Cybersecurity Panel

ABA Mutual Community Bank Conference
Marriott Marquis Hotel, Washington, D.C.
Your Panel

• Speakers:
  – Bill Nelson, President and CEO, Financial Services Information Sharing and Analysis Center
  – Al Williams, Chief Operating Officer, Dollar Bank

• Moderator:
  – Doug Johnson, Senior Vice President, Payments and Cybersecurity Policy, American Bankers Association
The Threat Landscape and FS-ISAC Overview

Financial Services Information Sharing & Analysis Center
Agenda Today

- Threat Landscape
- FS-ISAC Background
  - Services
  - Examples of information shared
  - Membership Tsunami
- Community Bank resources
  - Maximize value of FS-ISAC membership
- What’s Next?
Threat Trends

**Cyber Crime**
- Bad guys are mostly Eastern European although Asian groups are also active.
- A complete service based economy supporting their activities
- Attacks are a mix of social engineering and technical attack.

**Hactivists**
- Started with WikiLeaks
- “Anonymous”
- DDoS attacks
- Data loss – combination of hacking and insiders

**Nation State**
- Motivations: espionage (APT), disruption (AQCF)
- Targeting Government + private sector
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

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
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.
DDoS Attack

Your customers

Compromised PCs

Company X edge router

Your Internet ISP

Company X network and web server

Servers controlled by attackers
Background FS-ISAC
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: 5400+ members
- Sharing information globally

MISSION:

Sharing Timely, Relevant, Actionable Cyber and Physical Security Information & Analysis
FS-ISAC Operations

Information Sources
- DHS
- Treasury & FS Regulators
- FBI, USSS, NYPD
- Other Intel Agencies

GOVERNMENT SOURCES

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

Cross Sector (other ISACS)
Open Sources (Hundreds)

FS-ISAC 24x7 Security Operations Center

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 (Community Institution Council)
- 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**
- US and EU Government Sponsored Exercises
- CAPP Exercise
- Advanced Threat/DDoS Exercise
- Industry exercises- QD2/Pandemic

Financial Services Information Sharing & Analysis Center
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

- 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
- NEW:
  - Asset Managers (AM)
  - Dealer Brokers (DM)

**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
# Types of Information Shared

<table>
<thead>
<tr>
<th>Cyber Threats, Vulnerabilities, Incidents</th>
<th>Physical Threats, Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Malicious Sites</td>
<td>✓ Terrorism</td>
</tr>
<tr>
<td>✓ Threat Actors, Objectives</td>
<td>✓ Active Shooter</td>
</tr>
<tr>
<td>✓ Threat Indicators</td>
<td>✓ Hurricanes</td>
</tr>
<tr>
<td>✓ TTPs, Observables</td>
<td>✓ Earthquakes</td>
</tr>
<tr>
<td>✓ Courses of Action</td>
<td>✓ Other meteorological events</td>
</tr>
<tr>
<td>✓ Exploit Targets</td>
<td>✓ Geopolitical impacts</td>
</tr>
<tr>
<td>✓ Denial of Service Attacks</td>
<td>✓ Pandemic</td>
</tr>
<tr>
<td>✓ Malicious Emails: Phishing/Spearphishing</td>
<td>✓ Type, location, severity</td>
</tr>
<tr>
<td>✓ Software Vulnerabilities</td>
<td>✓ Impact analysis and risk mitigation</td>
</tr>
<tr>
<td>✓ Malicious Software</td>
<td>✓ Business resilience preparation and incident response</td>
</tr>
<tr>
<td>✓ Analysis and risk mitigation</td>
<td></td>
</tr>
<tr>
<td>✓ Incident response</td>
<td></td>
</tr>
</tbody>
</table>
FS-ISAC Community Institution Council reviewed impact on ATMs from Windows XP end of life

- Microsoft ends support of Windows XP April 8, 2014
- 95% of ATMs run on XP.
- Community Institution Council members shared strategies on
  1) extending maintenance,
  2) determining ATM Operating System,
  3) embedded XP support,
  4) network isolation options.
Advisories and recommendations from membership (Threat Intelligence Committee), government, and third parties (intel vendors)

- Shared websites with information about Heartbleed--
  - Heartbleed Overview
  - NIST NVD: CVE-2014-0160 (aka the Heartbleed Bug)
  - TrendMicro: Heartbleed Bug—Mobile Apps are Affected Too
- Community Institution Council shared information and recommendations to FS-ISAC SOC
- Shared website links identifying affected systems, websites, and status
  - US-CERT: Vendor Information for the "Heartbleed" Bug
  - CNET: Site Patch Status for the "Heartbleed" Bug
  - Reuters: 'Heartbleed' blamed in attack on Canada tax agency, more expected
  - Akamai: Heartbleed Update (v3)
- Emergency membership call
FS-ISAC Membership “Tsunami”

- FFIEC regulator webinar May 7, 2014 followed by FFIEC Guidance issued on November 3, 2014. FFIEC encourages all FIs to join FS-ISAC.

- Over 1,400 new members in the last twelve months.

- FS-ISAC has responded by:
  - Expanding its customer service and business relationship management staffs,
  - Adding a resource for community institutions,
  - Adding global 24x7 SOC services,
  - Completing Security Toolkit October 2014,
  - Finishing “Aid to Processing FS-ISAC Information.”
# Membership Tiers

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Basic</th>
<th>Core</th>
<th>Standard</th>
<th>Premier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Membership Dues</td>
<td>$250.00/yr.</td>
<td>$850.00/yr.</td>
<td>$5,000/yr</td>
<td>$10,000/yr.</td>
</tr>
<tr>
<td>Users Access Credentials</td>
<td>1</td>
<td>4</td>
<td>10</td>
<td>25</td>
</tr>
<tr>
<td>CINS, Government, Member, and Partner Alerts</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Member Contact Directory</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Ability to Join Committees and Working Groups</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Attendance to Bi-Weekly Threat Calls</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Ability to Join Business Resilience Committee and Threat Intelligence Committee</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
FS-ISAC Community Bank Resources
Jeff Korte, Director Community Institutions and Associations

Sept 2014– hired to support Community Bank and Association activities.

Work Experience:
• VP Bank Security Officer for a $2.5B community bank
• Corporate Security and Info Sec Manager
• Investigations Officer

Association Experience:
• Chair of a state bankers association FI security taskforce
• ABA credit card security task force
• FS-ISAC CIC member
Community Institution Goals

Create value-added programs that focus on community institutions by:

• Perform data analysis from community institution perspective
• Create and distribute relevant and actionable threat and vulnerability awareness alerts
• Generate weekly C-level threat summaries
• Monitor and comment on Community Institution Council (CIC) email listserver
• Facilitate monthly CIC calls
• Devise relevant quarterly community institution webinars
• Create and facilitate working groups
• Develop services based upon member feedback and requests
Weekly Risk Summary Reports provide C-Level management with overviews of the week's top critical threats.
Making Choices to Filter Relevant and Actionable Information

• FS-ISAC provides summary reports for managers and technical reports for analysts.
• Bank staff have different roles within most banks. Examples: information security, fraud, payments risk.
• Assign portal accounts to individuals with key responsibilities.
• Employ FS-ISAC portal filtering of alerts.
• Use MS Outlook filters as needed for additional routing or filtering.
• Goal: Make informed choices based on roles and eliminate unnecessary emails.
What’s Next?

Financial Services Information Sharing & Analysis Center
Potential Emerging Threat Landscape

**Mobile Platforms**
Bandwidth and continuous connectivity makes it an ideal platform for launching attacks. Tools are now available on Google Play and for the iPhone.

**Social Media**
People instantly, globally connected 24/7. Syrian Electronic Army hacking of AP Twitter demonstrated moving markets

**Supply Chain**
Compromise of supply chain has occurred within financial sector. Hardware and software integrity are resource intensive challenges
Evolution from Disruptive to Destructive Attacks

Advanced DDOS – 2012, 2013
• 40+ FIs targeted, wake-up call for FS industry
• Resulted in dynamic, effective information sharing

Shamoon – 2012
• Malware executable spread using network shared drives
• Corrupts files and wipes device boot blocks at specified date
• A group named "Cutting Sword of Justice" claimed responsibility
• Attack on 30,000 Saudi Aramco workstations

South Korean Attacks – 2013
• 2 banks, media company and insurance company, patch systems targeted
• Wipers hit Windows, Linux and UNIX OS and removed file systems. Over 3,000 machines made unbootable

Sony – 2014
• Data breach but more importantly destructive malware installed on their network and core systems including back-up.
• Intellectual property and sensitive information released publically.
• Impact– financial system data destroyed, inability to disburse payments, still can’t produce financials for 3rd quarter 2014.
12/3/2014 speech-- Sarah Raskin, Deputy Secretary of the U.S. Treasury provided guidance to chief executive officers, chief risk executives and boards of directors for assessing cybersecurity preparedness:

**Baseline Protections**

- Is cybersecurity part of your current risk management framework?
- Is your FI following the National Institute for Standards and Technology (NIST) Framework?
- Do you know the cyber risks of using your vendors and third-party service providers and do you know the rigor of their cybersecurity controls?
- Do you have cyber risk insurance?
- Do you engage in basic cyber hygiene (*to protect your enterprise and your customers*)?
Sarah Raskin guidance (continued)

Information Sharing
✓ Do you share information with the Financial Services Information Sharing & Analysis Center, as well as other industry groups, and if so, how often?

Response and Recovery
✓ Do you have a cyber-incident playbook, and who is the point person for managing the response and recovery?
✓ What roles do senior leaders and the board play in managing and overseeing the cyber incident response?
✓ When and how do you engage law enforcement after a breach?
✓ After a cyber-incident, when and how do you inform customers, investors and the general public?
Information Sharing

One Organization’s Incident becomes the Industry Response
Contact Information

Bill Nelson, President & CEO        bnelson@fsisac.us
Eric Guerrino, EVP Operations      eguerrino@fsisac.us
Jeff Korte, Director Community Institutions jkorte@fsisac.us
Denise Anderson, VP Gov’t & Cross-Sector Programs danderson@fsisac.us
                                      Chair, Nat’l Council of ISACs
Rick Lacafta, Director Insurance Services rlacafta@fsiac.us
Charles Bretz, Director Payment Services cbretz@fsisac.us
Beth Hubbard, Director of Member Services bhubbard@fsisac.us

www.fsisac.com
Thank You for Your Time Today

Financial Services
Information Sharing & Analysis Center
Things you need to know
CYBERSECURITY

Questions every CEO should be asking
While Cyber Security is a very difficult topic to cover in a brief session, there are a number of areas that management can make inquiries into with IT security staff that will give a good indication of the current level of cyber security within your institution.

For those institutions that have outsourced the IT function, these questions should be addressed to your vendor.
Does the IT unit prepare an IT risk assessment which includes a cybersecurity risk evaluation

Does the risk report provide recommendations

Has this been communicated to the board of directors
SECURITY AWARENESS TRAINING

- Is there security awareness training for all new employees?
- Do all existing employees (including all Senior Management) receive security awareness training at least annually.
- Can you produce a documented report of the completion of such training.
Have you and the senior risk officer and/or Board committee reviewed the following type of reports:

- Number of blocked inbound emails
- Number of blocked outbound emails which contained personal customer information
- Number and type of intrusion attempts on your network
Bank Tool:

Spam Prevention: Email caught and blocked from entering Bank

Inbound Email allowed or blocked as spam

<table>
<thead>
<tr>
<th>Month</th>
<th>Blocked Inbound Email (Spam, corrupt or invalid)</th>
<th>Accepted Inbound Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec-13</td>
<td>2,526,199</td>
<td>481,498</td>
</tr>
<tr>
<td>Jan-14</td>
<td>2,480,350</td>
<td>501,651</td>
</tr>
<tr>
<td>Feb-14</td>
<td>2,331,873</td>
<td>486,313</td>
</tr>
</tbody>
</table>
Bank Tool:

Encryption of outbound email

![Bar chart showing encryption of outbound email from December 2013 to February 2014.](chart.png)
Bank Tool: DLP
Data Loss Prevention (DLP) ensures that outgoing email containing sensitive information is blocked if the sender did not encrypt the email.

Breakdown of blocked outbound sensitive data:

<table>
<thead>
<tr>
<th></th>
<th>Dec-13</th>
<th>Jan-14</th>
<th>Feb-14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card #</td>
<td>2</td>
<td>4</td>
<td>11</td>
</tr>
<tr>
<td>Debit Card #</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>TRA Account #</td>
<td>70</td>
<td>87</td>
<td>80</td>
</tr>
<tr>
<td>Social Security #</td>
<td>26</td>
<td>48</td>
<td>29</td>
</tr>
</tbody>
</table>
Bank Tool:
- Incoming email: Protects against viruses and malware
- Incoming email: Protects by filtering out spam
- Outgoing Email: Performs email encryption

### Malware blocked by xxxxxx

<table>
<thead>
<tr>
<th>Malware</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>gen:variant.kazy.333943</td>
<td>283</td>
</tr>
<tr>
<td>General (virus-like behavior)</td>
<td>221</td>
</tr>
<tr>
<td>trojan.spy.zbot.fjw</td>
<td>208</td>
</tr>
<tr>
<td>trojan.ranapama.n</td>
<td>177</td>
</tr>
<tr>
<td>gen:variant.graftor.132099</td>
<td>155</td>
</tr>
</tbody>
</table>

February 2014: Top 5 Malware  

Company Confidential
Bank Tool: Endpoint Protection & Endpoint Security *
Provides anti-virus and anti-malware protection on end-user computers and servers.

Malware on Desktops, Laptops, or Servers

- Blocked or Detected & Cleaned
- Still Infected Posing a Risk to Bank
Some DDOS attacks against banks have been initiated to distract bank security personnel. Then business customer computers which have been compromised by man in the middle malware send out fraudulent wire transfers or ACH files.

What type of layered controls do you have on outgoing wires and ACH files.
Customers

- What type of education have you provided to your retail and business customers
- Have you really provided two factor authentication in online banking sessions
- Have you provided any security enhancement tools to your high risk customers
Are you preparing the bank to make the best use of the new top level domain - .bank
- Process for obtaining a .bank name
- Trademark clearing house
- Marketing plan
- IT changes
- Customer education on enhanced security features of .bank
In a world consisting of .coms and .govs...

Over one thousand new domains being added
The Internet financial world will also change...
Key Marketing Themes

• Robust Operational Requirements
  – Eligibility Standards; who can participate
  – Name Selection; what kinds of names can be registered
  – Acceptable Use / Anti-Abuse; how domains may be used
  – Prohibition of Proxy Registrations
  – Mandatory verification of all registrations prior to activation

• Enhanced Technical Requirements
  – Domain Name Security (DNSSEC) deployment across registration chain (i.e., registry, registrar and registrant)
  – Multi-factor authentication by registry and registrar (NIST level 3 or higher)
  – Enhanced encryption standards
  – Email authentication records (e.g., DMARC, DKIM, SPF)
  – Exploring options for DDoS mitigation via real-time monitoring and detection
.bank is expected to launch June 15, 2015 but you need to be ready sooner

**TRADEMARK REGISTRATION PERIOD**
- Prior to May 18, 2015
  - Register organizations’ trademarked names with ICANN’s Trademark Clearinghouse.

**SUNRISE PERIOD**
- May 18 – June 17, 2015
  - Trademark holders registered with ICANN’s clearinghouse can register for domains matching trademarks.

**GENERAL AVAILABILITY**
- June 24 – Ongoing
  - Verified members of the banking community can register domains on a first come, first served basis.
Go to: ABA.com/dotbank for the latest

 bankers are making their way to the Internet. ABA partnered with banking industry participants to establish FTLD Registry Services to operate .bank and ensure it is governed in the best interests of banks and their customers. Only verified members of the banking community will be able to register .bank domains.

Why .bank?

.bank provides a more protected, trusted, easily identifiable place for banks to do business on the Internet.

.bank Timeline

General availability for banks across the globe is expected in mid-2015.