

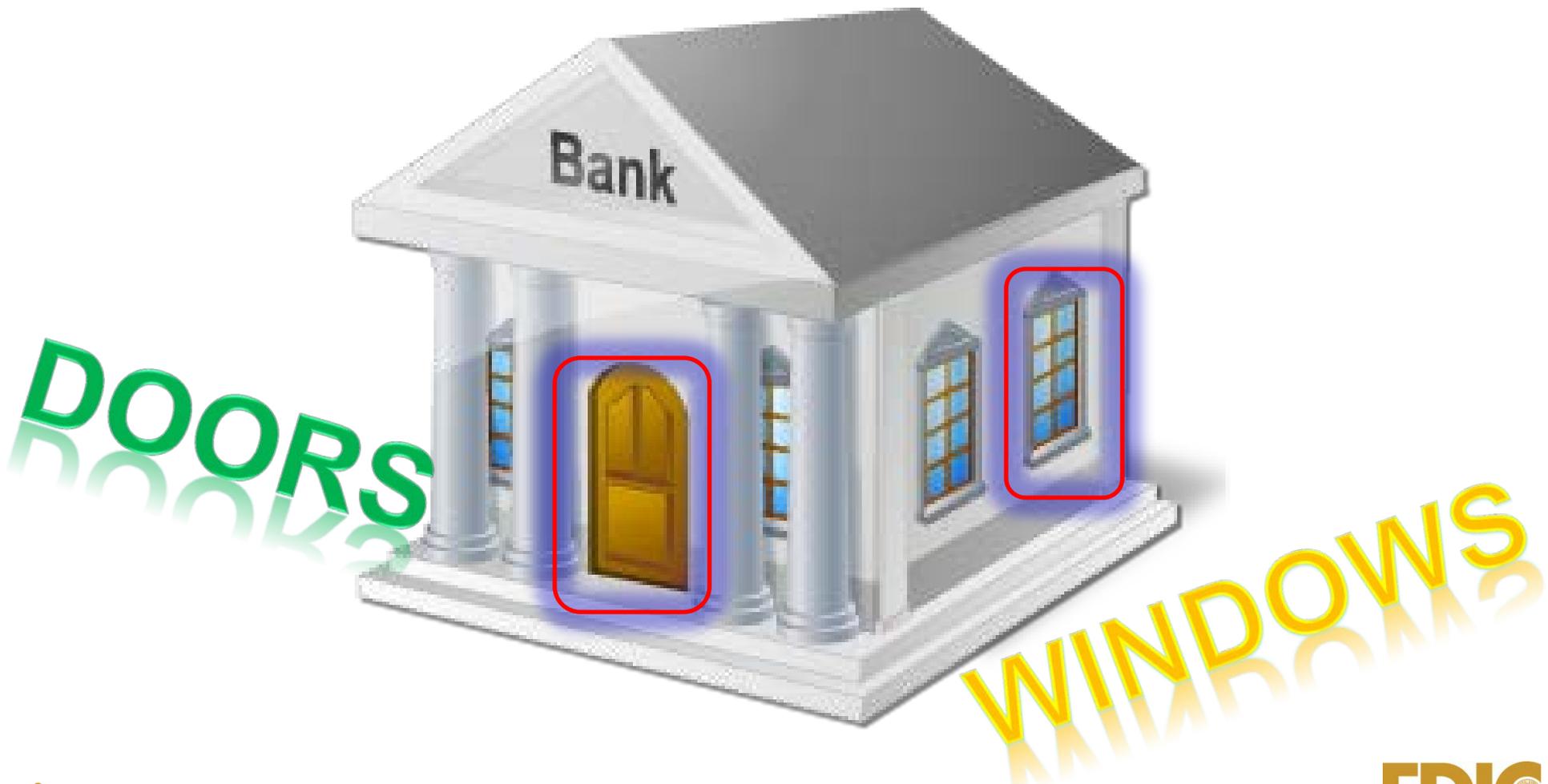


Cybersecurity Intelligence, Resilience, and Management
Atlanta Region Banker Call
April 21, 2016

Objectives

- Data Security Evolution
- Risk Management Programs
 - People and Patches
 - Threat Environment
- Third-Party Management
 - Resilience
- Incident Management Program

Evolution of Data Security



Definition

Identify

“The process of protecting information by preventing, detecting, and responding to attacks.”

Detect

Respond

Recover

Protect

Risk Management



Risk Management - Governance

- ◆ Strategic Planning and Budgeting
- ◆ Accountability
- ◆ Framework
- ◆ Audit Plan
- ◆ Board Reporting

Cyber Risk is a Business Risk!

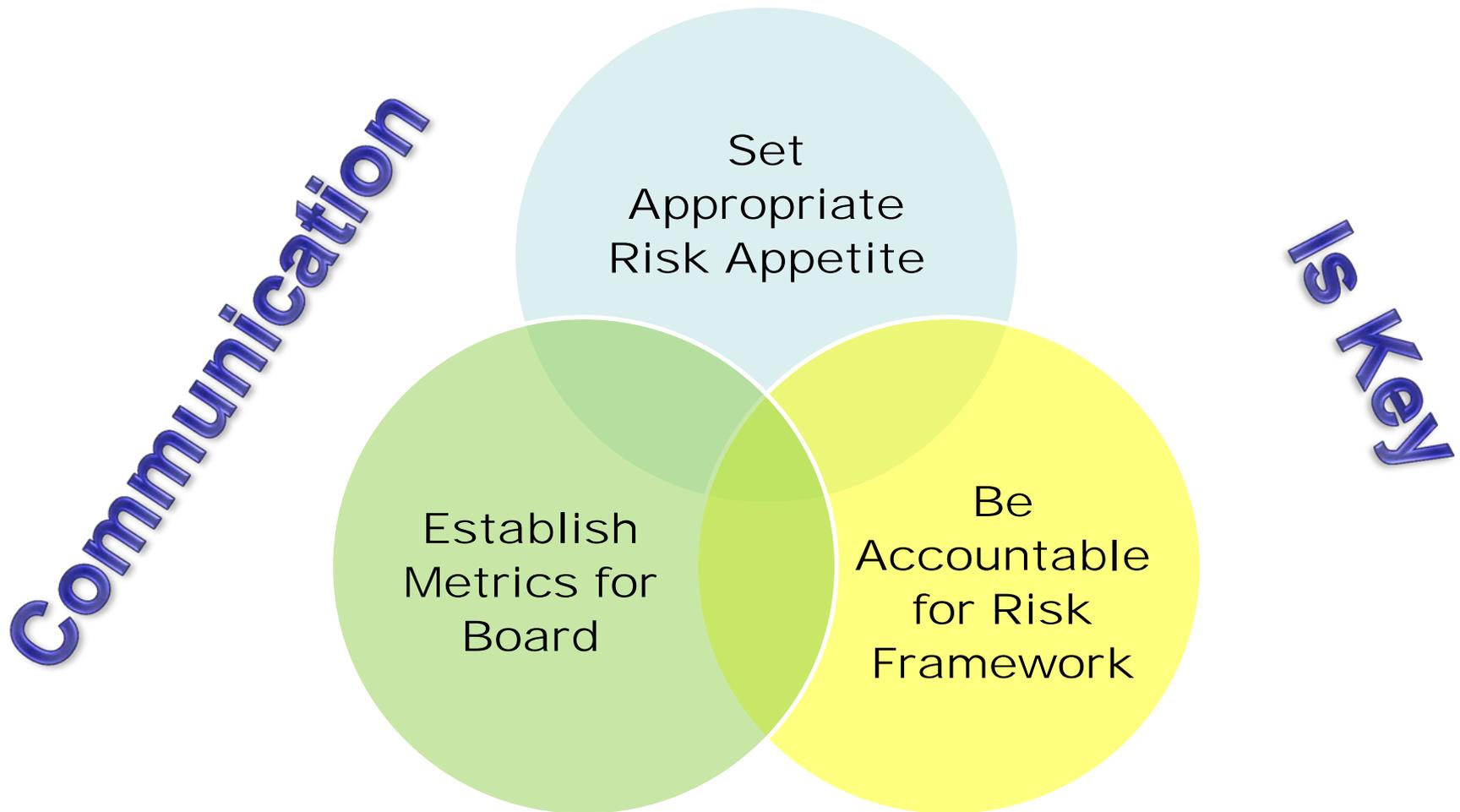
Risk Management - Governance

Oversee Senior Leadership

Promote Appropriate Corporate Culture

Align Performance Reviews

Risk Management - Governance



Since 1999

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
- Ensure the proper disposal of customer information and consumer information

People and Patches

S

“...a campaign of just ten e-mails yields a greater than 90% chance that at least one person will become the criminal’s prey...”

t

a

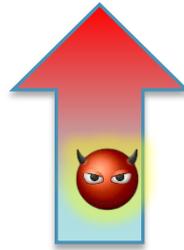
t

“...11% of recipients of phishing messages click on attachments.”

S

Source: Verizon 2015 Data Breach Investigations Report

Increasing Inherent Risk



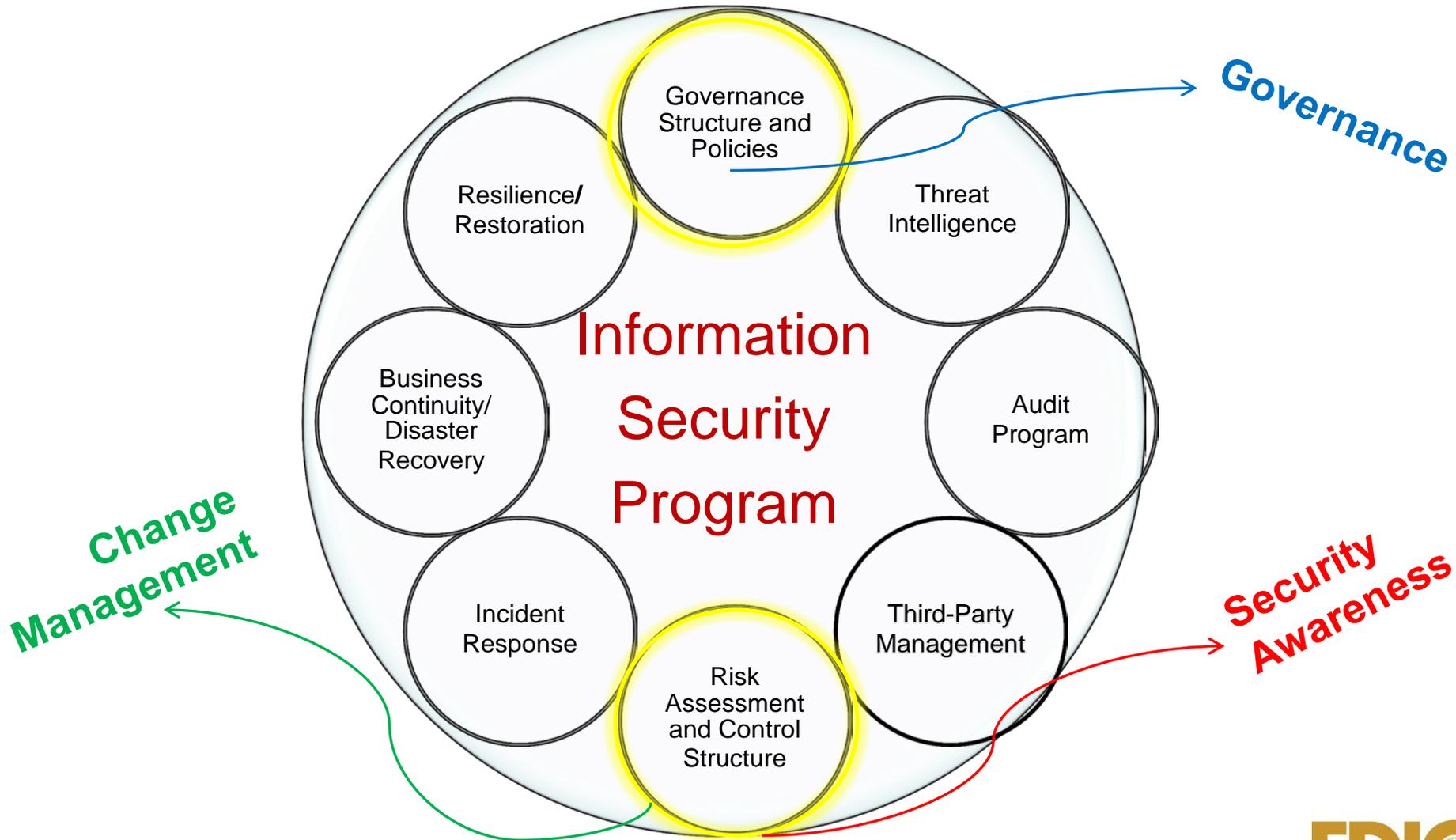
- Growing Vulnerabilities
 - ◆ Interconnected systems
 - ◆ New delivery channels
 - ◆ Legacy products
 - ◆ Emerging/Unknown

- Increasing Threats
 - ◆ Number/types of actors
 - ◆ Nature/volume of attacks
 - ◆ Level of sophistication
 - ◆ Emerging/Unknown

Threat Environment - General Defenses

- Vulnerability Assessment and Penetration Test
- Web Application Stress Test and Code Review
- Social Engineering Test
- Enterprise Security Risk Assessment
- Third-Party Management
- BCP/DR

Information Security Program



People and Patches - Training

Security Awareness
Training

```
graph TD; A[Security Awareness Training] --- B[Enterprise-wide]; A --- C[Role-specific]; A --- D[Customers/Merchants]; A --- E[Third Parties]; A --- F[Cybersecurity Culture];
```

Enterprise-
wide

Role-
specific

Customers/
Merchants

Third Parties

Cybersecurity
Culture

“Think Before You Click”

People and Patches - Success

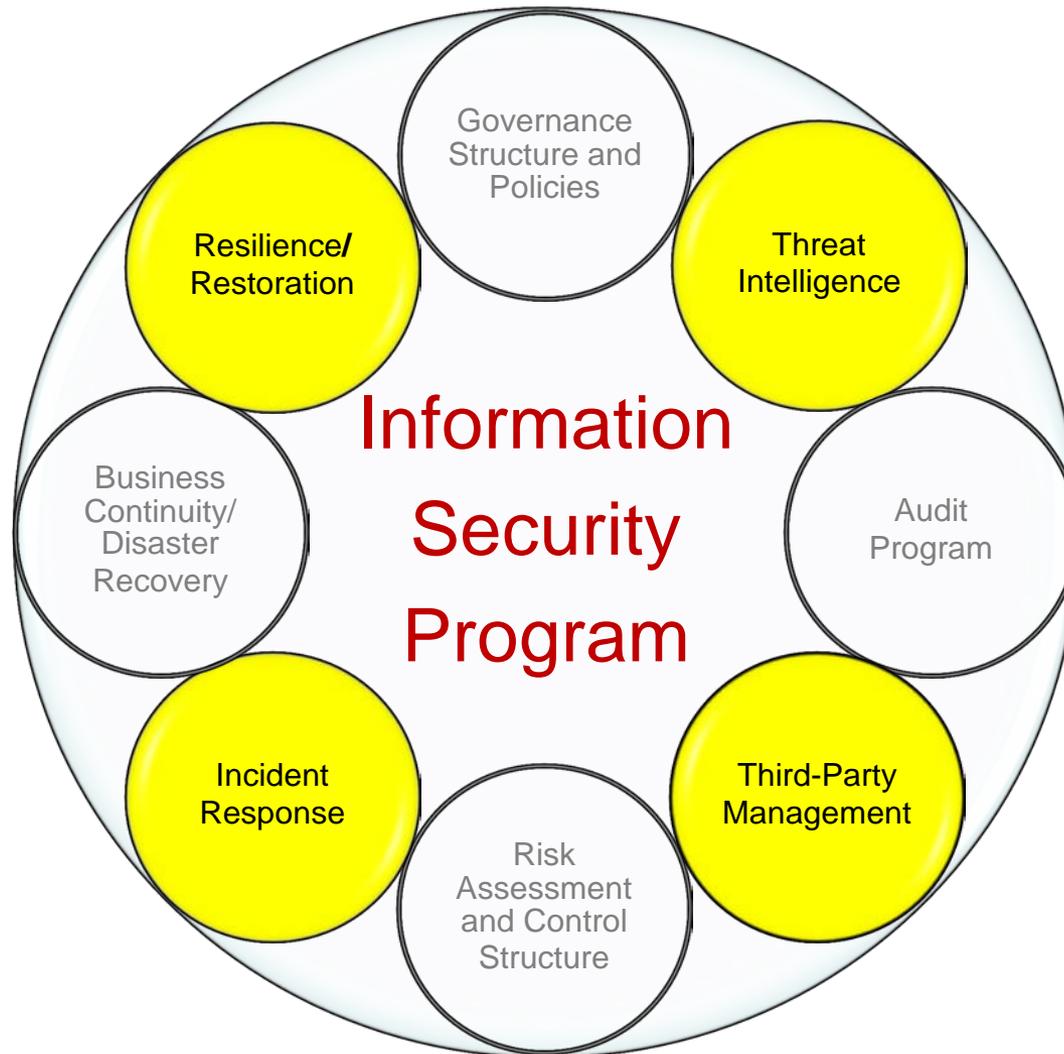
1. Get Executive Buy-In. Early and Often.
2. Culture, Context, & Continuity are Essential.
3. Be Clear. Use Real-World Scenarios & Applications.
4. Try to Avoid A Long Boring List of "Don'ts".
5. Give Good Reasons. Explain Security Guidelines.
6. Consider Role-Specific, Risk-Based Security Training.
7. Be Creative. Include Multiple Channels and Formats.

Control Structure - Change Management

- ◆ **Formal Written Policy and Procedures**
 - Develop system for identifying, prioritizing, applying, and testing patches
 - Create/maintain asset inventories
 - Timely updates
 - Integrate threat intelligence
 - Mitigate risk from unsupported operating systems and applications
 - Report to board and senior management

◆ **Audit Should Validate Program**

Information Security Program



Information Security Program - Enhanced

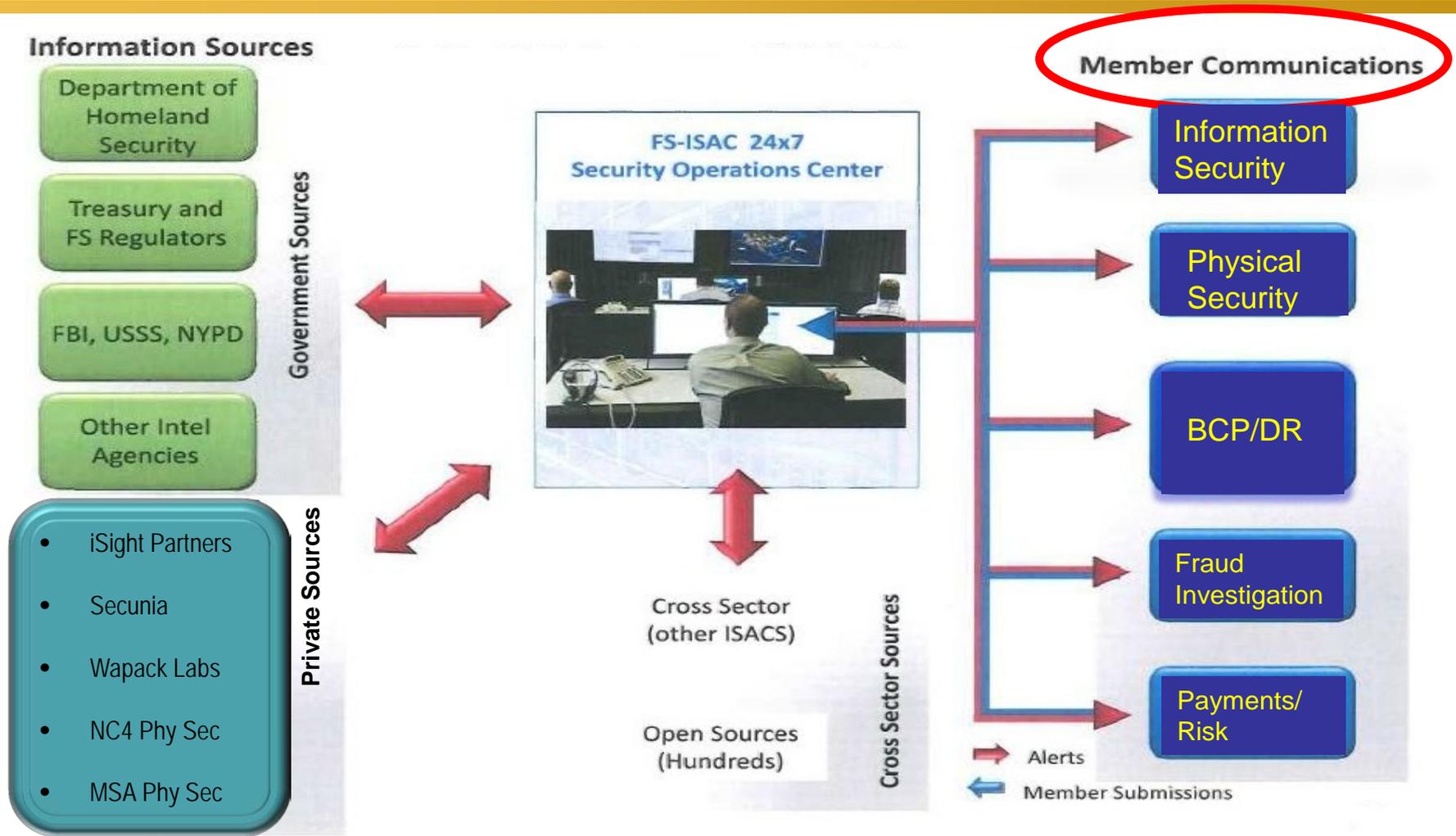
- **Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement**
 - ◆ “Financial institution management is expected to monitor and maintain sufficient awareness of cybersecurity threats and vulnerability information so they may evaluate risk and respond accordingly.”

- **FFIEC Business Continuity Planning Handbook, Appendix J – Strengthening the Resilience of Outsourced Technology Services**

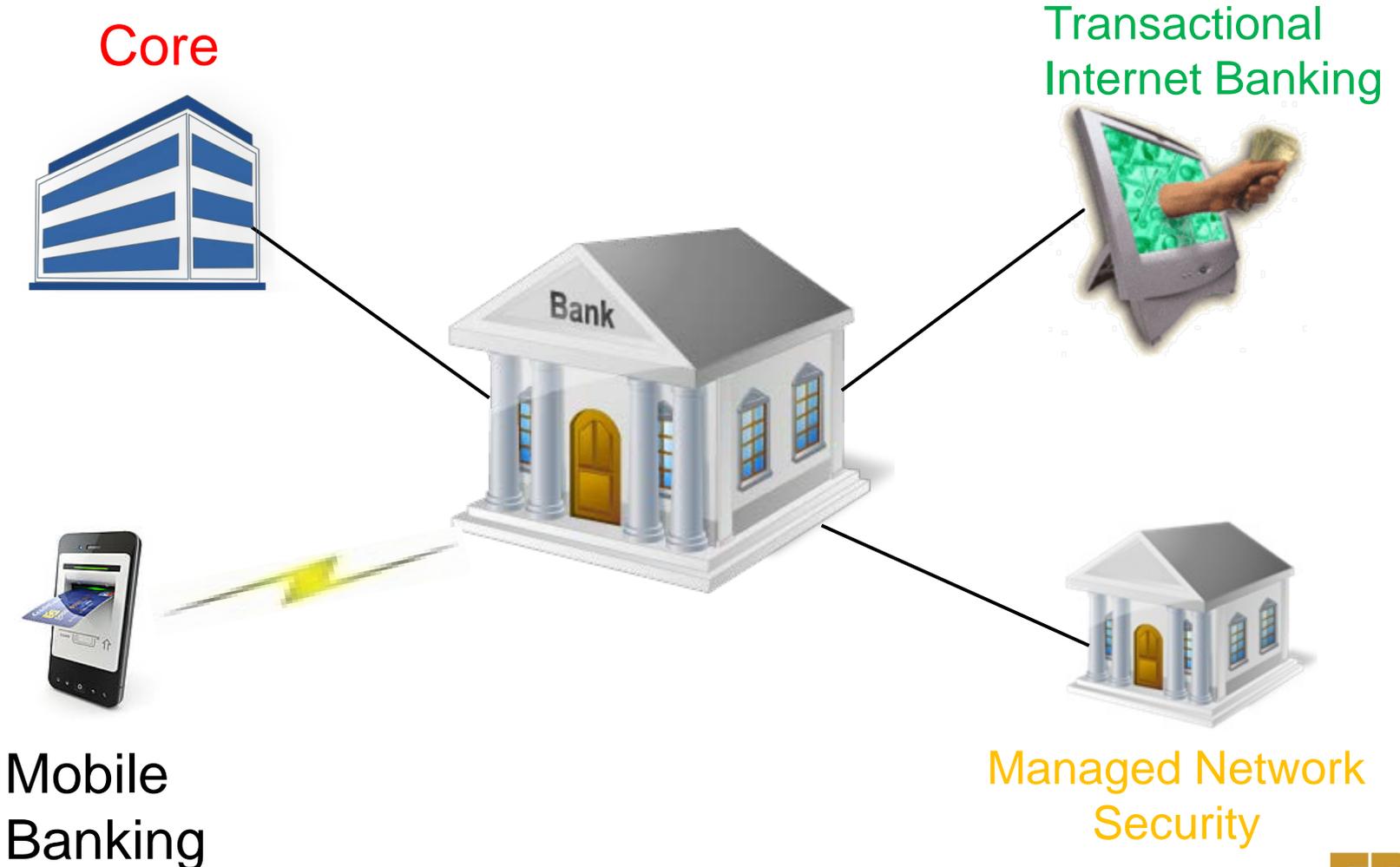
Threat Intelligence



Threat Intelligence - FS-ISAC



Third-Party Management



Appendix J - Third-Party Management

- Relationship Management
 - ◆ Due Diligence
 - ◆ Contracts
 - ◆ Ongoing Monitoring
- Resiliency and Testing
 - ◆ Mission Critical Services
 - ◆ Capacity
 - ◆ Service Provider Continuity Scenarios
 - ◆ Gap Analysis
 - ◆ Service Provider Alternatives

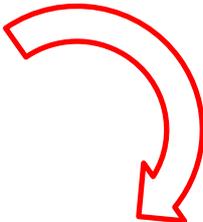
Key Elements

Appendix J - Resilience

- ◆ **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 Management

- **Test against foreseeable cyber threats**
- **Integrate service provider considerations**

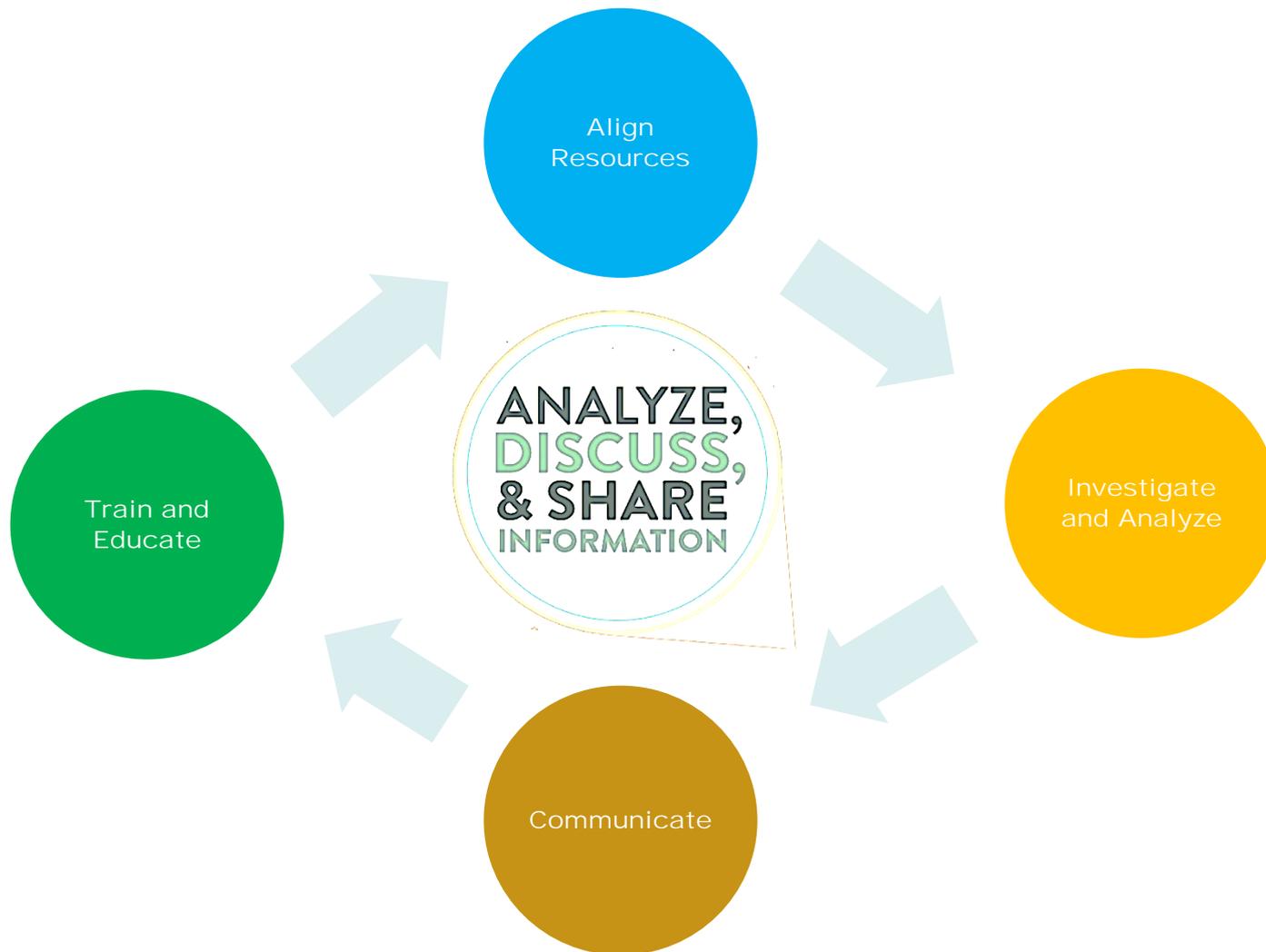
FIL-27-2005 

- **“Final Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice”**

Incident Response - Pillars



Incident Response - Team



Cybersecurity Assessment Tool

- Identifies factors affecting cyber risk
- Assesses cybersecurity preparedness
- Evaluates cybersecurity preparedness and risk alignment
- Performs gap analysis
- Identifies risk management strategies

Summary

- ISP = Cybersecurity
- Threat Environment
- Change Management
- Gap Analysis
- Cybersecurity Assessment Tool
- Risk Management Program
- Resilience

Questions?

ATLConferenceCall@FDIC.gov

Resources

- 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 (Cont.)

- **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

Cybersecurity Assessment Tool

Questions regarding the Cybersecurity Assessment Tool can be submitted through:

https://fdicsurveys.co1.qualtrics.com/jfe/form/SV_4JgplWXWB9Gjps1

Director's Resource Center

- www.fdic.gov/regulations/resources/director/
- **Technical Assistance Video Program**
 - ◆ Information Technology (IT)
 - ◆ Corporate Governance
 - ◆ Third-Party Risk
 - ◆ Vendor Management
 - ◆ Cybersecurity Awareness
 - ◆ **Cyber Challenge: A Community Bank Cyber Exercise**
 - Vignette 1: Item processing failure
 - Vignette 2: Customer account takeover
 - Vignette 3: Phishing and malware problem
 - Vignette 4: Technology service provider problem
 - Vignette 5: Ransomware
 - Vignette 6: ATM Malware
 - Vignette 7: DDoS as a Smokescreen

Regional Contacts

- **Atlanta Region**

- ◆ Richard Snitzer – RSnitzer@fdic.gov
- ◆ Lenna Escosa – MEscosa@fdic.gov