FEDERAL DEPOSIT INSURANCE CORPORATION

Cybersecurity Awareness

Part 2

Objectives

Cybersecurity Awareness

- Discuss the Evolution of Data Security
- Define and Discuss Cybersecurity
- Review Threat Environment

Part 1

- Discuss Information Security Programs
  - Enhancements for Cybersecurity Risks
    - Threat Intelligence
    - Third-Party Management
    - Cyber-Resilience
    - Incident Response
- Describe Cybersecurity Assessment Tool & Other Available Resources

Part 2

Information Security Program

Cybersecurity Awareness

Governance

Cybersecurity Awareness

- Board and Senior Management Duties and Responsibilities
  - Ensuring strategic planning and budgeting provide sufficient resources.
  - Providing sufficient authority, resources, and independence for information security.
  - Ensuring policies and procedures address cybersecurity.
  - Incorporating cyber risk into the risk-based audit plan.
  - Providing reports to reassure the Board the ISP is working.

- Cyber Risk is a Business Risk!

Control Structure

Cybersecurity Awareness

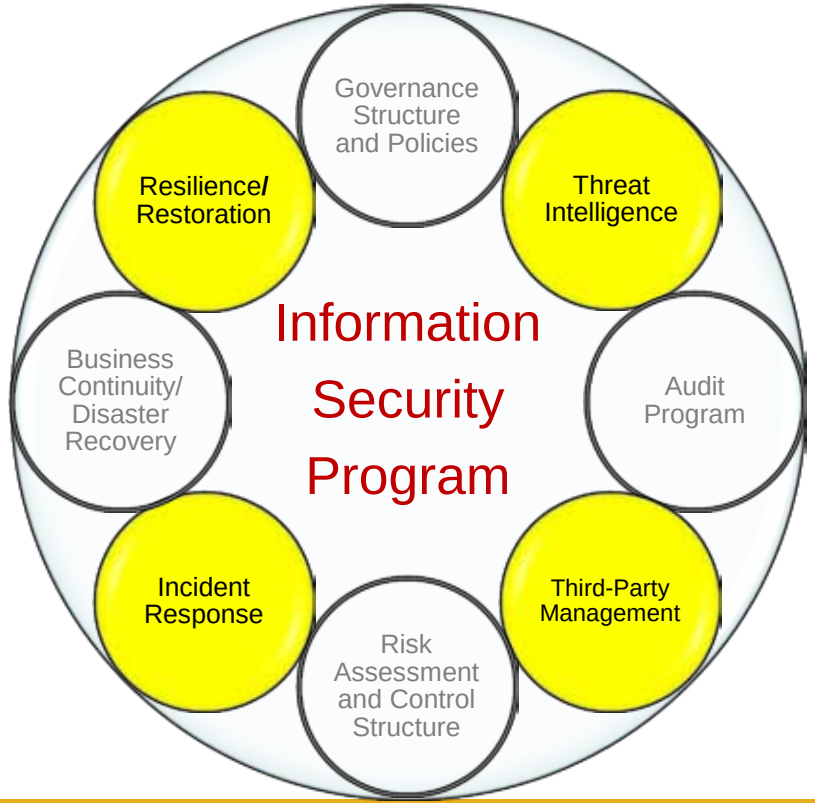
- Security Awareness Training
  - Enterprise-wide
  - Role-specific
  - Customers/Merchants
  - Third Parties
  - Cybersecurity Culture

“Think Before You Click”

- Patch Management
  - Formal written policies and procedures
    - Develop system for identifying, prioritizing, applying, and testing patches
    - Create/maintain asset inventories
      - Software (e.g., Microsoft and non-Microsoft)
      - Firmware (e.g., routers and firewalls)
    - Integrate threat intelligence
    - Establish strategies to migrate from unsupported products
    - Report to board and senior management
  - Audit and internal reviews should validate

Information Security Program: Refocused

Cybersecurity Awareness



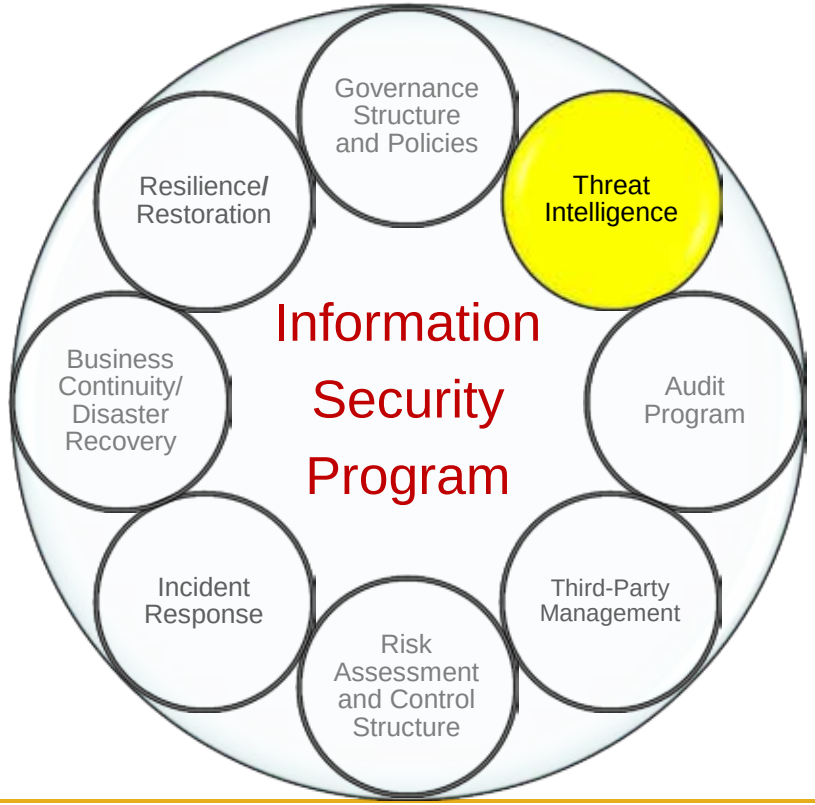
Information Security Program: Refocused

Cybersecurity Awareness

- FFIEC Guidance: “Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement,” dated November 3, 2014
  - “Financial institution management is expected to monitor and maintain sufficient awareness of cybersecurity threats and vulnerability information so they may evaluate risk and respond accordingly.”
  - Participation in Financial Services Information Sharing and Analysis Center (FS-ISAC) is encouraged.
- FFIEC Business Continuity Planning Booklet, Appendix J released on February 6, 2015 – Strengthening the Resilience of Outsourced Technology Services

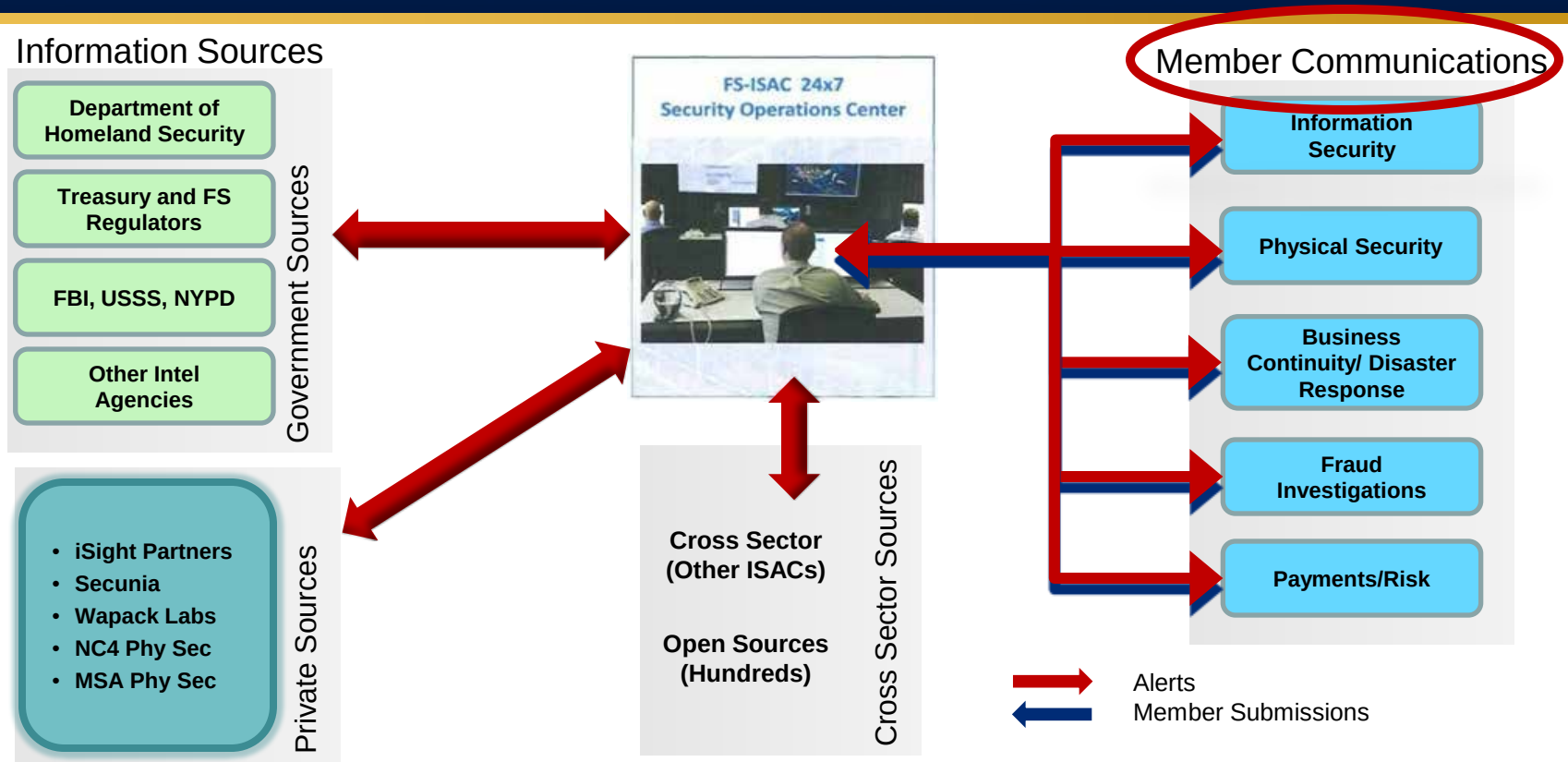
Information Security Program: Refocused

Cybersecurity Awareness



Threat Intelligence: FS-ISAC

Cybersecurity Awareness



Threat Intelligence: FS-ISAC

Cybersecurity Awareness

Step 2: *Understand the Criticality and Priority*

- ANC = Priority 1-10, 8-10 is high priority
- CYT = Risk 1-10, 8-9 is Urgent, 10 is Crisis
- CYI = Risk 1-10, 8-9 is Urgent, 10 is Crisis
- COI = No Criticality Metric
- CYV = Risk 1-10, 8-9 is Urgent, 10 is Crisis
- PHT = Risk 1-10, 8-9 is Urgent, 10 is Crisis
- PHI = Informational, Minimal Impact, Moderate Impact, Significant Impact, Major Business Disruption

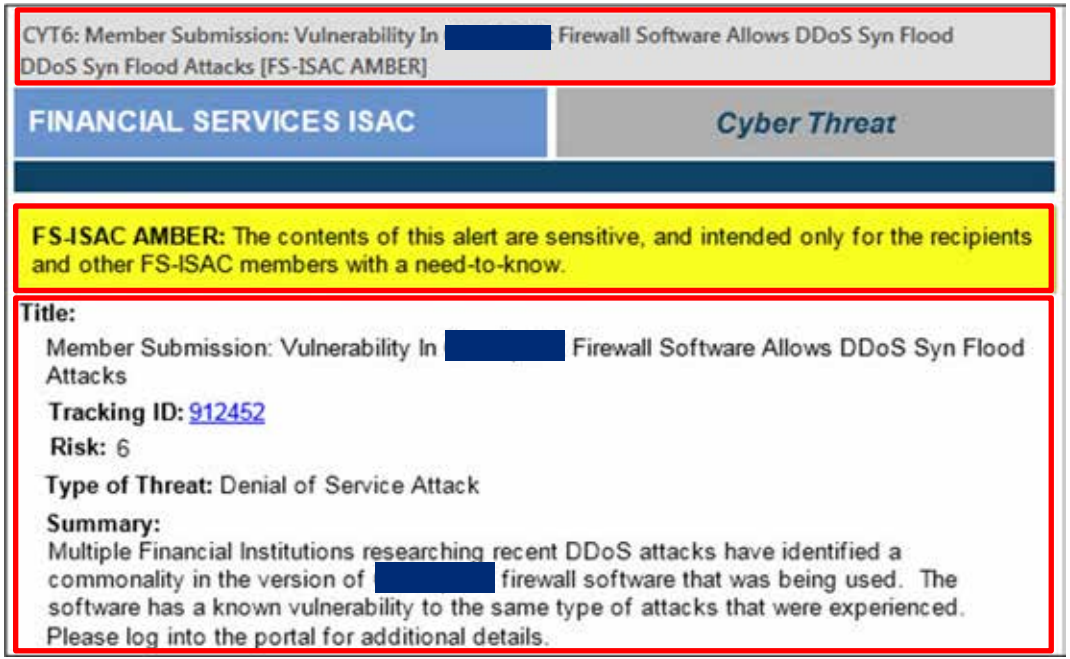
Step 3: Determine Distribution

- Analysts and those involved in risk assessments, vulnerability/ patch management, and intelligence gathering should receive CYV alerts.
- Provide portal accounts to bank staff based on each individual's role. This will allow them to employ portal filtering for their unique assignments.
- Provide summary reports for managers and technical reports for analysts. Making informed choices based on each person's role eliminates unnecessary emails.

FINANCIAL SERVICES ISAC

Threat Intelligence: FS-ISAC Alert

Cybersecurity Awareness



CYT6: Member Submission: Vulnerability In [redacted] Firewall Software Allows DDoS Syn Flood DDoS Syn Flood Attacks [FS-ISAC AMBER]

FINANCIAL SERVICES ISAC | *Cyber Threat*

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

Title:

Member Submission: Vulnerability In [redacted] Firewall Software Allows DDoS Syn Flood Attacks

Tracking ID: 912452

Risk: 6

Type of Threat: Denial of Service Attack

Summary:

Multiple Financial Institutions researching recent DDoS attacks have identified a commonality in the version of [redacted] firewall software that was being used. The software has a known vulnerability to the same type of attacks that were experienced. Please log into the portal for additional details.

The abbreviation and criticality level will always appear in the subject line, along with the title.

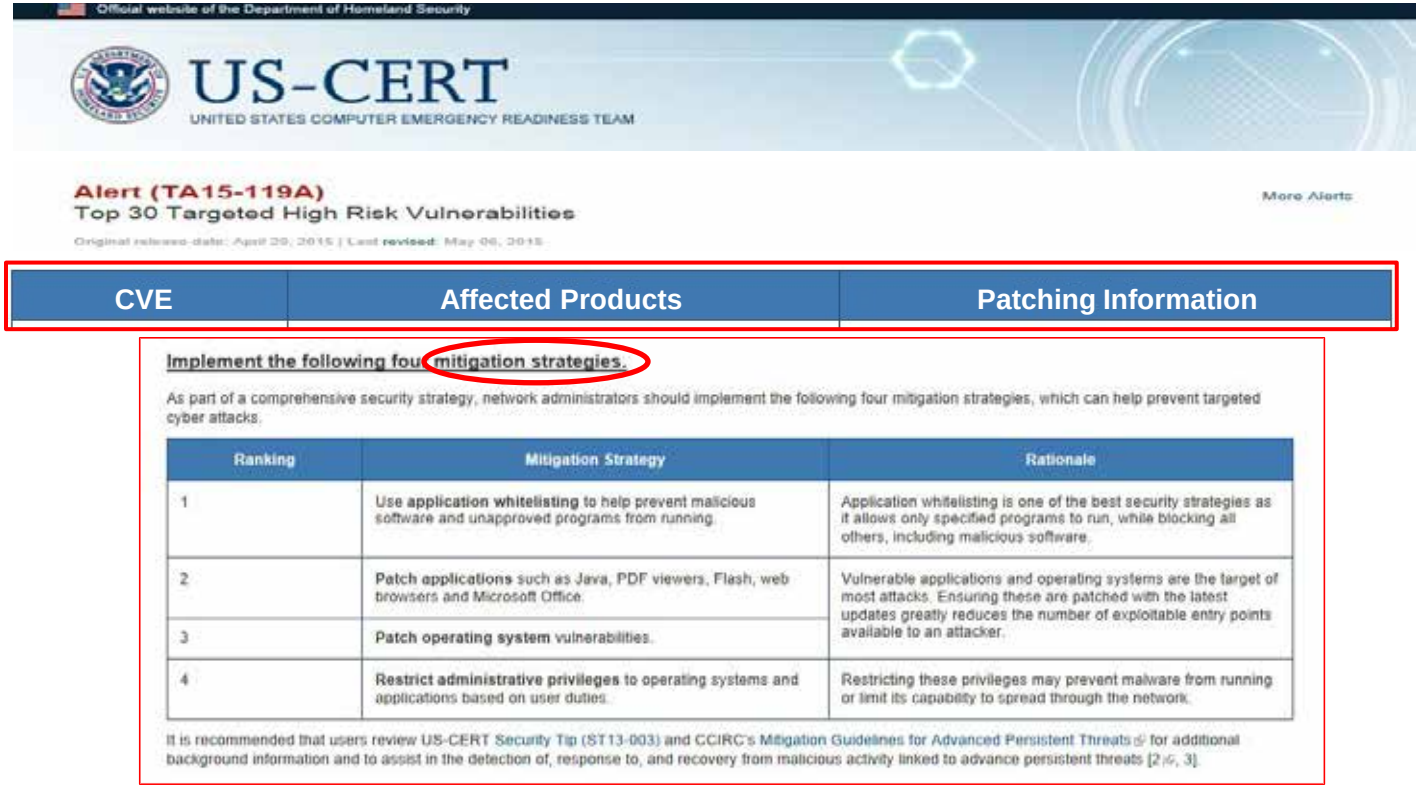
FS-ISAC's Traffic Light Protocol

White	**Share freely but copyrighted**
Green	**Share among FS-ISAC members and partners only. Not public.**
Amber	**Share among FS-ISAC members only.**
Red	**Restricted to a defined group.**

The alert will go into more detail such as the type of threat, summary, and handling instructions.

Threat Intelligence: US-CERT Alert

Cybersecurity Awareness



Official website of the Department of Homeland Security

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Alert (TA15-119A)

Top 30 Targeted High Risk Vulnerabilities

More Alerts

Original release date: April 29, 2015 | Last revised: May 06, 2015

CVE	Affected Products	Patching Information

Implement the following four mitigation strategies.

As part of a comprehensive security strategy, network administrators should implement the following four mitigation strategies, which can help prevent targeted cyber attacks.

Ranking	Mitigation Strategy	Rationale
1	**Use application whitelisting** to help prevent malicious software and unapproved programs from running.	Application whitelisting is one of the best security strategies as it allows only specified programs to run, while blocking all others, including malicious software.
2	**Patch applications** such as Java, PDF viewers, Flash, web browsers and Microsoft Office.	Vulnerable applications and operating systems are the target of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.
3	**Patch operating system** vulnerabilities.	
4	**Restrict administrative privileges** to operating systems and applications based on user duties.	Restricting these privileges may prevent malware from running or limit its capability to spread through the network.

It is recommended that users review US-CERT Security Tip (ST13-003) and CCIRC's Mitigation Guidelines for Advanced Persistent Threats for additional background information and to assist in the detection of, response to, and recovery from malicious activity linked to advance persistent threats [2, 3].

Threat Intelligence

Cybersecurity Awareness

External Sources

- FS-ISAC
- US-CERT
- Third-Party Servicers
  - e.g., core, telecommunications, managed security services

Internal Sources

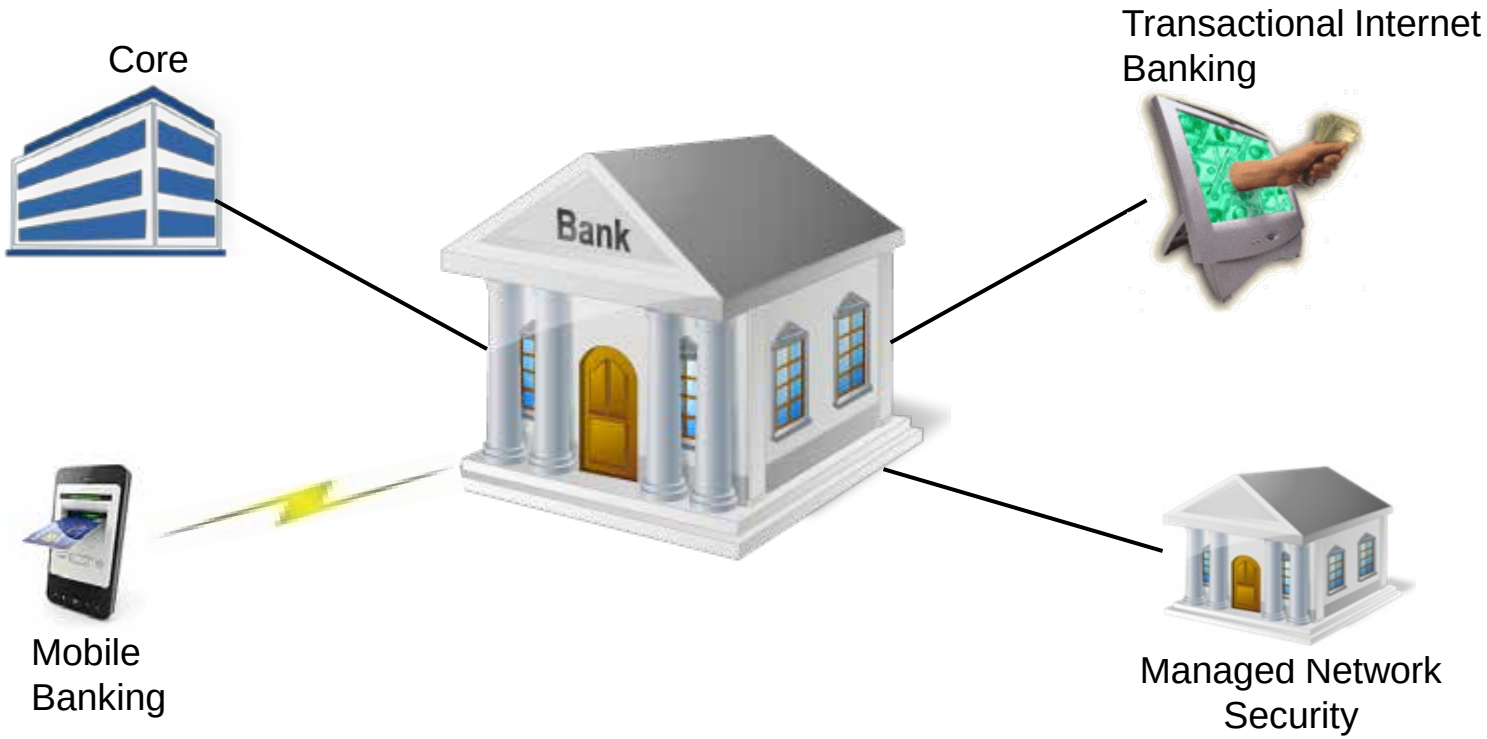
- Reports
  - Operational Reports
  - Internal Audit Reports
  - Fraud Detection Reports
  - Logs

Information Security Program: Refocused

Cybersecurity Awareness

Third-Party Management

Cybersecurity Awareness



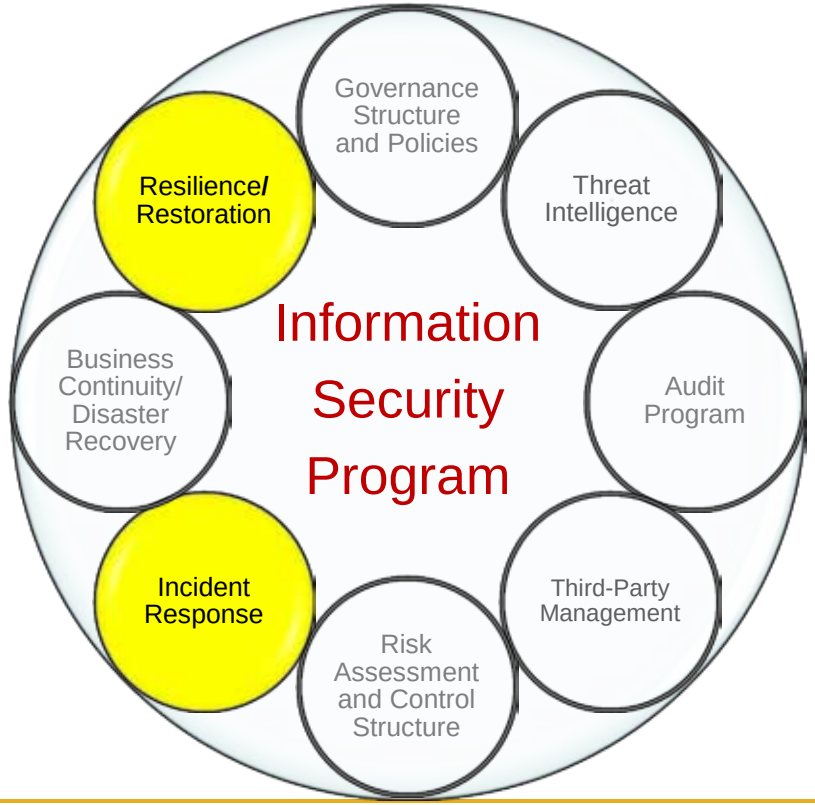
Appendix J: Third-Party Management

Cybersecurity Awareness

- Relationship Management
  - Due Diligence
  - Contracts
  - Ongoing Monitoring
- Resiliency and Testing
  - Mission-Critical Services
  - Capacity
  - Service Provider Continuity Strategies
  - Evaluate/Understand Gaps
  - Service Provider Alternatives

Information Security Program: Refocused

Cybersecurity Awareness



Appendix J: Resilience

Cybersecurity Awareness

- **Consider incorporating the following mitigating controls into business continuity plans:**
  - **Data backup architecture and technology**
  - **Data integrity controls**
  - **Independent, redundant communication providers**
  - **Layered security strategies**
  - **Enhanced planning for the possibility of simultaneous attacks**
  - **Increased awareness of potential insider threats**
  - **Prearranged third-party forensic and incident management services**

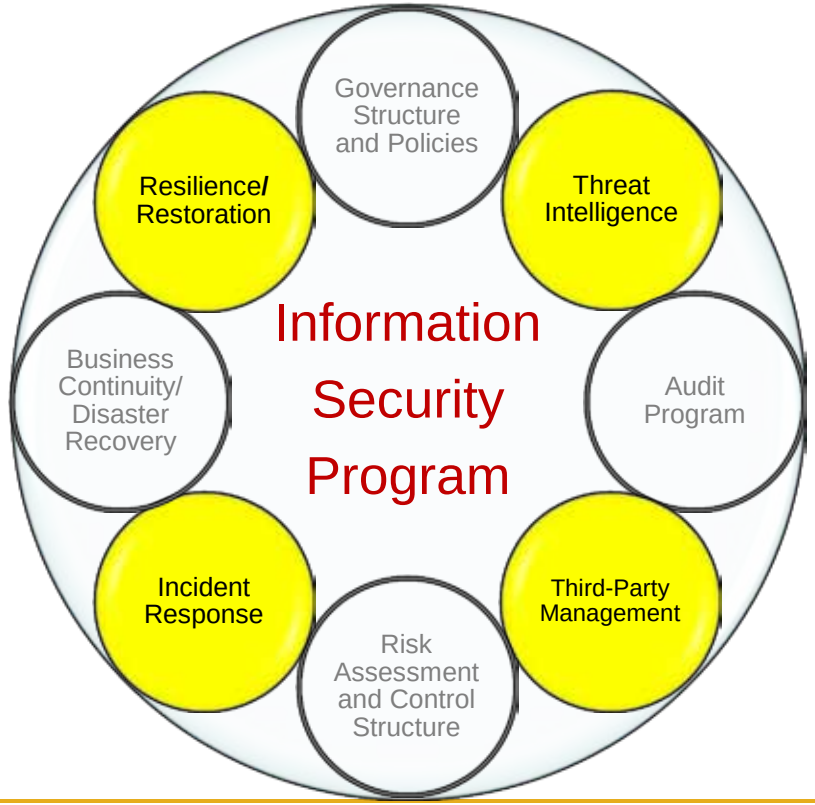
Appendix J: Incident Response

Cybersecurity Awareness

- **Enhance and test incident response plans to incorporate potential cyber threats**
- **Integrate service providers into incident response planning**
- **FFIEC Guidance: "Final Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," dated April 1, 2005**
  - Assess nature/scope and contain/control the incident
  - Notify primary Federal regulator
  - File Suspicious Activity Report (SARs) and notify law enforcement
  - Notify customers if there is a reasonable likelihood the information will be misused

Information Security Program: Refocused

Cybersecurity Awareness



FFIEC Cybersecurity Assessment Tool

Cybersecurity Awareness

- FFIEC Press Release: Cybersecurity Assessment Tool, dated June 30, 2015
  - Voluntary tool that provides management with a repeatable and measurable process to assess an institution's risks and cybersecurity preparedness
  - Consists of two parts: Inherent Risk Profile and Cybersecurity Maturity
  - Consider periodically reevaluating the Inherent Risk Profile and Cybersecurity Maturity over time as threats, vulnerabilities, and operational environments change

Benefits to the Institution:

- Identify factors contributing to and determining the institution's overall cyber risk profile.
- Assess the institution's cybersecurity preparedness.
- Evaluate whether the institution's cybersecurity preparedness is aligned with its risks.
- Determine risk management practices and controls that could be enhanced and actions that could be taken to achieve the desired state of cyber preparedness.
- Inform risk management strategies.

Evolution of Data Security

Cybersecurity Awareness

Threat Intelligence Resources

Cybersecurity Awareness

- Financial Services-Information Sharing and Analysis Center (FS-ISAC)
  www.fsisac.com/
- United States Computer Emergency Readiness Team (US-CERT)
  www.us-cert.gov/
- InfraGard **www.infragard.org/**
- U.S. Secret Service Electronic Crimes Task Force
  www.secretservice.gov/ectf.shtml
- The Top Cyber Threat Intelligence Feeds
  www.thecyberthreat.com/cyber-threat-intelligence-feeds/

Resources

Cybersecurity Awareness

- FFIEC IT Examination Handbooks
  http://ithandbook.ffiec.gov
- FFIEC Cybersecurity Awareness
  http://ffiec.gov/cybersecurity.htm
- FDIC Financial Institution Letters
  www.fdic.gov/regulations/resources/director/risk/it-security.htm

Directors' Resource Center

Cybersecurity Awareness

- Directors' Resource Center
  www.fdic.gov/regulations/resources/director/

- Technical Assistance Video Program
  - Information Technology (IT)
  - Corporate Governance
  - Third-Party Risk
  - Cyber Challenge: A Community Bank Cyber Exercise

- Questions
  supervision@fdic.gov