FS-ISAC

CHARLES BRETZ

THE PUZZLE OF PAYMENTS SECURITY:

Fitting the Pieces Together to Protect the Retail Payments System

FINANCIAL SERVICES ISAC

Information Sharing

To be forewarned is to be fore-armed

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; 2014: 5900 participants
- 2500 members bound by operating rules
- Sharing information globally

FINANCIAL SERVICES ISAC

FS-ISAC Operations

Information Sources

GOVERNMENT SOURCES

- DHS
- Treasury & FS Regulators
- FBI, USSS, NYPD
- 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 Listservers (Payments Risk Council and Payment Processor Information Sharing Council)**
- Document Repository
- Member Surveys
- Risk Mitigation Toolkit
- Threat Viewpoints

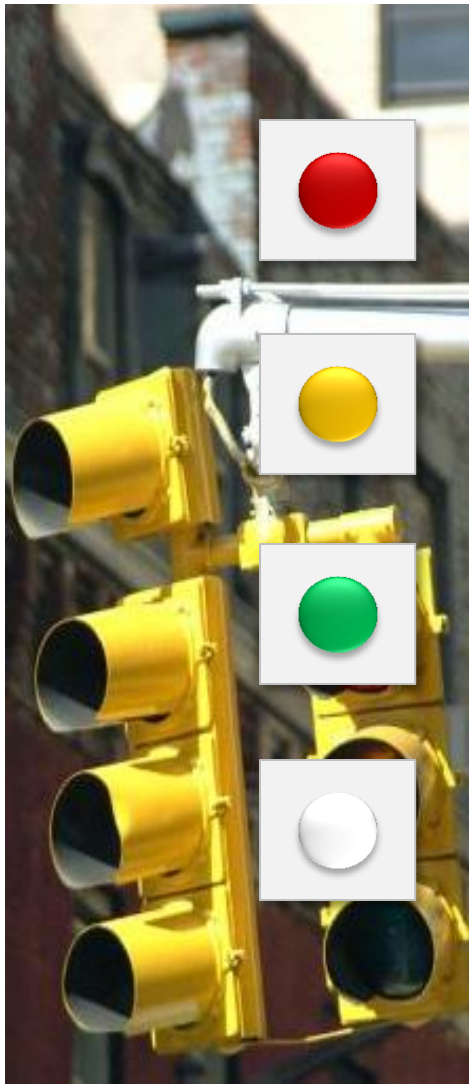
Ongoing Engagement

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

Readiness Exercises

- US and EU 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

How FS-ISAC Works: Circles of Trust

IRC	Insurance Risk Council
CHEF	Clearing House and Exchange Forum
PRC	Payments Risk Council
PPISC	Payment Processor Information Sharing Council
CIC	Community Institution Council
CAC	Compliance and Audit Council
TIC	Threat Intelligence Committee
Cyber Intel	Cyber Intelligence List

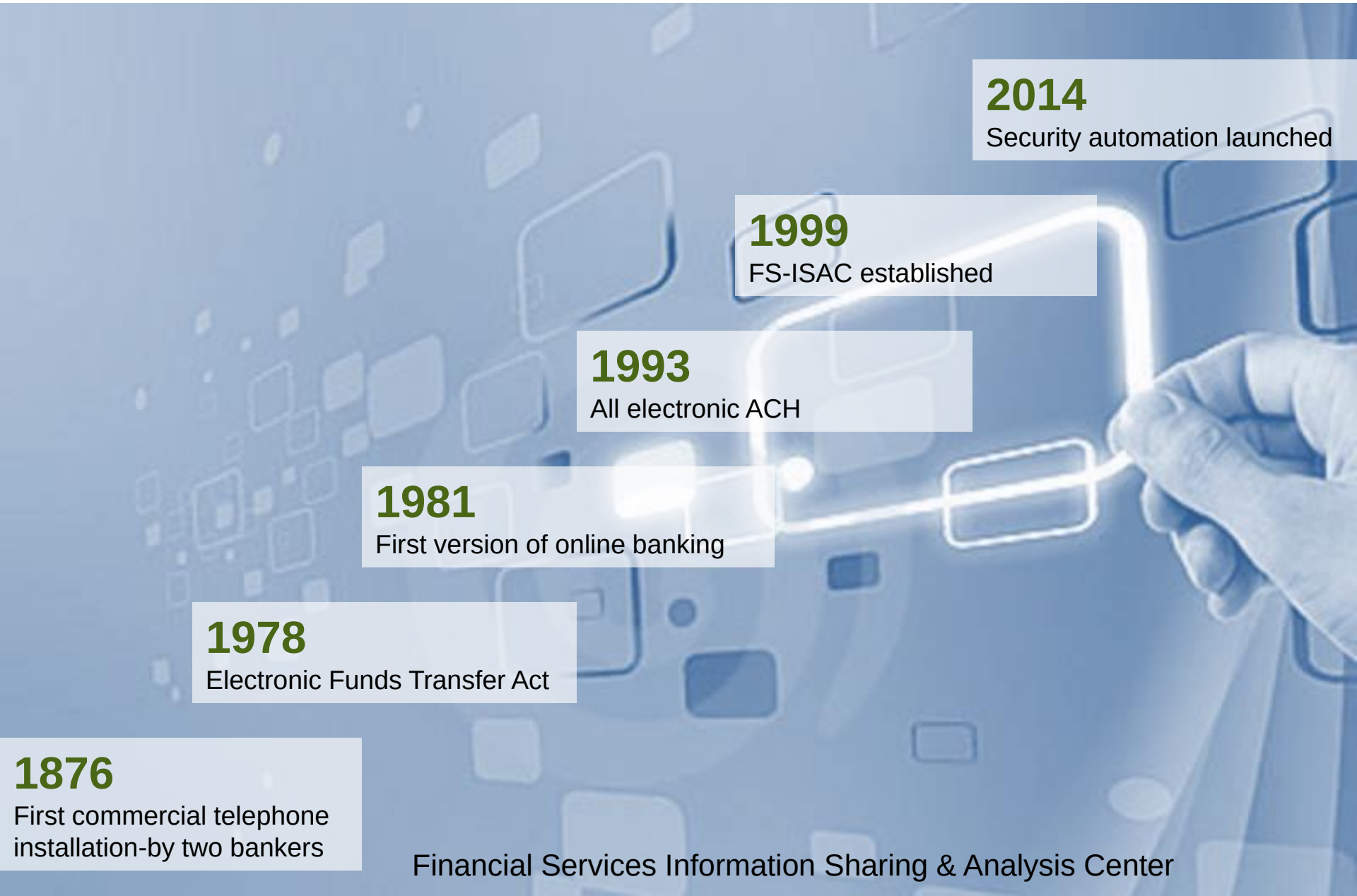
Member reports incident to Cyber Intel List

Members respond with initial analysis and recommendations

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

FINANCIAL SERVICES ISAC

Automation Inflection Points



2014
Security automation launched

1999
FS-ISAC established

1993
All electronic ACH

1981
First version of online banking

1978
Electronic Funds Transfer Act

1876
First commercial telephone installation-by two bankers

Financial Services Information Sharing & Analysis Center

The need for speed

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%

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
  - 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**
  - First available was on 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

STIX Constructs

An open standard to categorize cyber threat intelligence information

Atomic

What threat activity are we seeing?

Tactical

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

Operational

Where has this threat been seen?

What can I do about it?

What weaknesses does this threat exploit?

Strategic

Who is responsible for this threat?

Why do they do this?

What do they do?

SOLTRA

Threat Intelligence Automation Solution

- **Instead of 2% or less of attacks blocked, detected, or prevented, a much higher percentage of attacks are stopped.**