Cyber Attack against Payment Processes (CAPP) Exercise *Preliminary Results*

May 11, 2010

Dennis Simmons
President & CEO
SWACHA

FINANCIAL SERVICES ISAC

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

Agenda

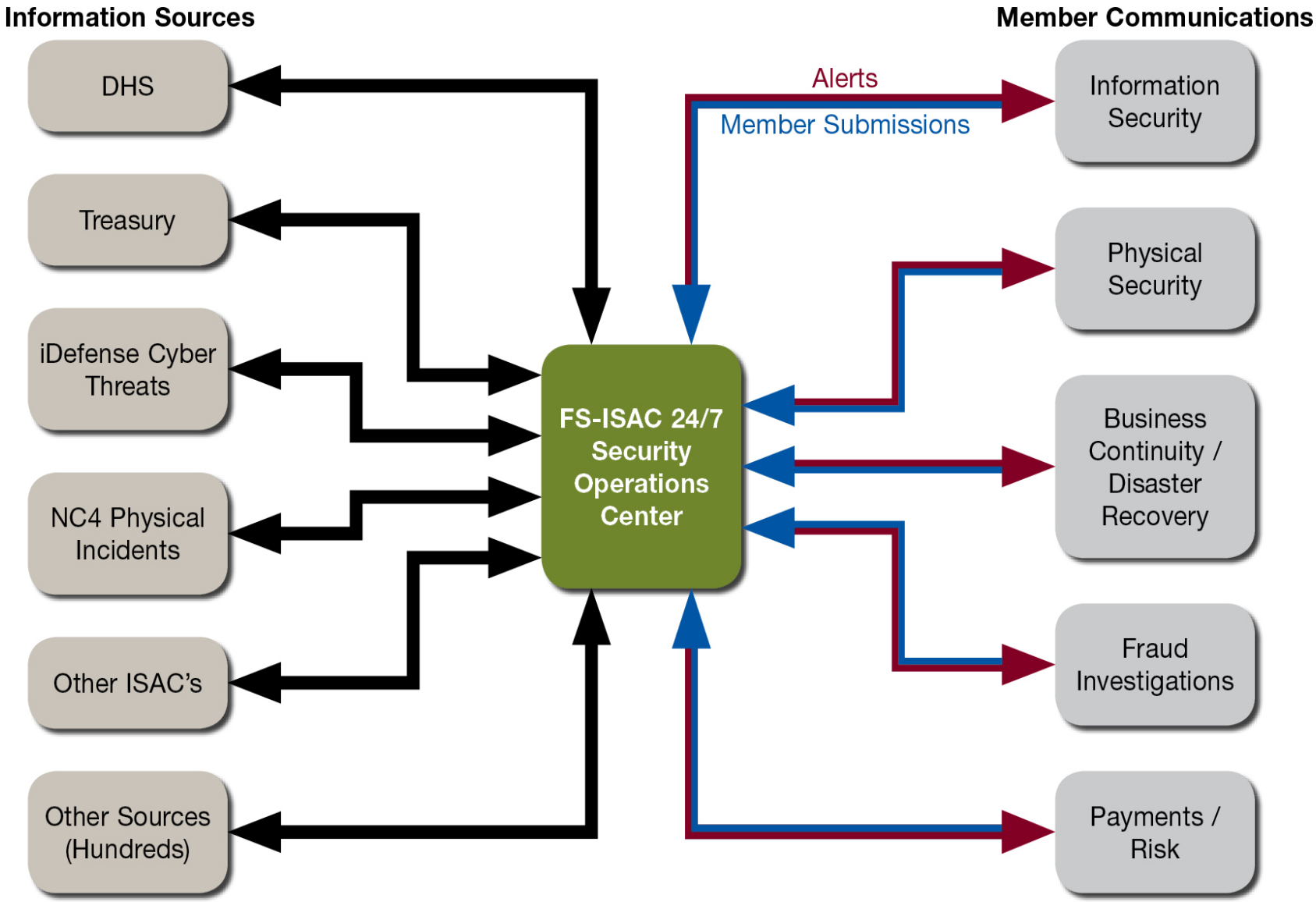
- FS-ISAC Background
- CAPP Exercise Objectives
- Conclusions & Recommendations

FS-ISAC Background and Goal

The Financial Services Information Sharing and Analysis Center is:

- A nonprofit private sector initiative
- Designed/developed/owned by financial services industry
- Lead agency: U.S. Treasury
- Goal: Provide a single source for sharing physical and cyber security information

FS-ISAC 24/7 Security Operations Center



CAPP Exercise
February 9-11, 2010

FINANCIAL SERVICES ISAC

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

Cyber Attack against Payment Processes (CAPP) Exercise, February 9-11, 2010

1. Test the ability of stakeholders to respond to major cyber attacks against payment systems
2. Raise awareness and educate financial services firms regarding cyber threats
3. Make recommendations for improvements to cyber incident response procedures
4. Evaluate and develop appropriate risk mitigation recommendations
5. Engage participants going forward on the need to share threat, vulnerability and incident information
6. Develop an after action report that can be used for workshops, webinars and ongoing education

CAPP Exercise Overview

- Planning Committee: IT security, ACH payments, card, treasury management professionals
- Attack vectors used in the exercise:
  - SQL injection in databases of electronic check conversion/remote capture vendors
  - DDoS attacks
  - Spear phishing/Zeus Trojan attack against business customers
- Process: exercise took place over three days, daily scenario and questions, all anonymous responses, TIC injects and recommendations
- Targets: four separate scenarios and question sets for various participants: FIs, card processors, retailers, businesses
- After Action Report – being compiled and reviewed

CAPP Exercise Breakdown of Participants

	Day 1	Day 2	Day 3
Financial Institutions	639	611	559
Business & Gov't Users	67	63	54
Card Processors	34	33	31
Retailers	29	27	24
Total:	**769**	**734**	**668**

Conclusions

Threat Horizon Conclusions

- Bad guys will find ways to inject their malware onto machines by whatever means necessary
- Broad attacks using DNS cache poisoning redirection, spear phishing, and SQL injection will continue to increase targeting both FI and customers
- Custom malware **WILL CONTINUE to** defeat AV. Client protection will be problematic as a result.
- Targeted attacks, leveraging social media, will continue to be a significant problem for intelligence vendors, increasing emphasis on both internal corporate and industry information sharing to detect and mitigate.

The Threat Horizon

- Attackers will expand their data mining on individuals and companies to increase the sophistication of their attacks
- Social engineering is powerful and requires both customer and internal education and awareness to mitigate
- Financial Institutions and their customers as well as third party processors are major targets
- Technical and non-technical attacks will increase against users of payment services
- Attacks are becoming more aggressive and persistent
- Weakest links will suffer the most

Impact on SWACHA Membership

- Significant number of DFI's impacted
- Wide variety of attacks
  - Small businesses
  - School districts
  - Churches
  - Even one bank's internal systems
- Most have not been made public
- Litigation pending = cannot discuss
- Known losses
  - School district - $700,000
  - 2 small businesses – $100,000 and $1.2 million
- Others have been widely publicized in press