FDIC

FEDERAL DEPOSIT INSURANCE CORPORATION

Cybersecurity Awareness

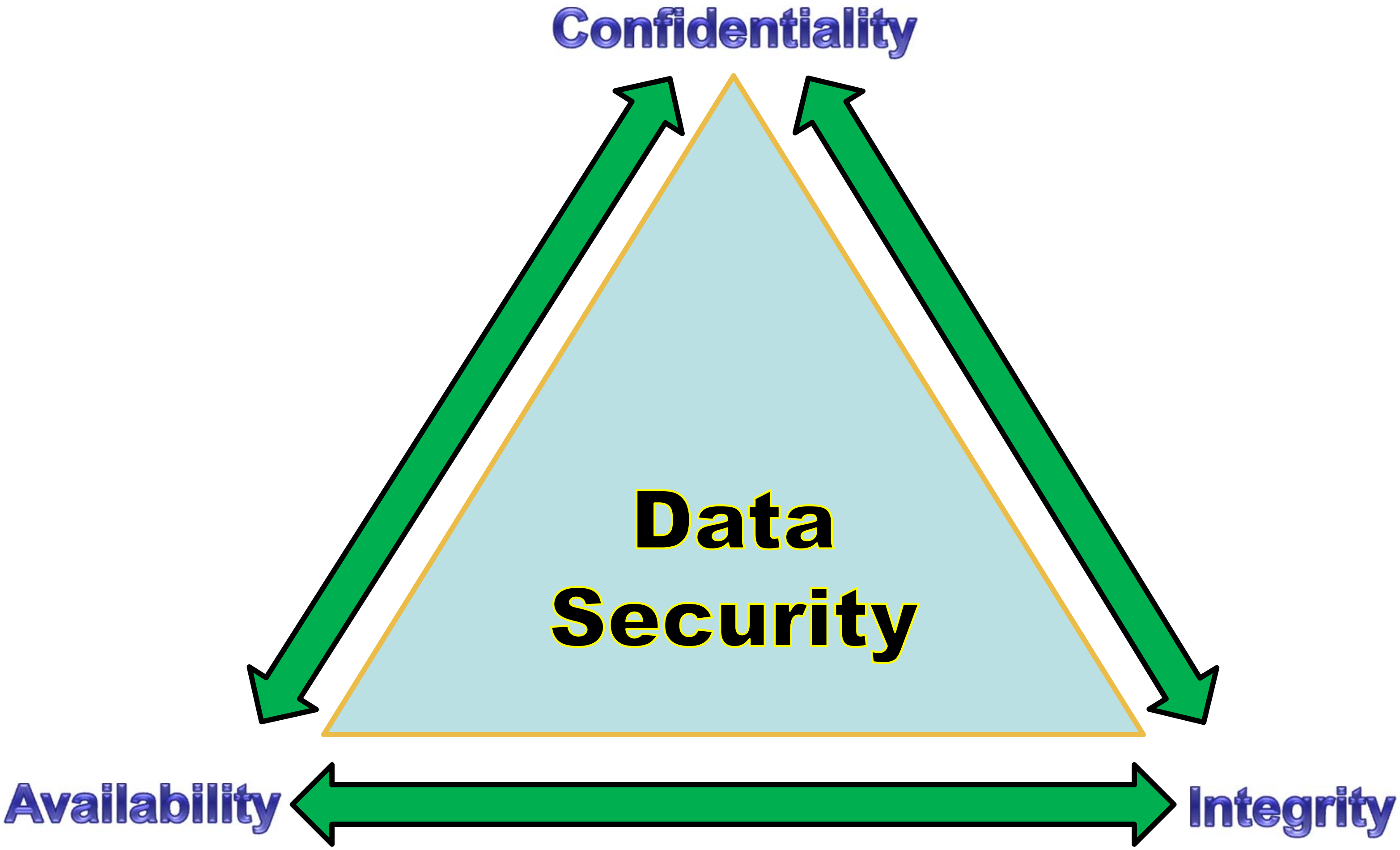
Objectives

Cybersecurity

- Discuss the Evolution of Data Security
- Define Cybersecurity
- Review Threat Environment
- Discuss Information Security Program Enhancements for Cyber Risk
  - Threat Intelligence
  - Third-Party Management
  - Resilience
  - Incident Response
- Describe Cybersecurity Assessment Tool

Evolution of Data Security

Cybersecurity



Evolution of Data Security

Cybersecurity

Evolution of Data Security

Cybersecurity

Definition

Cybersecurity

- The National Institute of Standards and Technology (NIST) defines cybersecurity as:

> "The process of protecting information by preventing, detecting, and responding to attacks."

- NIST Framework for Cybersecurity

Identify

Protect

Detect

Respond

Recover

Appendix B to Part 364

Cybersecurity

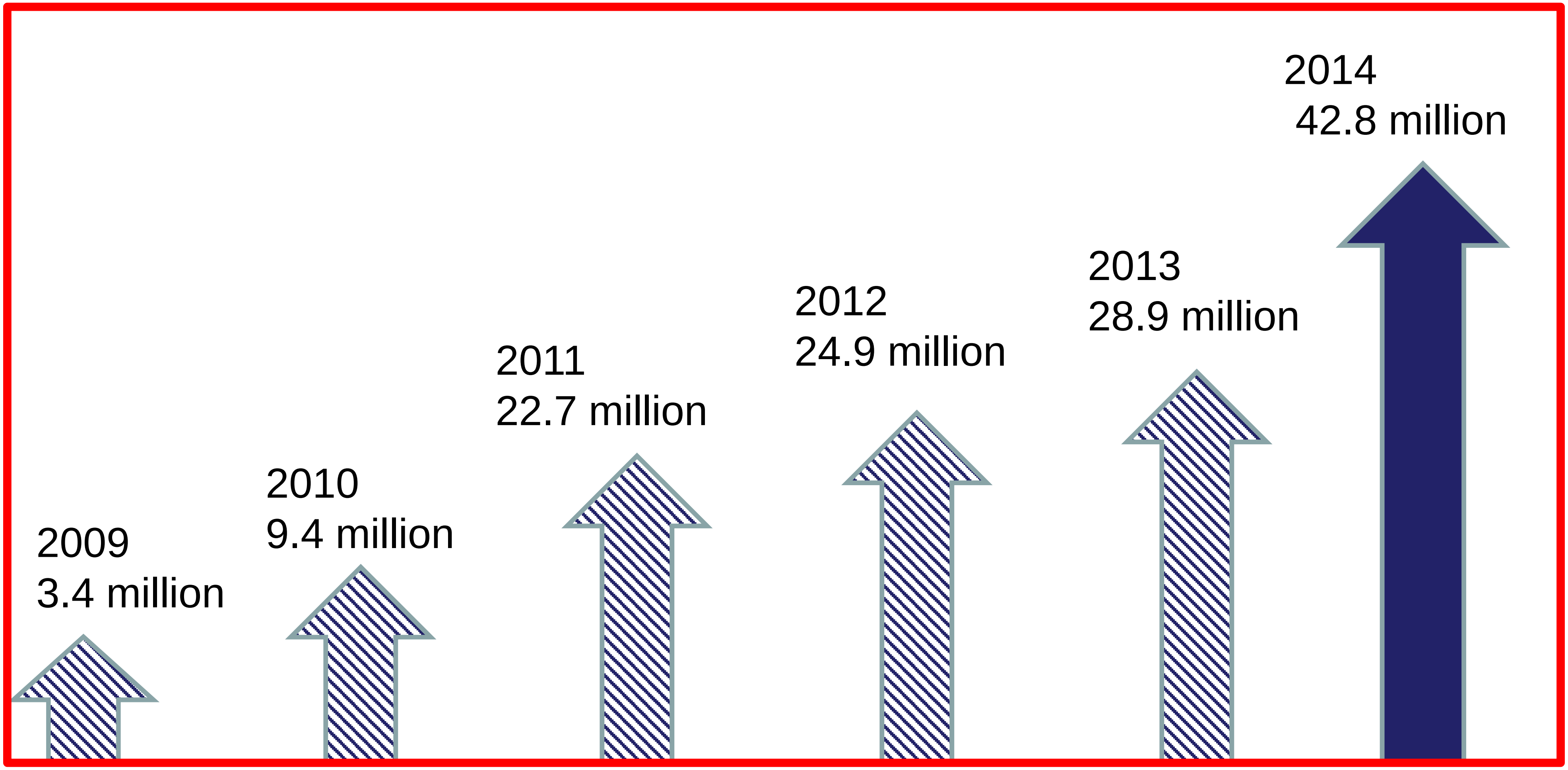
II. Standards for Information Security

- Ensure the security and confidentiality of customer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information;
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and
- Ensure the proper disposal of customer information and consumer information.

Information Security Incidents

Cybersecurity

2014 Information Security Incidents Up 48%



Source: PwC.com

Why Cybersecurity Is Important

Cybersecurity risks translate into business risks, and those risks can ultimately have a negative financial effect on the institution.

Data must be secured to safeguard the institution’s:

- Customer information,
- financial information, and
- reputation.

Cybersecurity is not just technology

- Cyber Risk needs to examine and adopt a holistic approach to:

- Policy – How regularly are policies:
  Created and Reviewed by the board,
  Updated after incidents and testing?

- Process – Are the appropriate resources & steps in place to:
  Record the event (simulated or real)
  Take appropriate action
  Maintain chain of evidence
  Record root cause, lessons learned, time to remediate

- People – Are they trained and tested regularly in:
  Cross-duty situations?
  Appropriate separation of duties?
  Internal threat awareness?

What Institutions Should Do

- Setting the tone from the top and building a security culture;
- Identifying, measuring, mitigating, and monitoring risks;
- Developing risk management processes commensurate with the risks and complexity of the institutions;
- Aligning cybersecurity strategy with business strategy and accounting for how risks will be managed both now and in the future;
- Creating a governance process to ensure ongoing awareness and accountability.

What institutions Should Do

(Continued)

- Ensuring timely reports to senior management that include meaningful information addressing the institution’s vulnerability to cyber risks.
- Practicing their response to a cyber event just as they do for a physical event through their business continuity plan.
- Talking about cyber security with their staff and their customers.
- Establishing relationships with experts so institutions know who to call in the event of a problem (Regulator, local FBI contact)

People and Patches

Cybersecurity

"…a campaign of just ten e-mails yields a greater than 90% chance that at least one person will become the criminal's prey…"

"…11% of recipients of phishing messages click on attachments."

Source: Verizon 2015 Data Breach Investigations Report

People and Patches

Cybersecurity

"99.9% of the exploited vulnerabilities had been compromised more than a year after the associated [patch] was published."

"Ten [vulnerabilities] accounted for almost 97% of the exploits observed in 2014."

"In 2014, there were 7,945 security vulnerabilities identified. That is 22 new vulnerabilities a day. Nearly one an hour."

Sources: Verizon 2015 Data Breach Investigations Report
NopSec

Threat Environment

Cybersecurity

Increasing Inherent Risk

- Growing Vulnerabilities
  - Interconnected systems
  - New delivery channels
  - Legacy products
  - Emerging/Unknown
- Increasing Threats
  - Number/types of actors
  - Nature/volume of attacks
  - Level of sophistication
  - Emerging/Unknown

Threat Environment: Vulnerabilities

Cybersecurity

- Technological
  - Weakness in hardware, software, network, or system configurations
- Organizational
  - Lack of awareness of threats/vulnerabilities, incomplete asset inventories, weaknesses in/over-reliance on third parties
- Human
  - Exploitation of human behavior such as trust and curiosity
  - Lack of effective security awareness training
- Physical
  - Theft, tampering, device failure, or introduction of infected media

Threat Environment: Actors

Cybersecurity

- Cyber Criminals - Financially motivated; attacks include account takeovers, ATM cash-outs, and payment card fraud.
- Nation States - Attempt to gain strategic advantage by stealing trade secrets and engaging in cyber espionage.
- Hacktivists - Maliciously use information technologies to raise awareness for specific causes.
- Insiders - Abuse their position and/or computer authorization for financial gain or as a response to a personal grievance with the organization.

Threat Environment: Attacks

Cybersecurity

- Malware/Destructive Malware
  - e.g., Key Loggers, Trojans, Ransomware, Wiper
- Phishing/Spear Phishing
- Distributed Denial of Service (DDoS)
- Compound Attacks
  - e.g., DDoS/Corporate Account Takeover, Phishing/Trojan
- The Unknown

Threat Environment: Example

Cybersecurity

Email

An employee within the targeted organization receives an email with malware

People

Installation

Upon opening the attachment, the Trojan/malware is installed

Patches

Execution

Trojan establishes communication to the attacker and downloads malware

Detection

- Account Takeover
- Ransomware
- Data Theft
- Data Destruction

Potential Concerns

Information Security + Cybersecurity

As noted in several recent FFIEC Cybersecurity press releases, many of the building blocks for an effective cybersecurity program are similar to those for any well-planned information security risk management program, including controls to prevent, detect, and respond to threats.

Information Security

"Information security is the process by which an institution protects and secures its systems, media, and facilities that process and maintain information vital to its operations. "

(SOURCE: FFIEC IT Handbooks – Information Security)

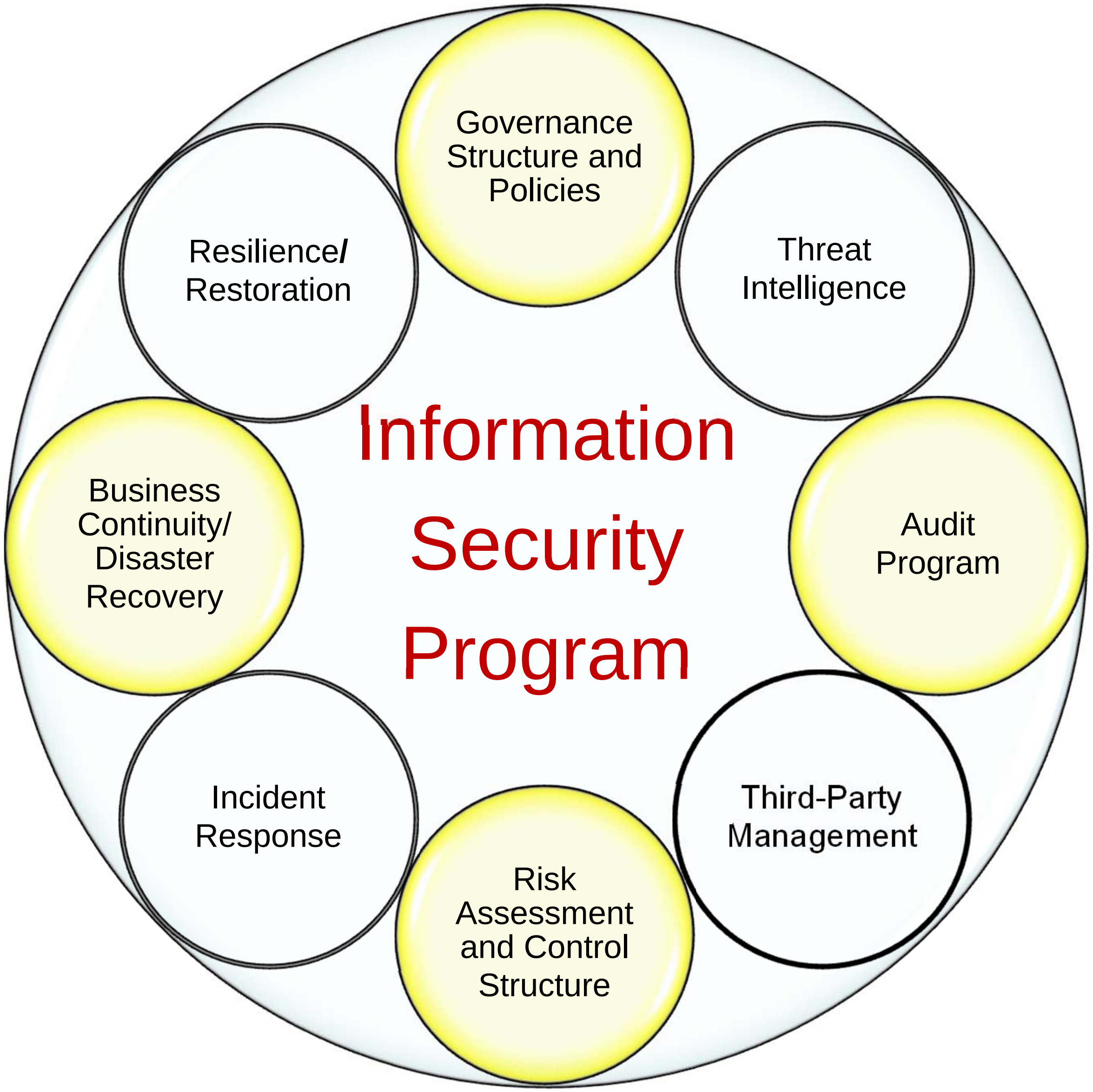
Cybersecurity

Cybersecurity is "the process of protecting information by preventing, detecting, and responding to attacks."

(SOURCE: National Institute of Standards and Technology (NIST) Framework

Information Security Program

Cybersecurity


Governance Structure and Policies
Threat Intelligence
Audit Program
Third-Party Management
Risk Assessment and Control Structure
Incident Response
Business Continuity/ Disaster Recovery
Resilience/ Restoration
Information Security Program

Governance/Structure/Policies

- Board and Senior Management Responsibilities and Duties
  - Ensure strategic planning and budgeting provide sufficient resources.
  - Provide sufficient authority, resources, and independence for information security.
  - Ensure policies and procedures address cybersecurity.
  - Incorporate cyber risk into the risk-based audit plan.
  - Provide reporting that assures the Board the ISP is working and included cybersecurity.

- Cyber Risk is a Business Risk!

Governance/Structure/Policies

- Cybercrime costs estimated $445B each year (Lohrmann, 2015)
- Internal threat riskier than external attack (Schneier, 2008)
- Payment systems are targeted focus of attack (Fischer, 2014)

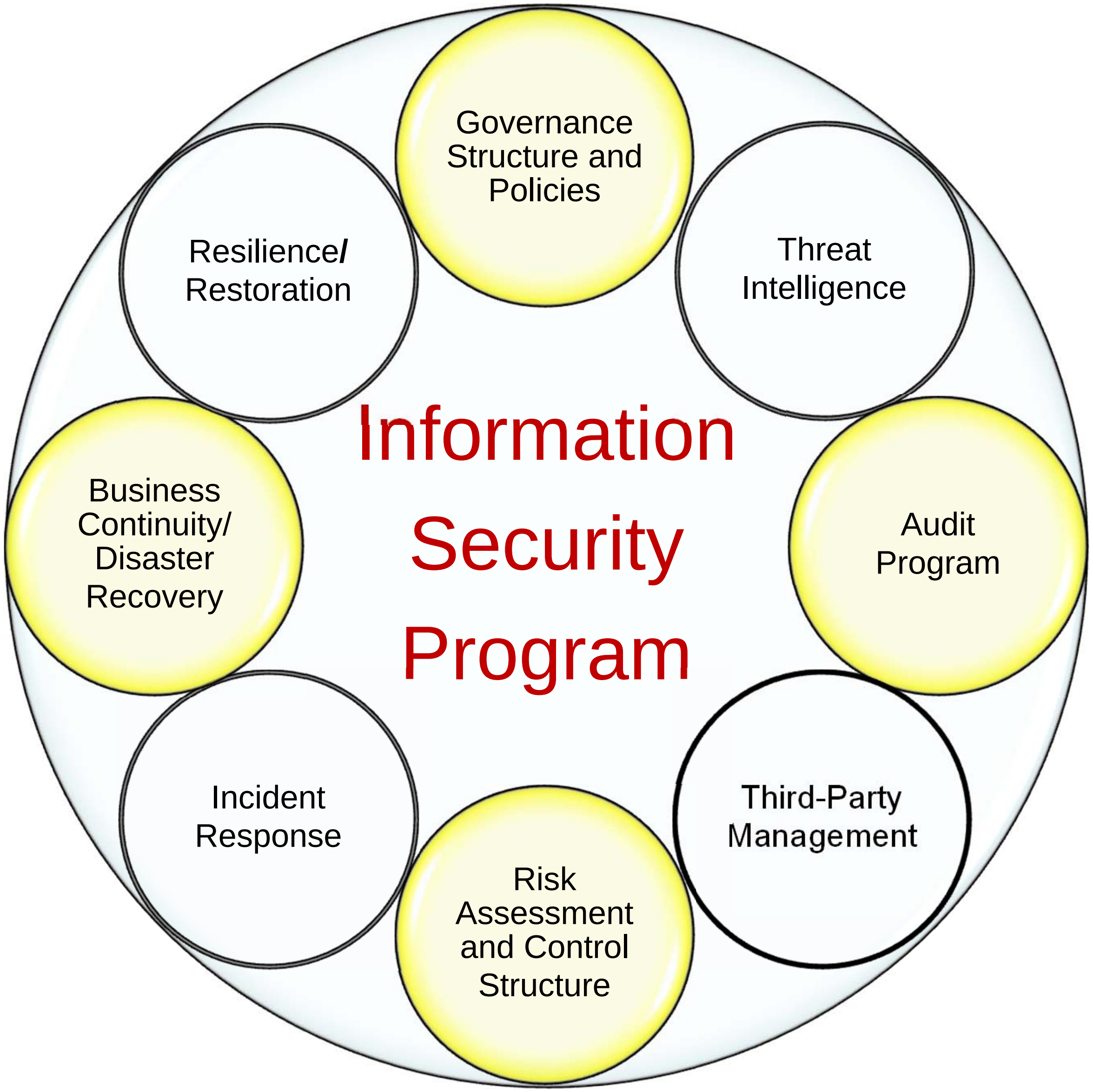
- Enterprise and Cloud systems underlie all transactions
- Probability isn't a question any more – when breached, not if

- Impact includes more than just monetary loss:
  Goodwill • Data Integrity
  Reputation • Lawsuits
  Criminal Action • Insolvency

- CRO and Risk Committees need to include cyber risk in every risk analysis – prioritize cyber as key threat vector

Information Security Program

Cybersecurity



Governance Structure and Policies

Threat Intelligence

Audit Program

Third-Party Management

Risk Assessment and Control Structure

Incident Response

Business Continuity/ Disaster Recovery

Resilience/ Restoration

Information Security Program

Risk Assessment

- Governance and accountability
- Enterprise-wide asset inventory
- Multi-disciplinary approach
- Threat analysis including cyber risks
- Identify inherent risk, determine controls, quantify residual risk
- Assesses changes in technology, operations, and cyber threat environment

Risk Assessment

- 80% of boards do not review risks at each meeting
- The majority of board's risk committees don't review cybersecurity plans at all (51%)
- Most cyber budgets are 1% of revenues or less
- More than 1/3 of banks didn't have a CISO
- 73% of boards were not conversant on cyber issues
- Boards assumed vendors had sufficient protections, and were moderately to heavily dependent upon them

Control Structure

- Cyber Hygiene
  - Security Awareness Training
  - Patch Management
  - Information Security Staff
  - Access Controls (Privileged Access)
  - Authentication
  - Detection Programs

Control Structure

- Encryption or Tokenization should cover:
  - Data at Rest
  - Data in Transit
  - Data in Process

- Separation of Duties should ensure data administrators and key managers are not same person

- Key management role should be held by the bank, not service provider, not shared

- Need to ensure minimal impact to business functionality

Control Structure

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

“Think Before You Click”

Control Structure

- Patch Management
  - Formal written policy and procedures
    - Develop system for identifying, prioritizing, applying, and testing patches
    - Create/maintain asset inventories
      - Software (Microsoft and Non-Microsoft)
      - Firmware (routers and firewalls)
    - Integrate threat intelligence
    - Mitigate risk from unsupported operating systems and applications
    - Report to board and senior management
    - BE TIMELY
  - IT Audit and internal reviews should validate

Control Structure

- Information Security Staff
  - Evaluate Staffing Adequacy
  - Organizational Chart
    - Independent functions
  - Job Descriptions
  - Certifications
    - e.g., Microsoft Certified Professional, CCNA, CISA, CISSP
  - Annual Training
    - Internal Training
    - External Training: e.g., ISACA, MISTI, Learning Tree, RSA Conference, NACHA Conference

Education isn't an annual test

- Cyber Risk needs a standard curriculum
  - Similar to investment analysis and risk management
  - Needs to be regular, repeated, required, refined
- Boards need to focus on known and emerging risks
- Preparation for the breach should be well established
- Acknowledgement that the incident could be caused either by internal or external actors is a key issue
- All aspects of technology, policy and processes should be included

Control Structure

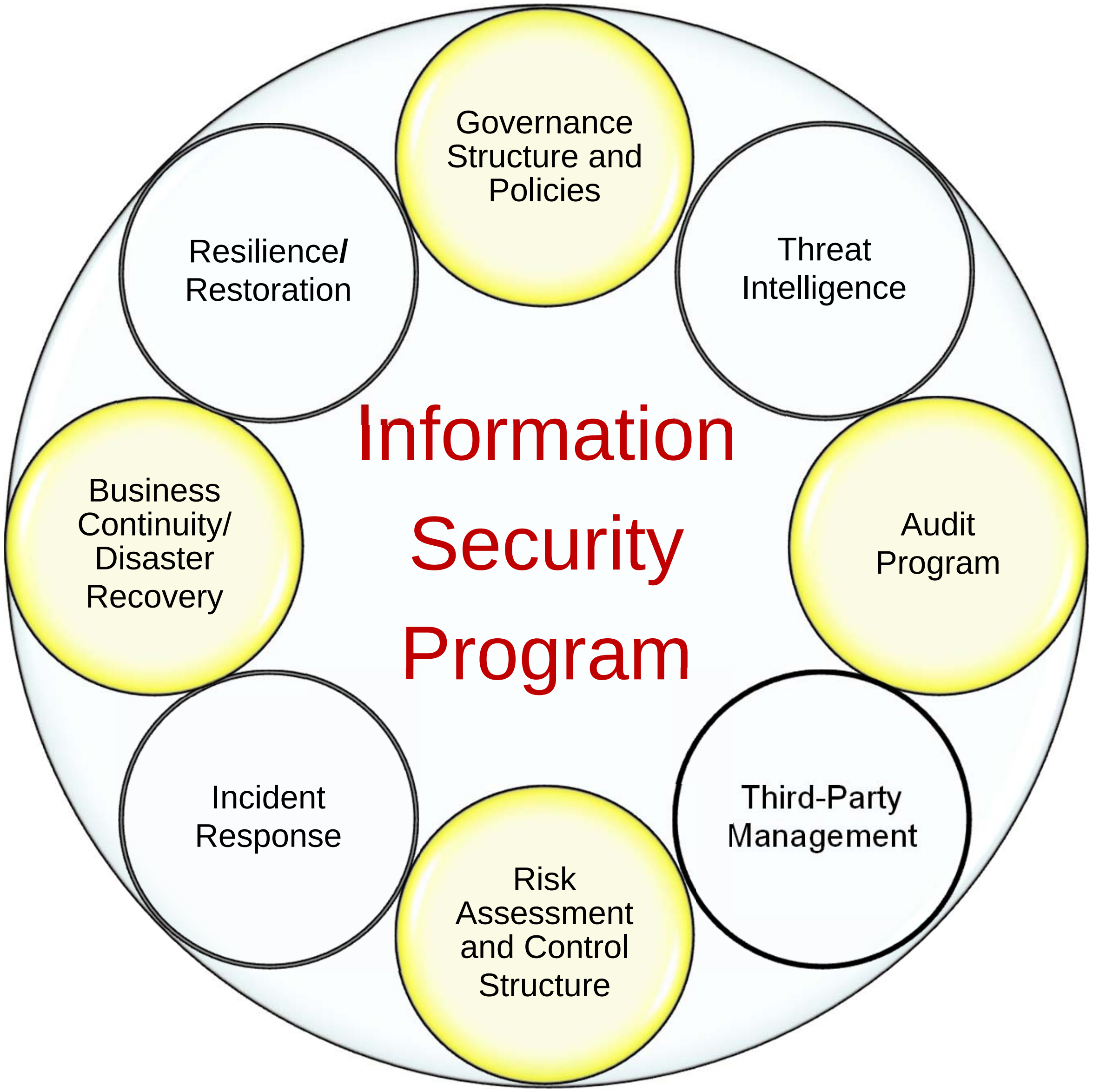
- Access Controls
  - Administered by an independent group
  - Emphasis on review of privileged access
  - Annual or regular, independent review of user access

Control Structure

- Detection Programs
  - Anti-virus Software/Malware Detection
  - Intrusion Detection/Intrusion Prevention
  - Activity Logging
    - Systems
    - Frequency/Content/Retention
    - Review/Automation
    - Reporting

Information Security Program

Cybersecurity



Governance Structure and Policies

Threat Intelligence

Audit Program

Third-Party Management

Risk Assessment and Control Structure

Incident Response

Business Continuity/ Disaster Recovery

Resilience/ Restoration

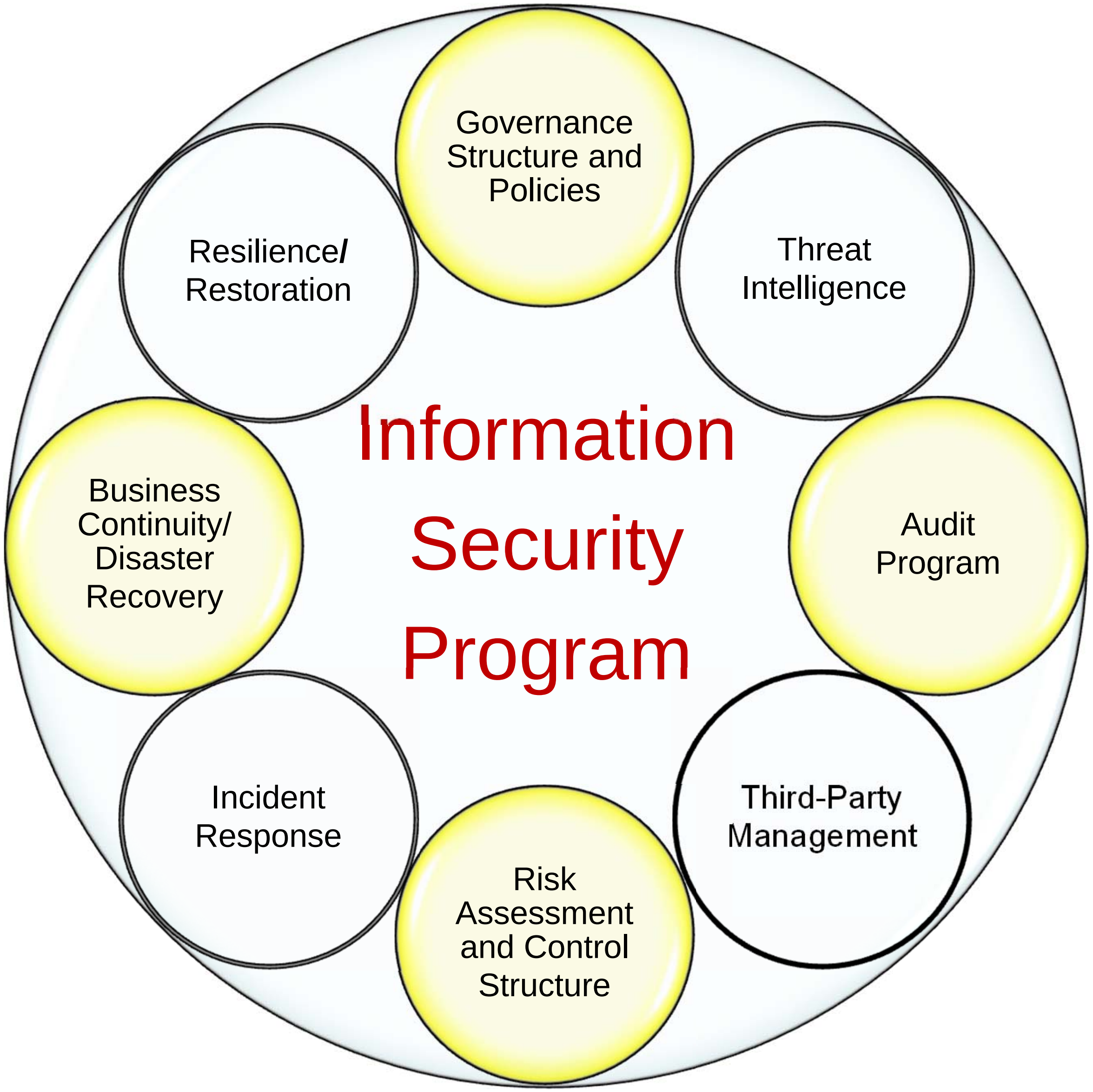
Information Security Program

Disaster Recovery/Business Continuity Planning

- Ensure cyber threats are added to business impact analysis (BIA)
  - Include probability and impact to critical applications and systems identified in BIA
- Ensure cyber threats identified in BIA are incorporated in recovery plans
- Include cyber scenarios in business continuity tests

Information Security Program

Cybersecurity


Governance Structure and Policies
Resilience/ Restoration
Threat Intelligence
Information Security Program
Business Continuity/ Disaster Recovery
Audit Program
Incident Response
Third-Party Management
Risk Assessment and Control Structure

Audit

Program
Charter/Policy
Committee
Universe (Scope) • Risk Assessment • Cybersecurity
Plan/Budget
Reporting
Findings/Tracking

Types
General Controls
GLBA
Vulnerability Assessment
Penetration Test
ACH/Wires
Social Engineering

Cyber Insurance – Necessary?

- Banks should ensure they have appropriate D&O and cyber coverage to include all areas of impact

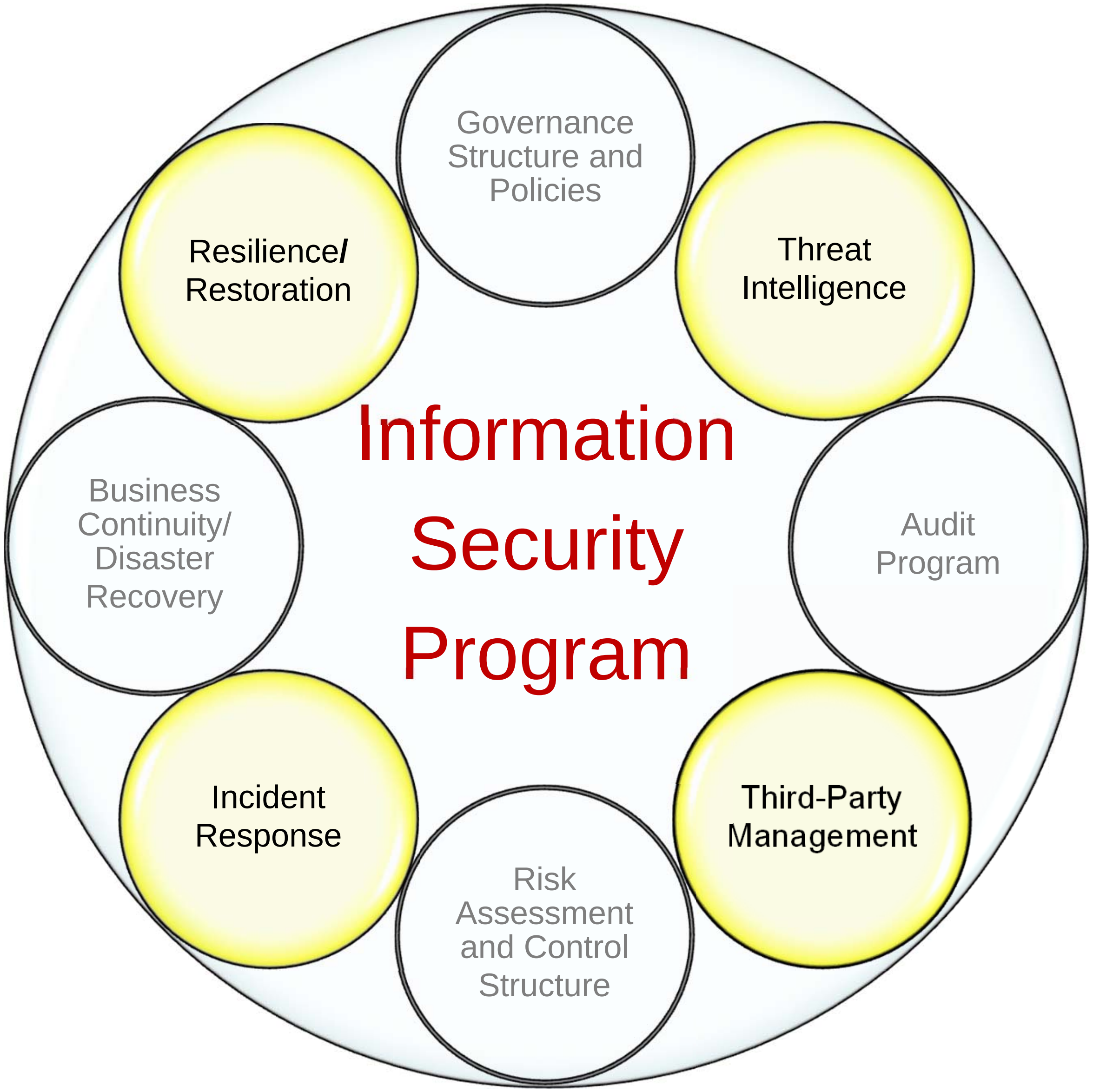
  Ensure PR and Disclosure remediation efforts are included in the costs, as they can endure beyond technology resolution requirements

  Ensure fiduciary duty and class-action litigation are also covered if caused by cyber incidents

  Forensics & Incident Response that ensures chain of evidence & responsibility to ensure due care should be included in the cyber plan to include appropriate insurance

Information Security Program: Refocused

Cybersecurity



Information Security Program

Governance Structure and Policies

Threat Intelligence

Audit Program

Third-Party Management

Risk Assessment and Control Structure

Incident Response

Business Continuity/ Disaster Recovery

Resilience/ Restoration

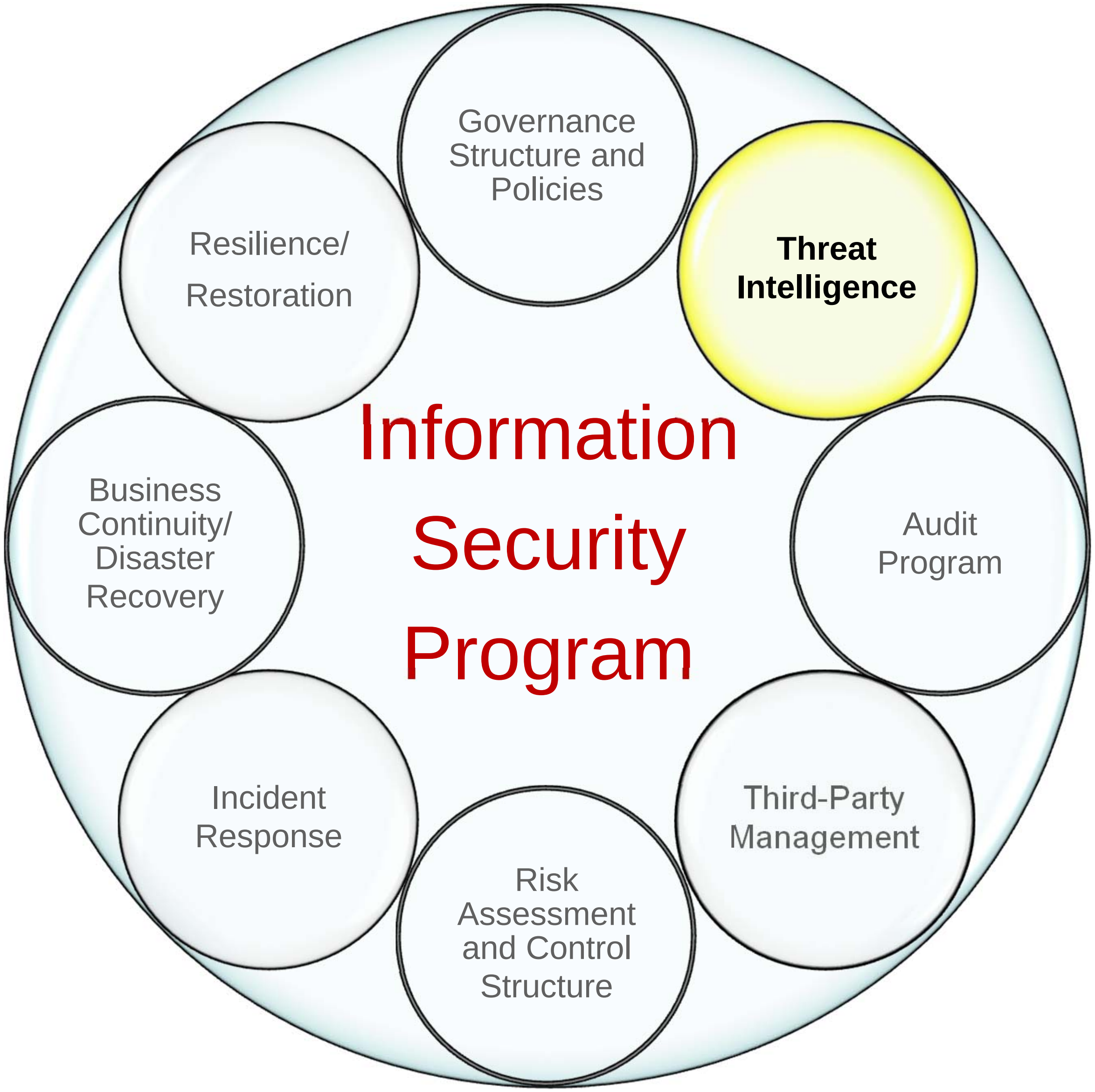
Information Security Program: Refocused

Cybersecurity

- **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 Handbook, Appendix J released on February 6, 2015 – Strengthening the Resilience of Outsourced Technology Services**

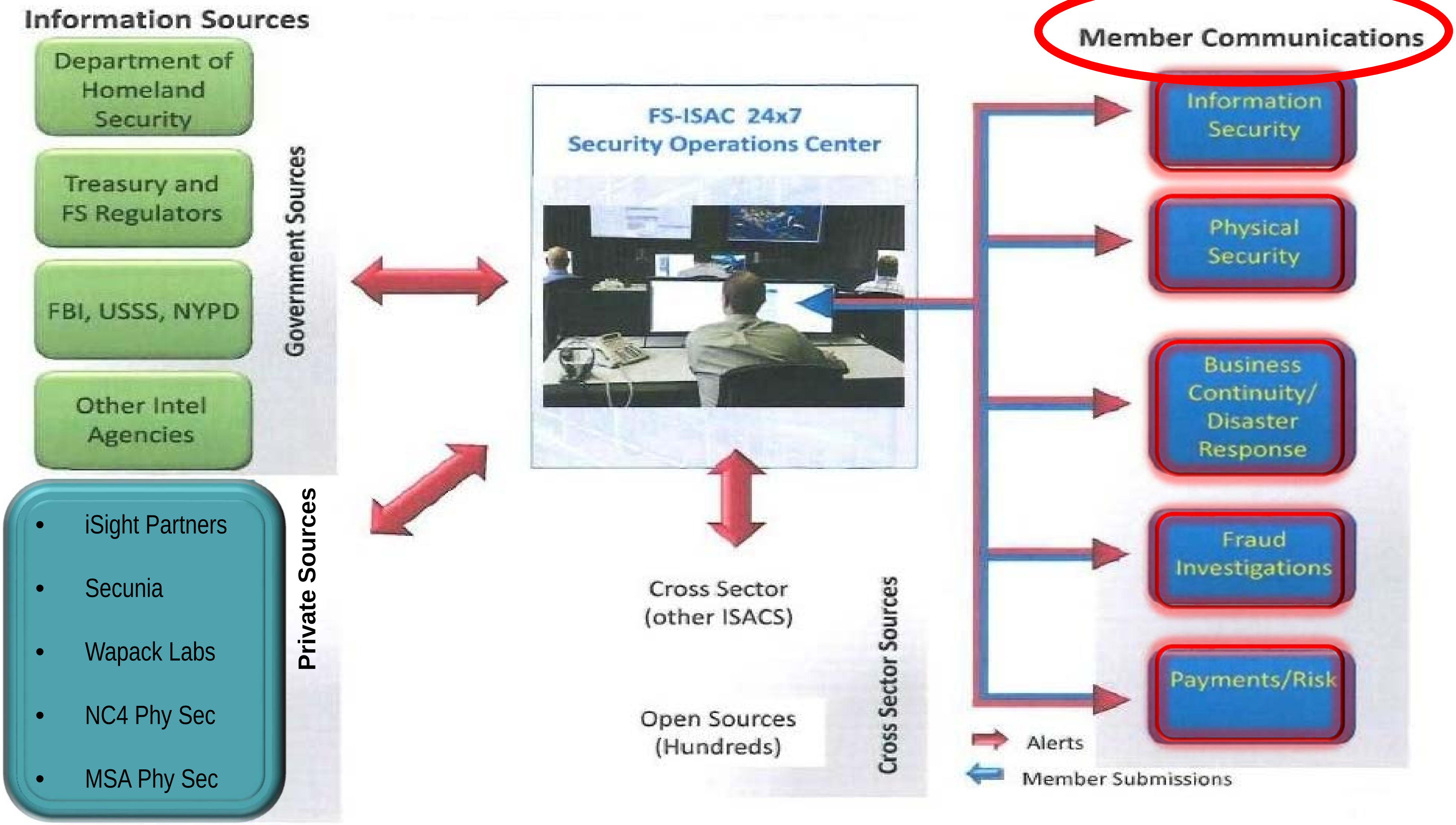
Information Security Program: Refocused

Cybersecurity


Governance Structure and Policies
Threat Intelligence
Audit Program
Third-Party Management
Risk Assessment and Control Structure
Incident Response
Business Continuity/ Disaster Recovery
Resilience/ Restoration
Information Security Program

Threat Intelligence: FS-ISAC

Cybersecurity



Information Sources

Department of Homeland Security

Treasury and FS Regulators

FBI, USSS, NYPD

Other Intel Agencies

Government Sources

- iSight Partners
- Secunia
- Wapack Labs
- NC4 Phy Sec
- MSA Phy Sec

Private Sources

FS-ISAC 24x7 Security Operations Center

Cross Sector (other ISACS)

Open Sources (Hundreds)

Cross Sector Sources

Member Communications

Information Security

Physical Security

Business Continuity/ Disaster Response

Fraud Investigations

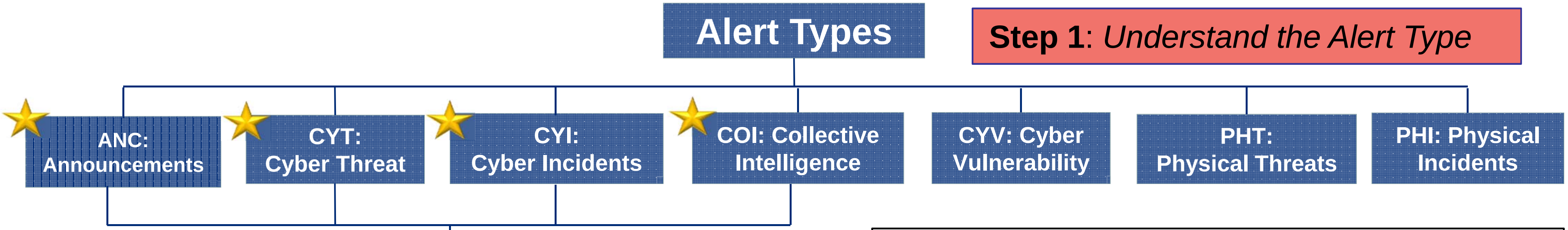
Payments/Risk

Alerts

Member Submissions

Threat Intelligence: FS-ISAC

Cybersecurity



Alert Types

Step 1: *Understand the Alert Type*

★ ANC: Announcements

★ CYT: Cyber Threat

★ CYI: Cyber Incidents

★ COI: Collective Intelligence

CYV: Cyber Vulnerability

PHT: Physical Threats

PHI: Physical Incidents

Depending on your role, you don't have to follow every update, but FS-ISAC recommends following these key reports. Doing so will limit emails to about 10/day.

Step 2: *Understand the Criticality and Priority*

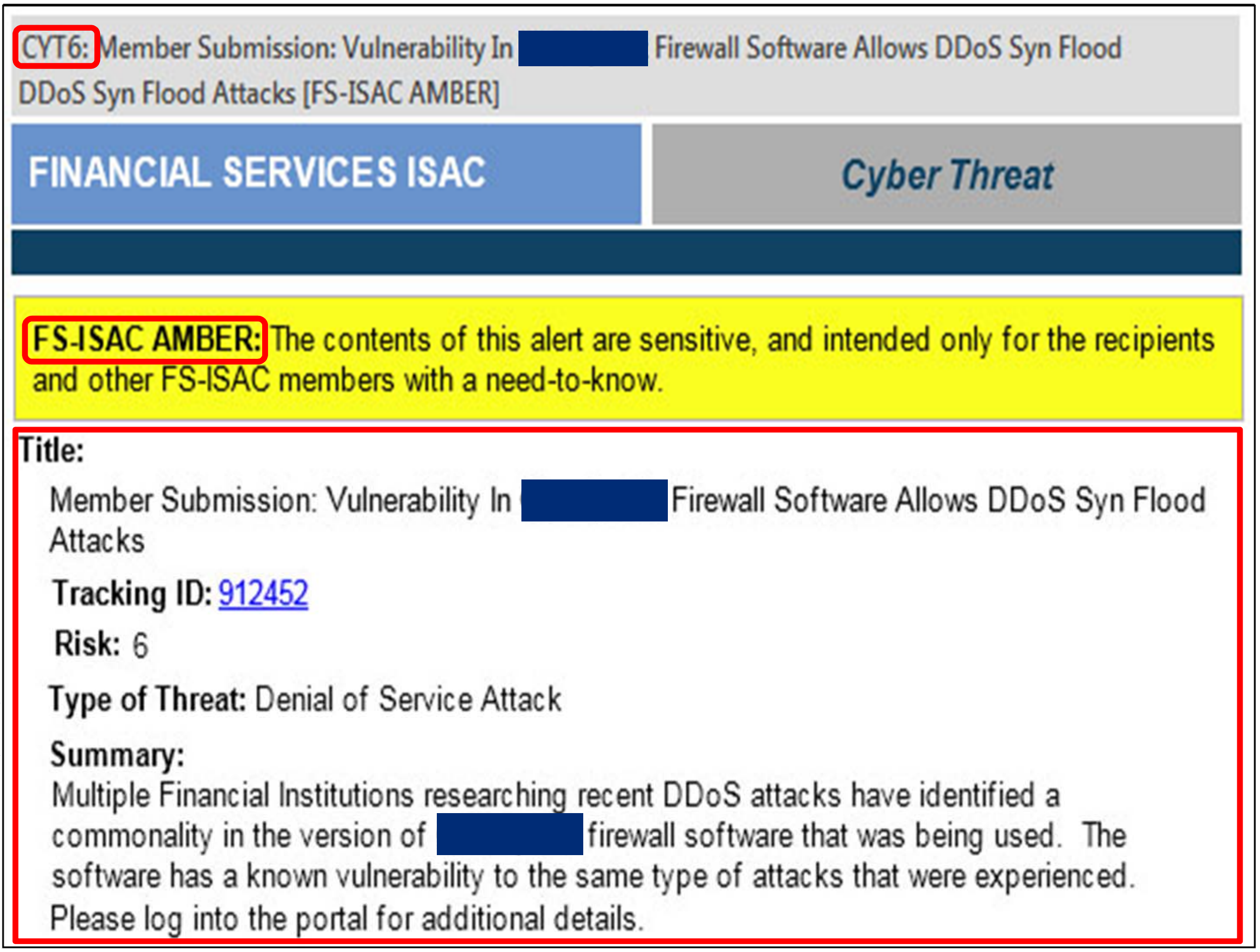
- ANC = Priority 1-10, 8-10 is high priority
- CYT = Risk 1-10, 8-9 is Urgent, 10 is Crisis
- CYI = Risk 1-10, 8-9 is Urgent, 10 is Crisis
- COI = No Criticality Metric
- CYV = Risk 1-10, 8-9 is Urgent, 10 is Crisis
- PHT = Risk 1-10, 8-9 is Urgent, 10 is Crisis
- PHI = Informational, Minimal Impact,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

Step 3: *Make Choices Based on Role*

- Analysts and those involved in risk assessment or vulnerability/patch management should receive CYV alerts.
- Intelligence analysts may also want to participate on the Cyber Intel listserv. POCs are automatically added, but a portal account is not necessary if you wish to add additional analysts to the distribution
- Provide portal accounts to your staff based on each individual's role. This will allow them to employ portal filtering for their unique assignments
- Provide summary reports for mangers and technical reports for analysts. Making informed choices based on your role eliminates unneeded emails

Threat Intelligence: FS-ISAC Alert

Cybersecurity



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

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.

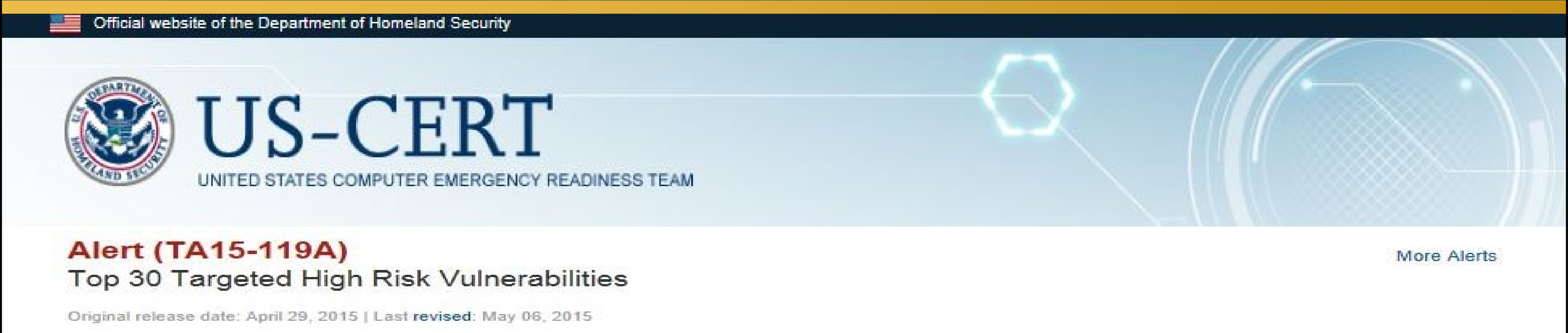
Be aware of FS-ISAC's Traffic Light Protocol.

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.**

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

Threat Intelligence: US-CERT Alert

Cybersecurity



Official website of the Department of Homeland Security

US-CERT

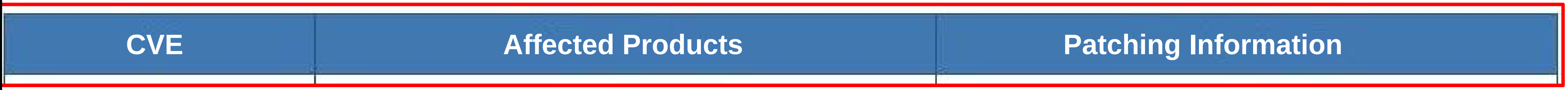
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Alert (TA15-119A)

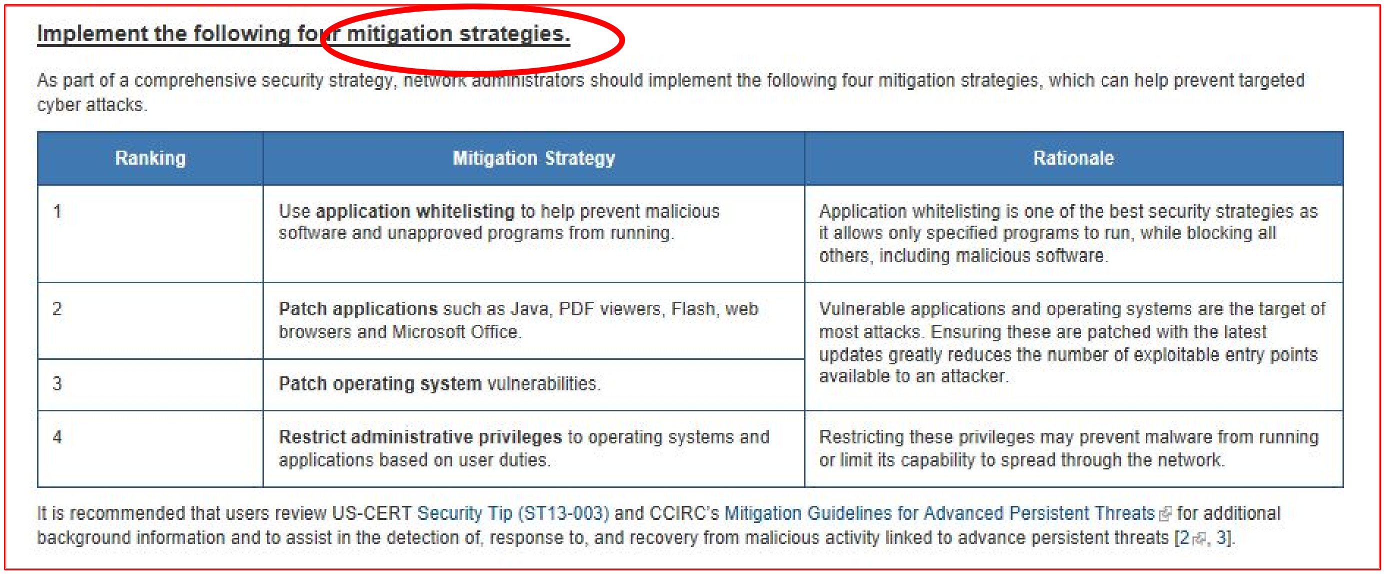
Top 30 Targeted High Risk Vulnerabilities

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].

Systems Affected …

Overview …

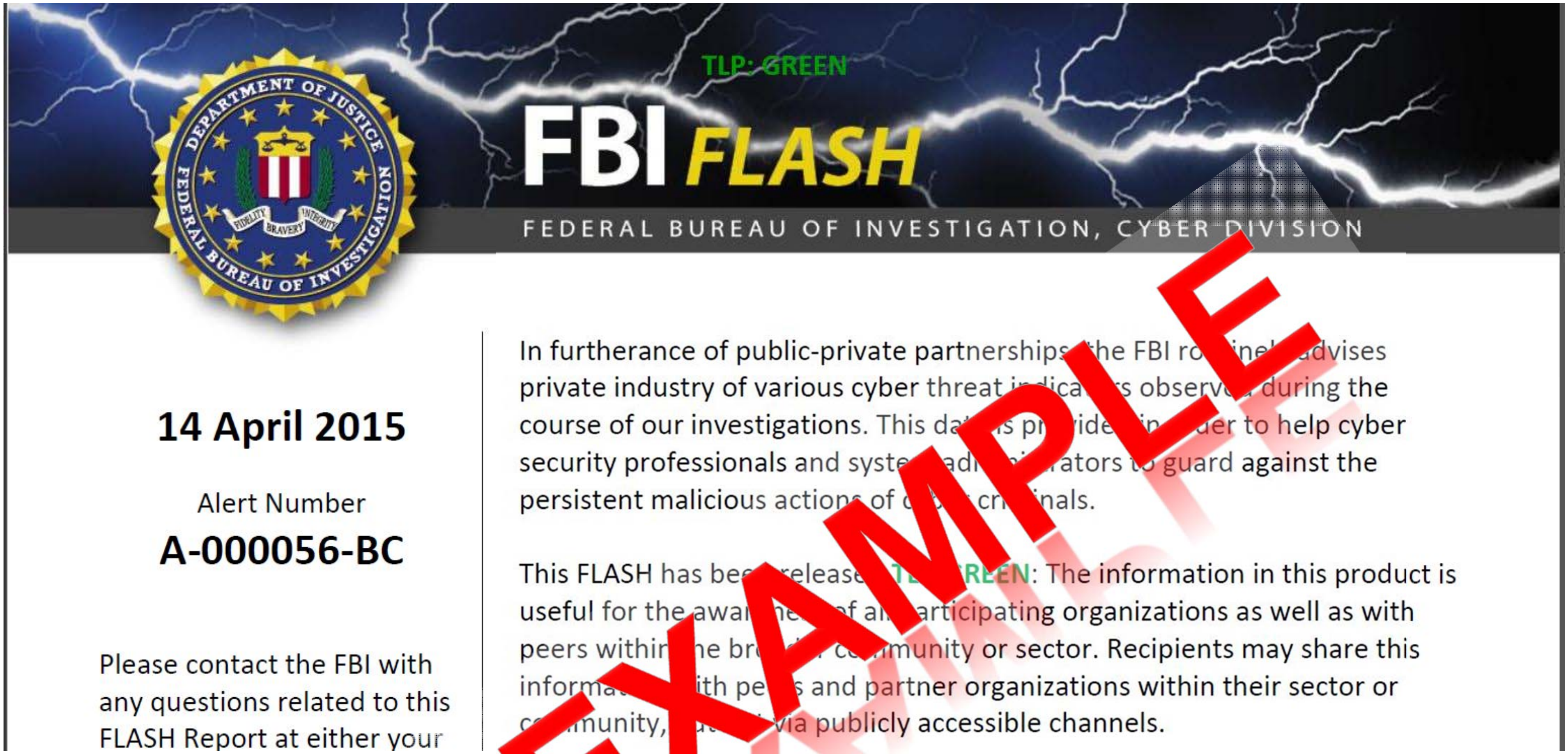
Description …

Impact …

Solution …

Threat Intelligence: FBI Flash Alerts

Cybersecurity



TLP: GREEN
FBI FLASH
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY

14 April 2015

Alert Number

A-000056-BC

Please contact the FBI with any questions related to this FLASH Report at either your

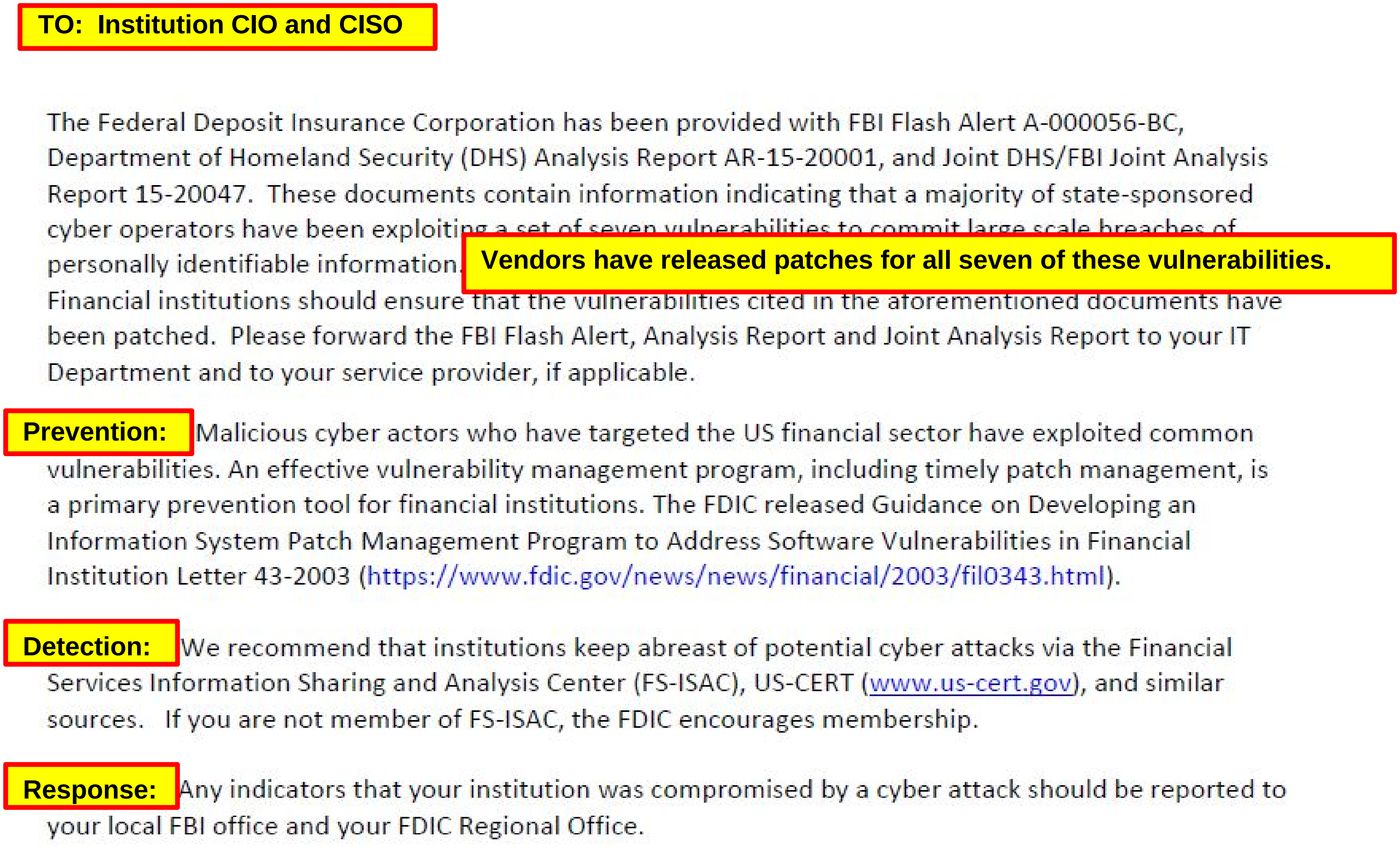
In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released TLP: GREEN: The information in this product is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

EXAMPLE

Threat Intelligence: FDIC Communications

Cybersecurity



TO: Institution CIO and CISO

The Federal Deposit Insurance Corporation has been provided with FBI Flash Alert A-000056-BC, Department of Homeland Security (DHS) Analysis Report AR-15-20001, and Joint DHS/FBI Joint Analysis Report 15-20047. These documents contain information indicating that a majority of state-sponsored cyber operators have been exploiting a set of seven vulnerabilities to commit large scale breaches of personally identifiable information. Financial institutions should ensure that the vulnerabilities cited in the aforementioned documents have been patched. Please forward the FBI Flash Alert, Analysis Report and Joint Analysis Report to your IT Department and to your service provider, if applicable.

Vendors have released patches for all seven of these vulnerabilities.

Prevention: Malicious cyber actors who have targeted the US financial sector have exploited common vulnerabilities. An effective vulnerability management program, including timely patch management, is a primary prevention tool for financial institutions. The FDIC released Guidance on Developing an Information System Patch Management Program to Address Software Vulnerabilities in Financial Institution Letter 43-2003 (https://www.fdic.gov/news/news/financial/2003/fil0343.html).

Detection: We recommend that institutions keep abreast of potential cyber attacks via the Financial Services Information Sharing and Analysis Center (FS-ISAC), US-CERT (www.us-cert.gov), and similar sources. If you are not member of FS-ISAC, the FDIC encourages membership.

Response: Any indicators that your institution was compromised by a cyber attack should be reported to your local FBI office and your FDIC Regional Office.

Threat Intelligence

Cybersecurity

External Sources

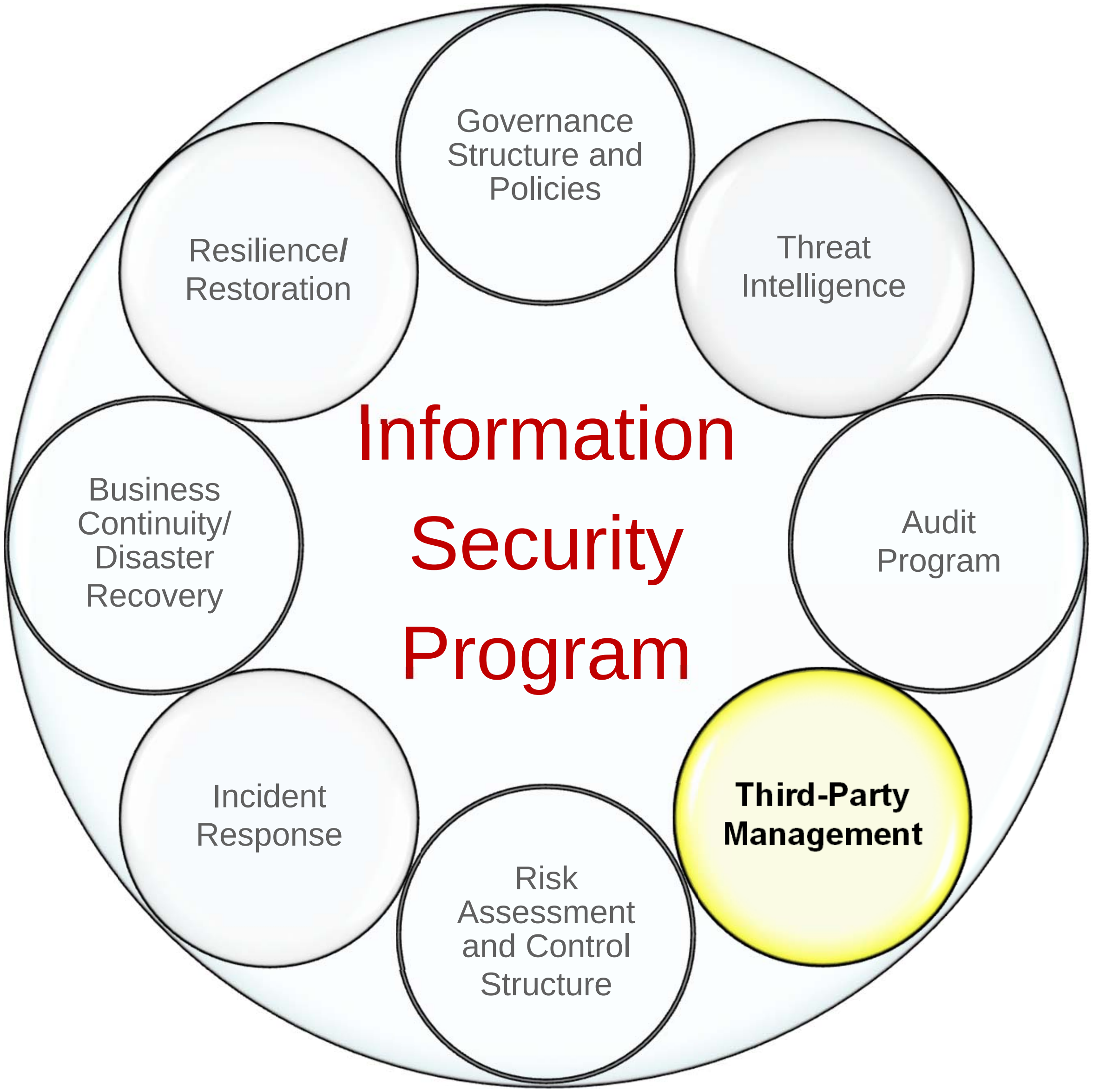
- FS-ISAC
- US-CERT
- Third-Party Servicers
  - e.g., core, telecommunications, managed security services

Internal Sources

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

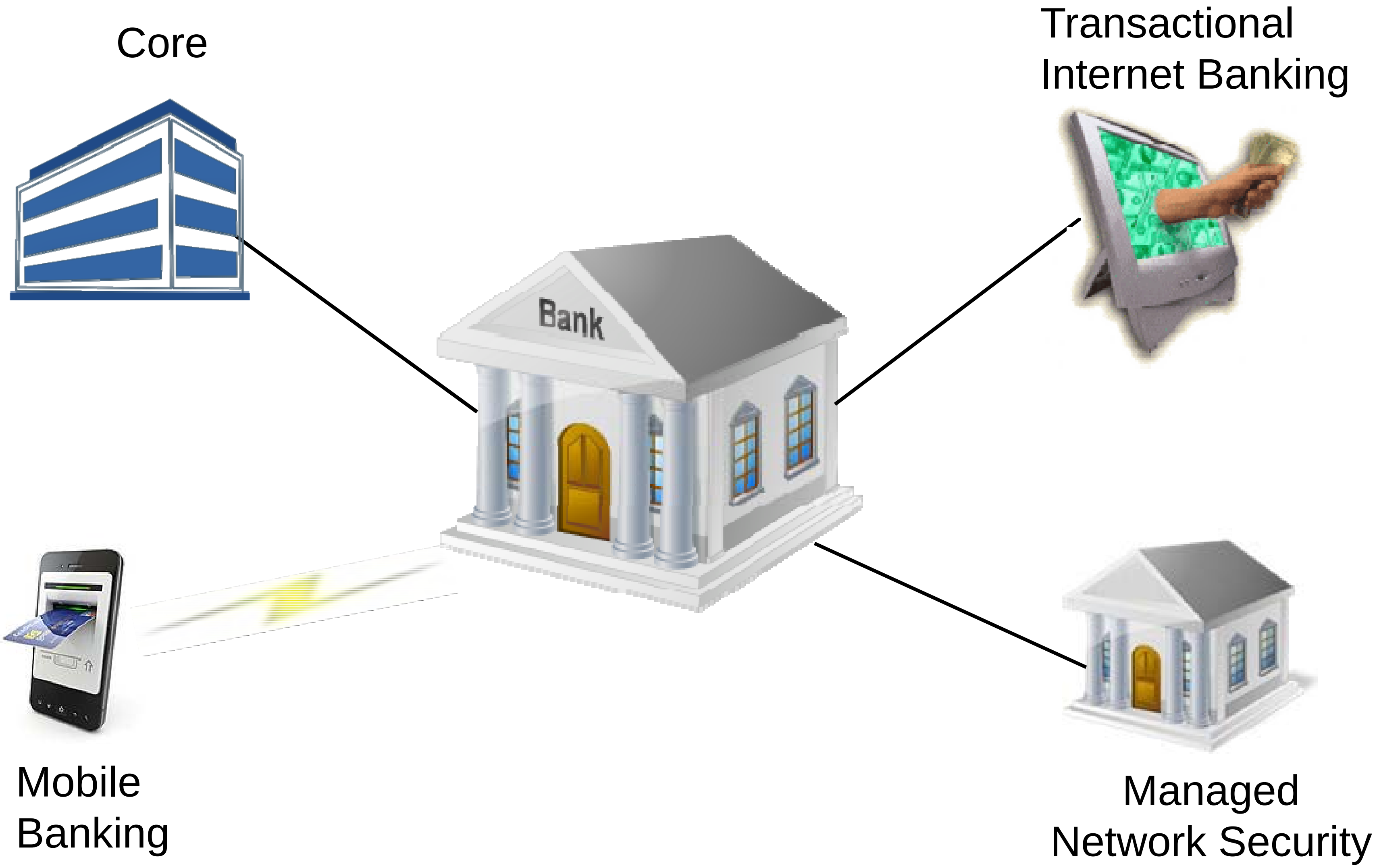
Information Security Program: Refocused

Cybersecurity


Governance Structure and Policies
Threat Intelligence
Audit Program
Third-Party Management
Risk Assessment and Control Structure
Incident Response
Business Continuity/ Disaster Recovery
Resilience/ Restoration
Information Security Program

Third-Party Management

Cybersecurity



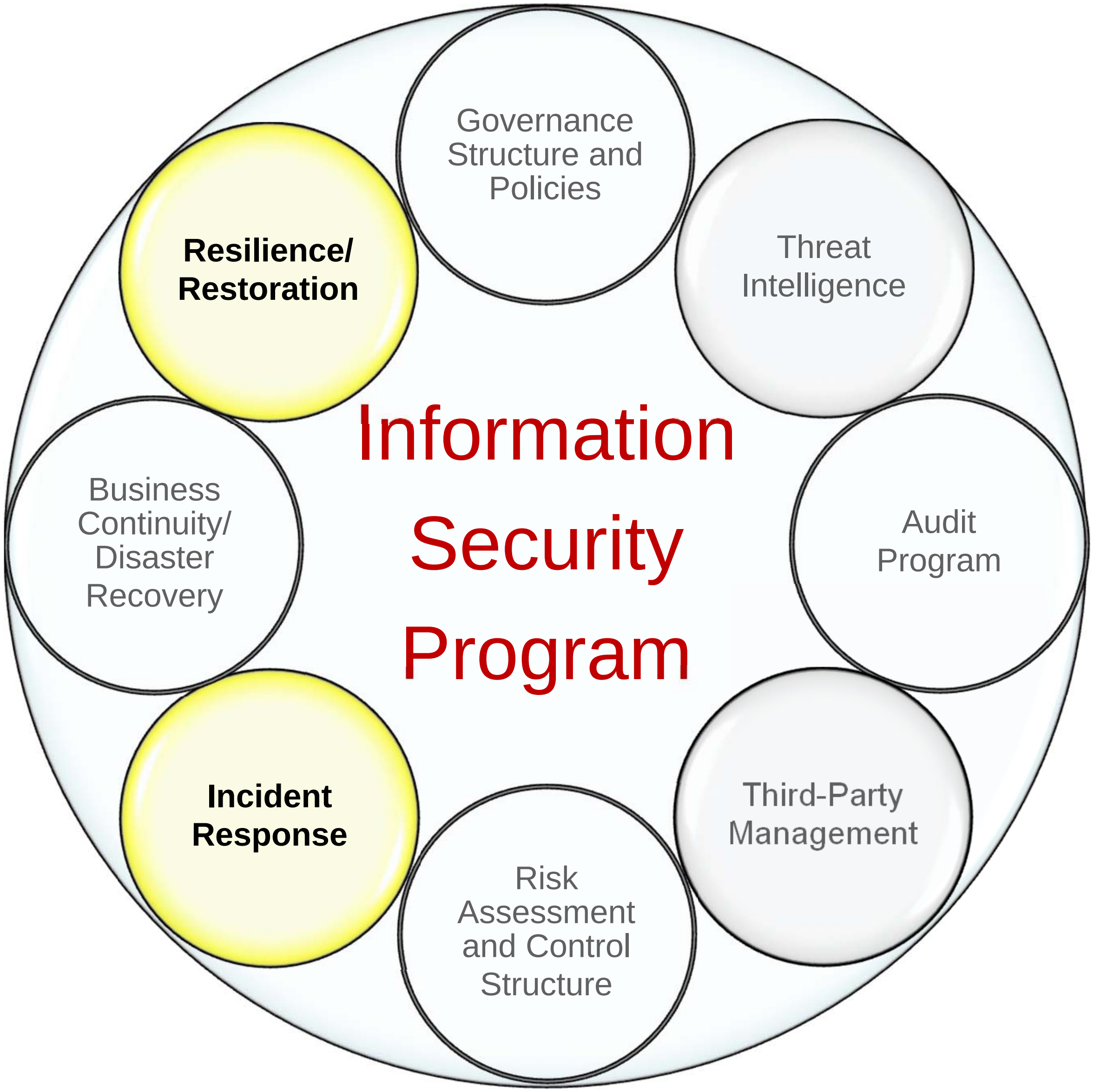
Appendix J: Third-Party Management

Cybersecurity

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

Information Security Program: Refocused

Cybersecurity


Governance Structure and Policies
Threat Intelligence
Resilience/ Restoration
Information Security Program
Business Continuity/ Disaster Recovery
Audit Program
Incident Response
Third-Party Management
Risk Assessment and Control Structure

Resiliency

- Banks are increasingly complex, adaptive systems
  - Need to leverage adversity to grow stronger
  - Anticipate incidents will happen
  - Respond and document root-cause, remediation
  - Correct issues, apply lessons learned holistically
- Adopt improved processes, training, methods
- Between incidents, audit, test, train and repeat
- Include all staff on simulations and tests
- Ensure cross training between duty assignments

Appendix J: Resilience

Cybersecurity

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

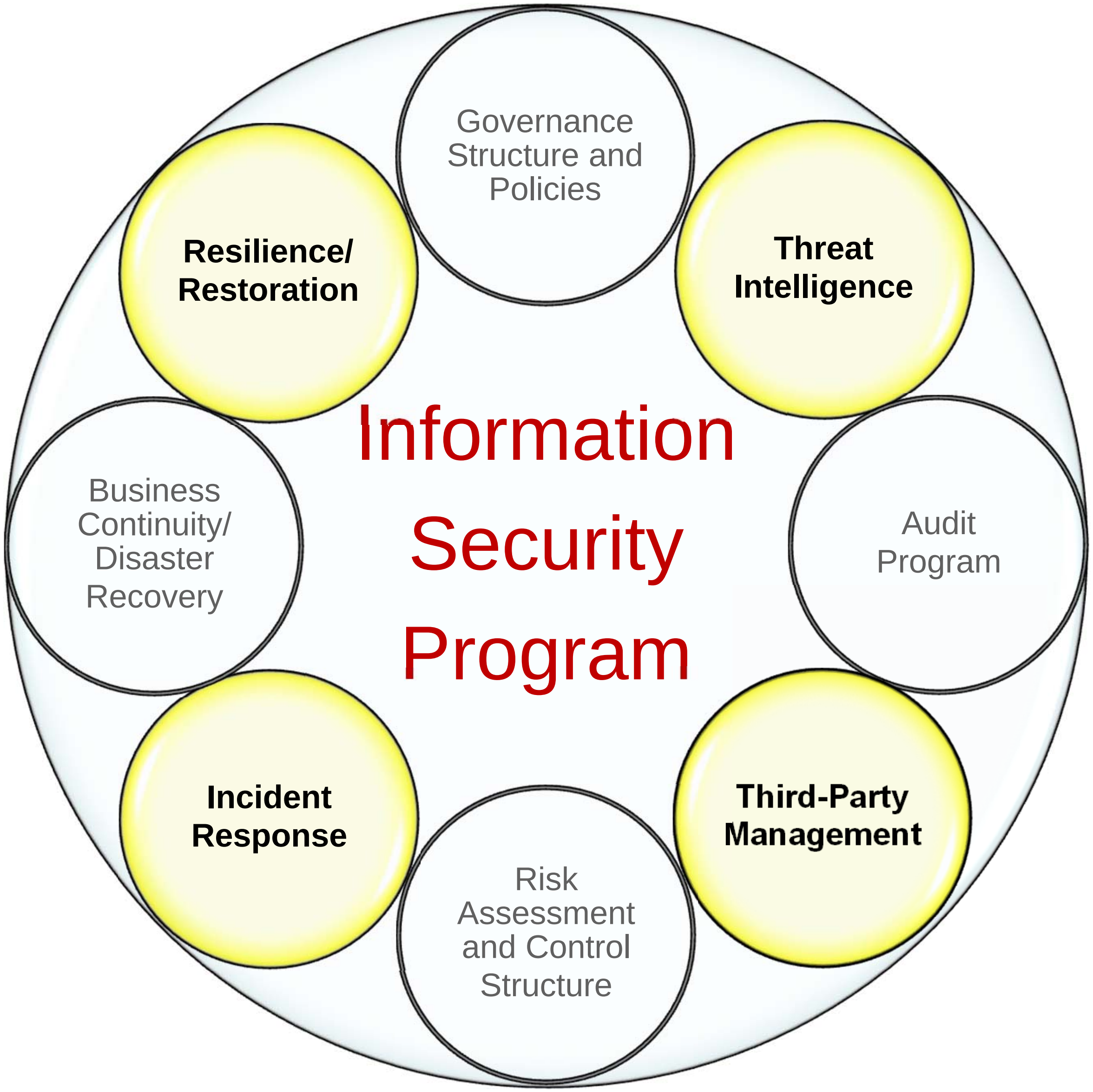
Appendix J: Incident Response

Cybersecurity

- **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


Governance Structure and Policies
Resilience/ Restoration
Threat Intelligence
Information Security Program
Business Continuity/ Disaster Recovery
Audit Program
Incident Response
Third-Party Management
Risk Assessment and Control Structure

FFIEC Cybersecurity Assessment Tool

Cybersecurity

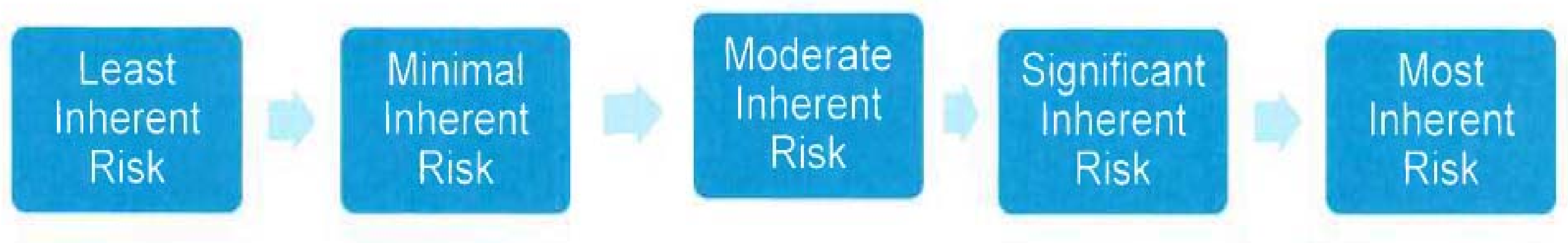
- FFIEC Press Release: Cybersecurity Assessment Tool, dated June 30, 2015
  - Voluntary tool to assist banks in identifying their risk profile and assessing their cybersecurity preparedness
  - Provides banks with a repeatable and measurable process to inform management of their institution’s risks and cybersecurity preparedness over time

Assessment Tool

- FFIEC created an assessment tool for banks (June 2015)
- First step on cyber-risk journey
- Includes Risk Profile and Maturity Assessment
- Directs CEOs and Boards towards Gaps and Risks
- Prescriptive steps are logical follow-on

  Need to work with banks to create action plans

  Gaps need to be more than goals, but funded efforts



Least Inherent Risk

Minimal Inherent Risk

Moderate Inherent Risk

Significant Inherent Risk

Most Inherent Risk

FFIEC Cybersecurity Assessment Tool

Cybersecurity

- **Inherent Risk Profile**
  - Technologies and Connection Types
  - Delivery Channels
  - Online/Mobile Products and Technology Services
  - Institution Characteristics
  - External Threats
- **Cybersecurity Maturity**
  - Cyber Risk Management and Oversight
  - Threat Intelligence and Collaboration
  - Cybersecurity Controls
  - External Dependency Management
  - Cyber Incident Management and Response

FFIEC Cybersecurity Assessment Tool

Cybersecurity

- Maturity Levels:
  - Baseline
  - Evolving
  - Intermediate
  - Advanced
  - Innovative

Cyber Incident Reporting

Cybersecurity

- RMS is updating its technology incident reporting guidance.
    - RD Memo 25-2001, Technology Incident Report
    - IT ViSION Help Document
- Interim procedures:
    - Report time sensitive, cyber incidents affecting critical operations of a bank or servicer provider to your appropriate IT Examination Specialist (ITES), Case Manager, or Regional management.
    - For significant incidents, the ITES should report the incident to the appropriate Washington Office RMS staff.
    - RMS staff should first consult with the Washington Office prior to reporting bank incidents to parties outside of RMS.
    - Record the incident in ViSION per outstanding guidance.

Future FFIEC Cybersecurity Focus

- Cybersecurity Self-Assessment Tool
- Incident Analysis
- Crisis Management
- Training
- Policy Development
- Technology Service Provider Strategy
- Collaboration with Law Enforcement and Intelligence Agencies

Evolution of Data Security

Cybersecurity

RISK MANAGEMENT PROGRAM

Summary

Cybersecurity

- Cybersecurity risks translate into business risks, and those risks can ultimately have a negative financial effect on the institution.
- The building blocks of an effective cybersecurity program are similar to those for any well-planned information security risk management program, including controls to prevent, detect, and respond to threats.
- Engagement by the board of directors and senior management to include understanding of the institution’s cybersecurity inherent risk is required.
- Management should Include discussion of cybersecurity issues in meetings.
- Monitoring & maintaining sufficient awareness of threats and vulnerabilities.
- Establishing & maintaining a dynamic control environment.
- Managing connections to third parties.
- Develop/test business continuity & disaster recovery plans that incorporate cyber incident scenarios.

Threat Intelligence Resources

Cybersecurity

- 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

- FFIEC IT Handbooks
  http://ithandbook.ffiec.gov
- FFIEC Cybersecurity Awareness
  http://ffiec.gov/cybersecurity.htm
- Financial Stability Oversight Council 2015 Annual Report
  http://www.treasury.gov/initiatives/fsoc/studies-reports/Pages/2015-Annual-Report.aspx
- Financial Institution Letters
  www.fdic.gov/regulations/resources/director/risk/it-security.htm

Director's Resource Center

Cybersecurity

- **Director's Resource Center**

  www.fdic.gov/regulations/resources/director/

- **Technical Assistance Video Program**
  - **Information Technology (IT)**
  - **Corporate Governance**
  - **Third-Party Risk**
  - **Vendor Management (Coming Soon)**
  - **Cybersecurity 101 (Coming Soon)**
  - **Cyber Challenge: A Community Bank Cyber Exercise**
    - **Vignette 1: Item processing failure scenario**
    - **Vignette 2: Customer account takeover scenario**
    - **Vignette 3: Phishing and malware problem**
    - **Vignette 4: Problem with the bank's technology service provider**
    - **Vignettes 5-7: Coming Soon**

Regional Contacts

Cybersecurity

- **Atlanta Region**
  - Richard Snitzer – RSnitzer@fdic.gov
  - Lenna Escosa – MEscosa@fdic.gov

Question/Answers

Cybersecurity

Questions?

E-mail Questions to:

CybersecurityATL@fdic.gov