Objectives

- Data Security Evolution
- Risk Management Programs
  - People and Patches
  - Threat Environment
- Third-Party Management
  - Resilience
- Incident Management Program
Evolution of Data Security
“The process of protecting information by preventing, detecting, and responding to attacks.”
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

- Communication: Set Appropriate Risk Appetite
- Establish Metrics for Board
- Be Accountable for Risk Framework

Is Key
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

“...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
Threat Environment

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

Governance Structure and Policies

Threat Intelligence

Audit Program

Third-Party Management

Risk Assessment and Control Structure

Incident Response

Business Continuity/Disaster Recovery

Resilience/Restoration

Governance

Change Management

Security Awareness
People and Patches - Training

Security Awareness Training

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.


4. Try to Avoid A Long Boring List of “Don’ts”.


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

- 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
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.”

Threat Intelligence

Information Security Program

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

Information Sources
- Department of Homeland Security
- Treasury and FS Regulators
- FBI, USSS, NYPD
- Other Intel Agencies
- iSight Partners
- Secunia
- Wapack Labs
- NC4 Phy Sec
- MSA Phy Sec

Member Communications
- Information Security
- Physical Security
- BCP/DR
- Fraud Investigation
- Payments/Risk

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

Private Sources

Government Sources

Alerts
Member Submissions
Third-Party Management

Core

Transactional Internet Banking

Mobile Banking

Managed Network Security
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
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

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

- Framework
- Key Metrics
- Executive Sponsor
- Empowerment
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/Answers

Questions?

ATLConferenceCall@FDIC.gov
Resources

- Financial Services-Information Sharing and Analysis Center (FS-ISAC) [www.fsisac.com/](http://www.fsisac.com/)
- United States Computer Emergency Readiness Team (US-CERT) [www.us-cert.gov/](http://www.us-cert.gov/)
- InfraGard [www.infragard.org/](http://www.infragard.org/)
Resources (Cont.)

- FFIEC IT Handbooks
  [http://ithandbook.ffiec.gov](http://ithandbook.ffiec.gov)

- FFIEC Cybersecurity Awareness
  [http://ffiec.gov/cybersecurity.htm](http://ffiec.gov/cybersecurity.htm)

- Financial Stability Oversight Council 2015 Annual Report

- Financial Institution Letters
  [www.fdic.gov/regulations/resources/director/risk/it-security.htm](http://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/](http://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