Threat Intelligence Sharing in the Financial Services Sector
Munich, Germany
February 24th, 2016

Ray Irving
Director CEMEA, FS-ISAC
rirving@fsisac.eu
Agenda

• About FS-ISAC
• About Threat Intelligence
• How FS-ISAC works
• European Sharing Landscape
• FS-ISAC European Strategy 2016
• Next Steps
About FS-ISAC
A nonprofit private sector initiative formed in 1999
- Designed/supported/owned by the financial services industry
- Mitigate cybercrime, hacktivist, nation state activity
- Process thousands of threat indicators per month
- 2004: 68 members; 2015: 6700 members
- Share information globally, 38 countries

"The FS-ISAC is not a service provider, it’s a community…Like a neighborhood watch for cyber and physical hazards.” – A Longtime Member
Investment in Protecting the Sector

- **Soltra Edge:** first industry-owned Cyber Threat Intelligence Repository
  - Uses industry standard protocols: Structured Threat Information eXpression (STIX™) & Trusted Automated eXchange of Indicator Information (TAXII™)
- **Civil litigation actions against botnet infrastructures. Last two targeted botnets targeting UK FIs and customers:**
  - Shylock 2014
  - Ramnit 2015
- **Sector Resilience Activities:**
  - Cyber Attack Against Payments
  - All Hazards Playbook and US sector activities could scale to Europe
- **Education and Training:**
  - Annual Summits (2 in the US, 1 in Europe, 1 in APAC). “Who’s who” of risk & security executives participate and speak.
  - Member meetings, workshops and trainings.
The Case for Information Sharing

ONE ORGANIZATION’S INCIDENT BECOMES THE INDUSTRY RESPONSE
About Threat Intelligence
“Intelligence is more than information. It is knowledge that has been specially prepared for a customer’s unique circumstances. ... The word ‘knowledge’ highlights the need for human involvement. Intelligence collection systems produce... data, not intelligence; only the human mind can provide that special touch that makes sense of data for different customers’ requirements.

... The special processing that partially defines intelligence is the continual collection, verification, and analysis of information that allows us to understand the problem or situation in actionable terms and then tailor a product in the context of the customer’s circumstances.

... If any of these essential attributes is missing, then the product remains information rather than intelligence.”

— Captain William Brei, ‘Getting Intelligence Right,’ US JMIC Publication
Senior Leaders: support business strategy by delivering insight into cyber threats which could (or have) impacted risk thresholds.

Middle Managers: timely, relevant & applied within a risk management framework to allow for review & testing of policy & controls.

Network Defenders tactical feeds of technical indicators supports the real-time defence of networks and provides a measure of the effectiveness of IT security controls.

Source: “Cyber Intelligence In Practice” a white paper produced by FSCG and FS-ISAC joint working group
Types of Threat Intelligence

**Tactical**
- How & What
  - MD5 hashes, IP addresses, malicious domains
  - hours/days
- Network defense on mail gateways, proxy servers, NIDS
- Analysts, CERT & SOC

**Operational**
- When, Where & How
  - Tactics, Techniques, Procedures
  - weeks/months
- Risk Matrix, Vulnerability Assessment

**Strategic**
- Who & Why
  - Intent, goals, strategy, political & economic factors
  - months/years
- Risk Matrix & Risk Registry
- Senior Stakeholders
How FS-ISAC Works
# Tools for sharing

<table>
<thead>
<tr>
<th>Tool</th>
<th>Intelligence Shared</th>
<th>Target Audience</th>
<th>Type of Intel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Intelligence mailing list</td>
<td>~40 mails/day: near real time observations, incidents, requests and queries from the community.</td>
<td>Threat Intelligence, Security Operations &amp; Malware Analysts</td>
<td>Tactical, Operational</td>
</tr>
<tr>
<td>Portal Alerts</td>
<td>~20 alerts/day: Cyber and Physical Threats &amp; Incidents; Vulnerabilities; Collective Intelligence.</td>
<td>Threat Intell. &amp; Malware Analysts, SOC and Physical security staff.</td>
<td>Tactical, Operational</td>
</tr>
<tr>
<td>Daily Summary</td>
<td>Daily overview of all alerts.</td>
<td>Head of Intelligence or Security Operations.</td>
<td>Tactical, Operational</td>
</tr>
<tr>
<td>Bi-weekly Threat Calls</td>
<td>Threat landscape review including 3rd party briefings and threat level discussion.</td>
<td>Risk and Information Security Management</td>
<td>Operational, Strategic</td>
</tr>
<tr>
<td>Member Meetings &amp; Summits</td>
<td>Member presentations on experiences and best practices.</td>
<td>All information security staff.</td>
<td>Operational, Strategic</td>
</tr>
</tbody>
</table>
FS-ISAC Information Flow

**Information Sources**
- CERTs
- FS Regulators
- Law Enforcement
- Other Intel Agencies

**Government Sources**
- Fox IT
- Secunia Vulnerabilities
- Wapack Labs Malware Forensics
- NC4 Phy Sec Incidents
- MSA Phy Sec Analysis

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

**Cross Sector Sources**
- Alerts
- Member Submissions

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

**FS-ISAC 24x7 Security Operations Center**
Traffic Light Protocol

**Red:** 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.

**Amber:** This information may be shared with FS-ISAC members.

**Green:** 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.

**White:** This information may be shared freely and is subject to standard copyright rules.

---

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

**Members or IAT respond in real time with initial analysis and recommendations**

**IAT completes analysis, anonymizes the source, and generates alert to general membership**
Types of FS-ISAC Alerts

Alert Types

ANC: Announcement
CYT: Cyber Threat
CYI: Cyber Incidents
COI: Collective Intelligence
CYV: Cyber Vulnerability
PHT: Physical Threats
PHI: Physical Incidents

Criticality and Priority:
- ANC = Priority – 1-10, 8-10 is high priority
- CYV = Risk – 1-10, 8-9 is Urgent, 10 is Crisis
- CYT = Risk – 1-10, 8-9 is Urgent, 10 is Crisis
- COI – No Criticality Metric
- PHT = Risk – 1-10. 8-9 is Urgent, 10 is Crisis

Observables
Indicators
Incidents
TTPs
European Sharing Landscape
UK Finance Sector Cyber Related Collaboration Groups

and their National and International Links
Community Defense Vision

- Intelligence Ecosystem
  - One Firm’s Intelligence becomes an Entire Community’s Defense
Automated Community Defense

Organization With Intelligence

Cyber Threat

Central Intelligence Repository

Trusted Member Organizations
## Build Trusted Communities

<table>
<thead>
<tr>
<th>Task</th>
<th>What / How?</th>
</tr>
</thead>
</table>
| 1. **Build Trusted Communities** | i. Link into in-country sharing schemes  
ii. Encourage / develop the JWGI  
iii. FS-ISAC (add value by linking national into regional /global network) |

**Task 1. Build Trusted Communities**

- **i.** Link into in-country sharing schemes
- **ii.** Encourage / develop the JWGI
- **iii.** FS-ISAC (add value by linking national into regional /global network)

---

**i. & iii. - Most EU countries have some degree of in-country sharing:**

- **FS-ISAC can be the proxy for sharing between in-country and regional sharing schemes.**
- **Country-based memberships can encourage anonymous sharing.**
- **FS-ISAC LE/Govt relationships can help mitigate internal PPP issues.**
“Engagement & Collaboration”

<table>
<thead>
<tr>
<th>Task</th>
<th>What / How?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2. Engagement / Collaboration:</strong></td>
<td>Link into / influence key nodes:</td>
</tr>
<tr>
<td>a. Law Enforcement</td>
<td><strong>Operational:</strong></td>
</tr>
<tr>
<td>b. Government</td>
<td>i. Europol (EC3)</td>
</tr>
<tr>
<td>c. Regulators</td>
<td>ii. In-country LE / CERTs</td>
</tr>
<tr>
<td></td>
<td><strong>Policy / Regulation:</strong></td>
</tr>
<tr>
<td></td>
<td>i. European Banking Federation (EBF)</td>
</tr>
<tr>
<td></td>
<td>ii. European Commission / Parliament</td>
</tr>
<tr>
<td></td>
<td>iii. ENISA</td>
</tr>
<tr>
<td></td>
<td>iv. National Banking Associations</td>
</tr>
</tbody>
</table>
Next Steps

• If you are an FS entity:
  – Cost to join FS-ISAC based on asset value (banks) or revenue (insurance).
  – We are a non profit so membership fees are very reasonable.
  – Talk to us about joining for a 6 month evaluation period.

• If you are a CERT:
  – We would like to establish a formal relationship with you.
  – As per the CERT UK model: this could be a Memorandum of Understanding allowing sharing of green and clear intel/products plus “as needed” sharing of amber intelligence.
  – Open to other suggestions.
Contact Information

Ray Irving
Director, Continental Europe, Middle East and Africa
rirving@fsisac.eu

www.fsisac.com