re: infected machines,
3. provides remediation tools and,
4. still allows for prosecution of defendants through criminal action.

MS Civil Litigation Next Steps

- Examination of all evidence collected
- June 29 Court appearance–
  - Dismiss defendants identified as “researchers”
  - Name specific defendants (2 currently in jail in the UK)
  - Share info about defendants with LE before they are identified
- Compile all information and evidence collected from the complaint and from MS Hotmail sources and turn over to FBI

QUESTIONS?

FINANCIAL SERVICES ISAC

Sharing Critical, Specific, Meaningful, Accurate, Reliable and Timely Information

Contact Information:

FS-ISAC
Bill Nelson
bnelson@fsisac.us
703-777-2803

Citi
Kevin Thomsen
kevin.thomsen@citi.com
212-657-2076

www.fsisac.com

Sharing Critical, Specific, Meaningful, Accurate, Reliable and Timely Information