FDIC

FEDERAL DEPOSIT INSURANCE CORPORATION

Cybersecurity Awareness

Part 1

Objectives

Cybersecurity Awareness

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

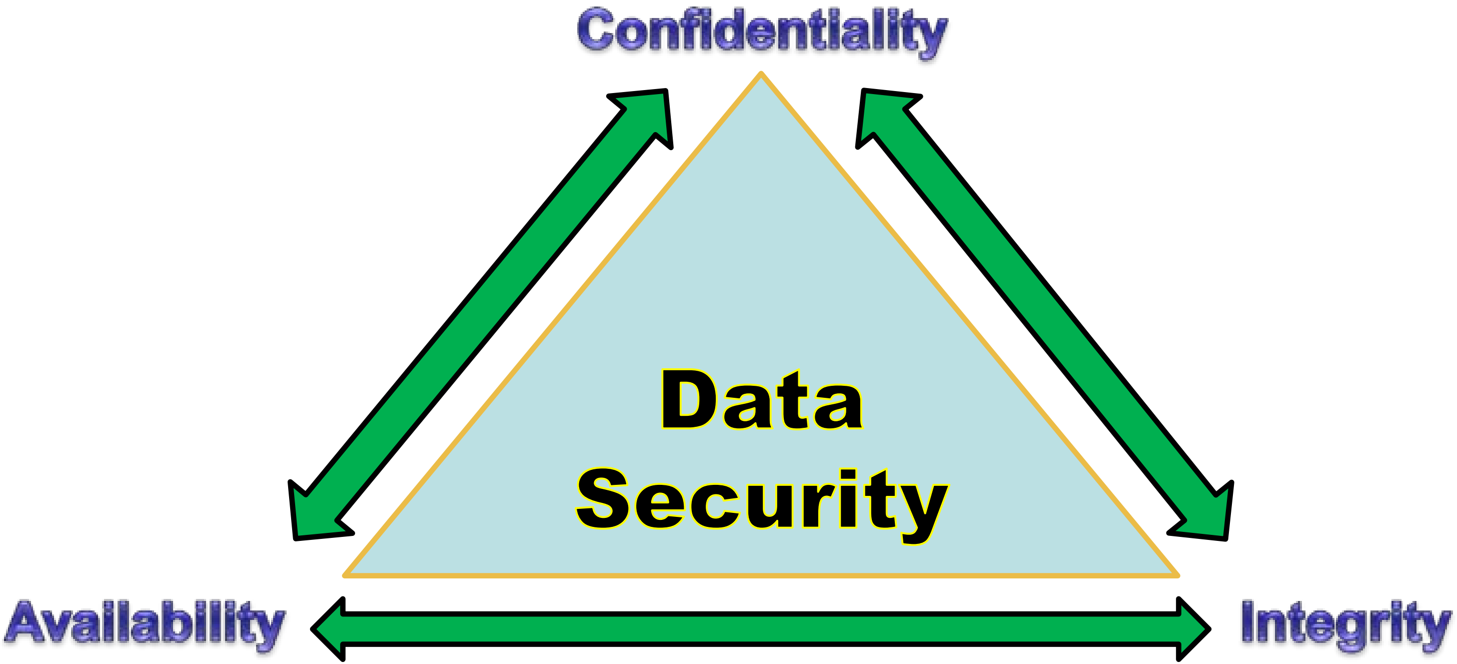
Part 1

- **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

Evolution of Data Security

Cybersecurity Awareness



Evolution of Data Security

Cybersecurity Awareness

Evolution of Data Security

Cybersecurity Awareness

Emerging
Bank
ATM
ONLINE BANKING
ACH

Definition

Cybersecurity Awareness

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

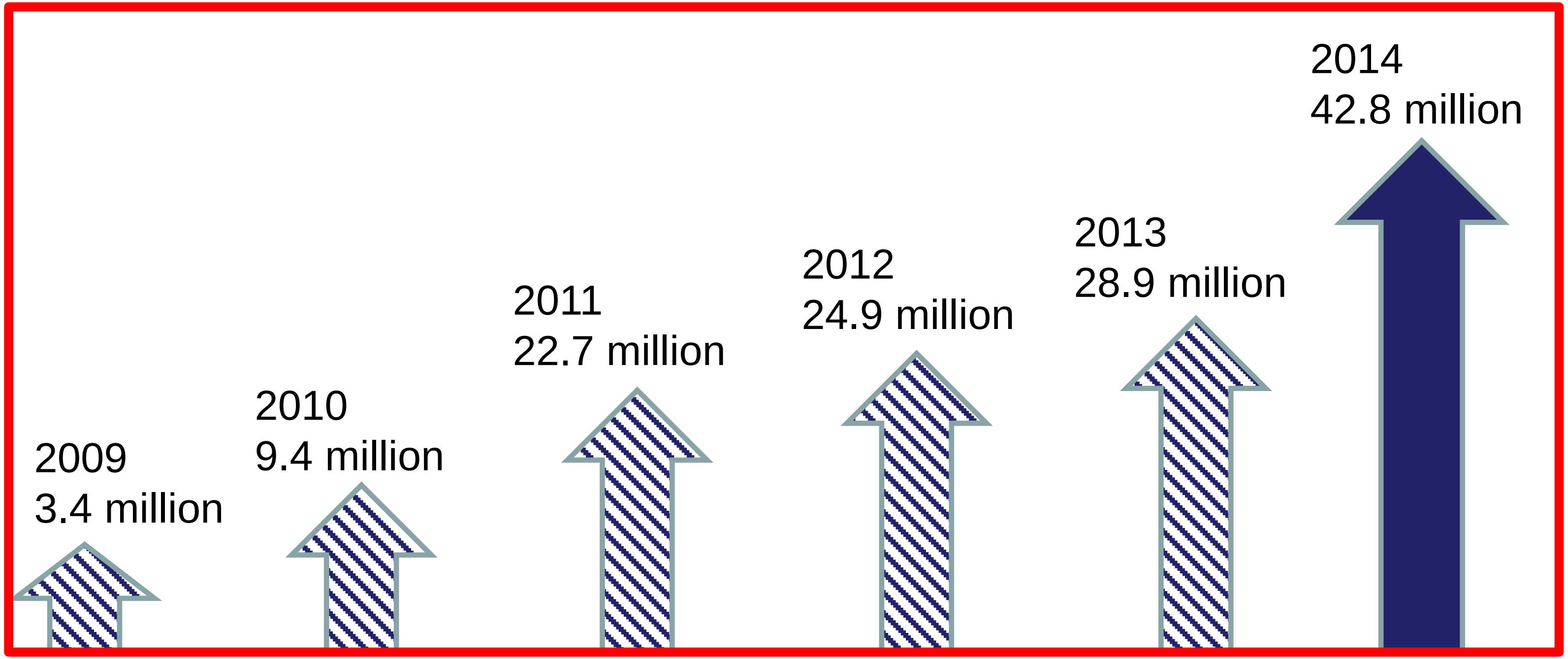
Cybersecurity Awareness

- **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 Awareness

2014 Information Security Incidents Up 48%



Source: PwC.com

People and Patches

Cybersecurity Awareness

“…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 Awareness

“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 Awareness

Increasing Inherent Risk

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

Emerging Vulnerabilities and Threats

Threat Environment: Vulnerabilities

Cybersecurity Awareness

- Technological
  - Weaknesses 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 Awareness

- 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 Awareness

- Malware/Destructive Malware
  - e.g., Key Loggers, Trojans, Ransomware, Wiper

Threat Environment: Attacks

Cybersecurity Awareness

- Malware/Destructive Malware
  - e.g., Key Loggers, Trojans, Ransomware, Wiper
- Phishing/Spear Phishing

Threat Environment: Attacks

Cybersecurity Awareness

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

Threat Environment: Example

Cybersecurity Awareness

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