Key Elements for Developing and Implementing a Strong Information Security Program

From Strategy to Reality!

Presented by:

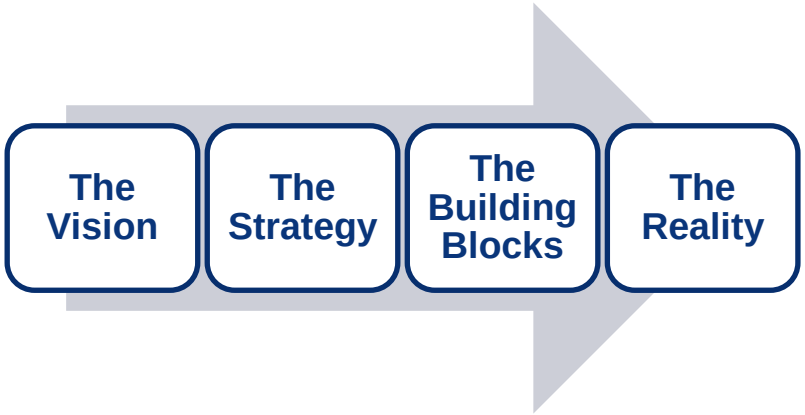
Mauricio Angée, CISSP

VP, Information Security Manager

Mercantil Commercebank N.A.

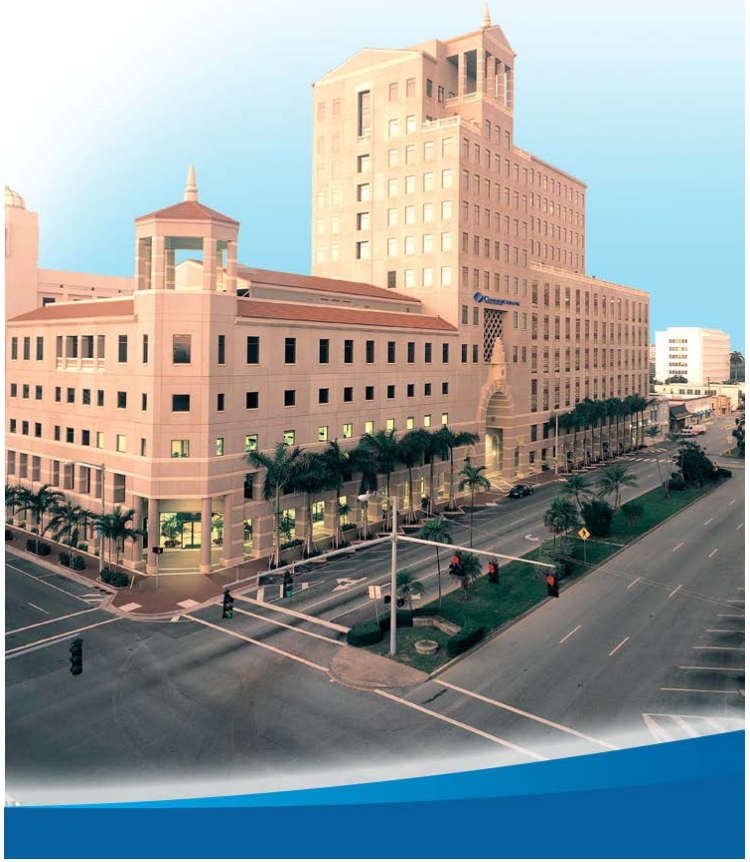
Overview

- About Mercantil Commercebank
- Provide a general overview of the presentation
- Define Information Security
- Outline the Components a Strong IS Program
- Measuring a Successful IS Program
- Provide Best Practices
- Final Remarks and Takeaways



Mercantil Commercebank Profile

- Headquartered in Coral Gables, Florida
- U.S. Markets:
  - South Florida – 15 Banking Centers
  - Houston Financial Center
  - New York Banking Center
- Over 100,000 customers and assets of $6.5 billion
- Over 30 years of banking experience
- A wholly-owned subsidiary of Mercantil Servicios Financieros, a global financial services institution based in Venezuela with over 85 years of experience
- Ranked as the third largest bank headquartered in South Florida; fifth largest in Florida in terms of total assets[1]
- Mercantil CB's holding company listed by the American Banker among the Top 150 banking holding companies in the U.S. based on total assets.



Objective

- Discuss the different aspects of successfully implementing an Information Security program, form conceptualization to execution including people, process, and technology.
- Provide an overview of the importance of the developing an IS framework and the integration of Information Security into business processes.
- Discuss the need for developing a collecting, analyzing and reporting meaningful metrics.
- Provide best practices that will lead to a successful implementation of an Information Security program.

Defining Information Security

- Information Security is simply the process of keeping information secure:
  - protecting its availability, integrity, and privacy.
- Information Security is about controlling access to information and resources.
- IT Security refers to Securing and protecting IT assets
- Effective Information Security incorporates security products, technologies, policies and procedures.

Information Security Areas of Concentration

IS Management

Implements Security program

Dictates/Enforce Policies

Sets strategy

IT Security / Protection

- Architectural Design
- Solution Implementation
- Protection (AV, FW, IPD/IDS, etc.)

Access and ID Management

- Periodic user access reviews
- Entitlement reviews
- Employee profiles

Incident Management & Monitoring

- Audit log reviews
- Incident response
- Vulnerability remediation

Threat Management (Red team)

- Vulnerability scans
- Pentesting / App Security Testing
- Patch management

Operational Security / Compliance

- Periodic reviews security controls
- Risk Assessments
- Provides recommendations

Business Continuity

- Disaster Recovery
- Testing
- Reporting

Defining the Components of an IS Program

- Select an IS Framework
- People, Processes and Technology
- Define and implement a data protection model
- Develop a Strategy
  - short, medium, and long term goals
- Implement/Enhance an IS Risk Management program
- Implement an ongoing Security Awareness Program
- Assess periodically

Choosing the Right Framework

Compliance and Regulations

Main Objective:

The protection of sensitive/customers/patients/cardholder/financial data

- **Financial Institutions**
  - Gramm-Leach-Bliley Act (GLBA)
  - Office of the Comptroller of the Currency (OCC)
  - FDIC
- **Government**
  - Federal Information Systems Management Act (FISMA)
- **Health Industry**
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Health Information Technology for Economic and Clinical Health Act (HITECH)
- **Public Companies**
  - Sarbanes–Oxley Act (SOX) - Accounting Reform & Investor Protection Act
- **Credit Card Industry**
  - Payment Card Industry (PCI) - PCI Security Standards Council
- **Educational Agencies and Institutions**
  - Family Educational Rights and Privacy Act (FERPA)
- **State Privacy Laws**

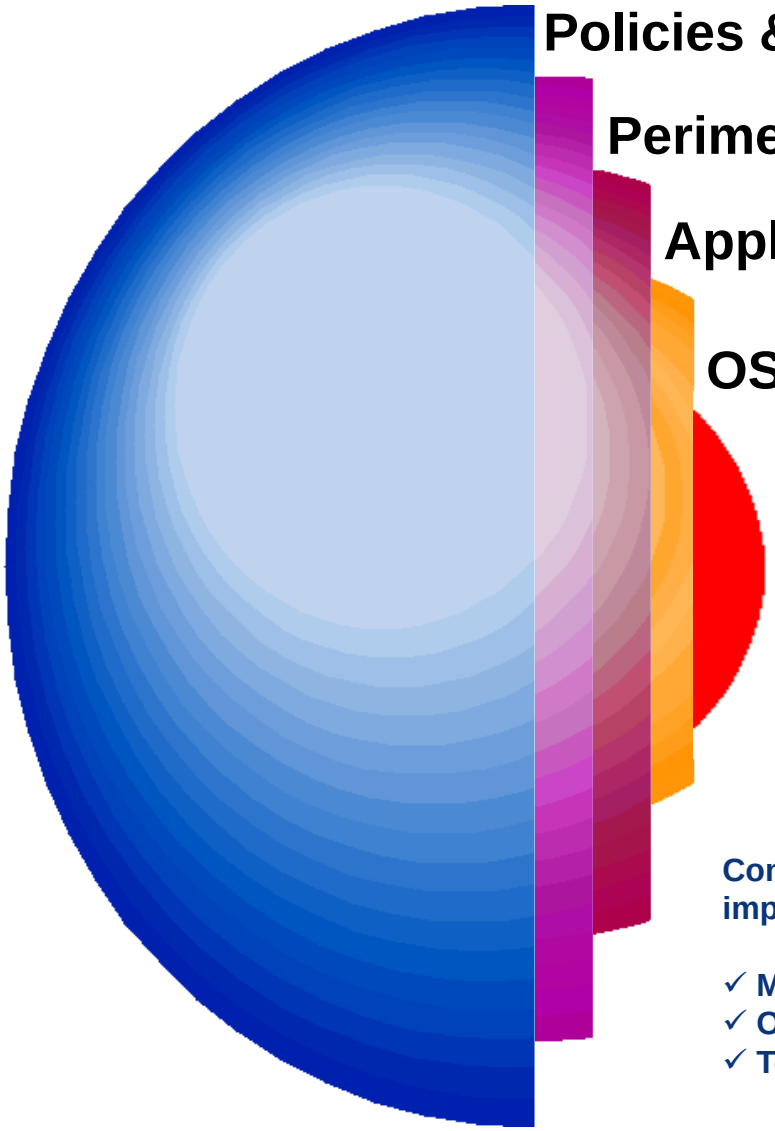
Defining the Components of an IS Program

- People
  - Assemble the right team and Clearly define roles and responsibilities
  - Your team must be qualified:
    - Education
    - Experience
    - Certifications
- Processes
  - Define the required processes
    - Starting at high level and identifying the key big steps is important to see the process from end to end.
  - Test and Adjust controls (Risk Assessments)
  - Implement continuous monitoring program
  - Training
- Technology
  - Develop road map and align with IT strategy
  - Ensure technology is aligned with business needs

Data Protection

- **Privacy**
  - Goal: Protecting sensitive information
- **Classification**
  - The classification of the data should determine the level to which the data needs to be controlled/secured.
- **Assessment**
  - Where is the data?
  - What is the business nedd data?
  - How is data accessed (shared folder, queries, etc)?
- **Definition Security Controls**
  - Data segmentation
  - Logical access controls
  - Encryption
- **Testing**
  - Periodic Vulnerability Scans
  - PenTesting
  - Application Security Testing
- **Monitoring**
  - Security Information and Event Management (SIEM)
  - Managed Security Services

Layered Security - Centric Protection



Policies & Procedures

Perimeter Controls

Applications Controls

OS Hardening Controls

Information Assets Protection Controls

Continuous Monitoring of the protection measures implemented to safeguard the information:

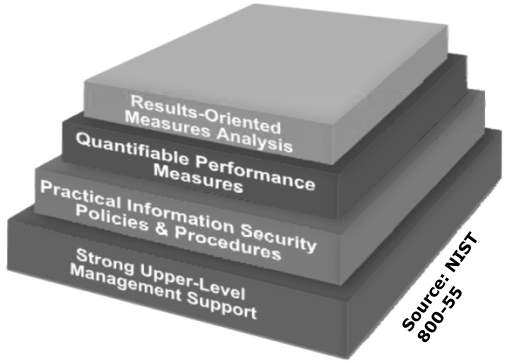
- ✓ **Management Controls – Policies**
- ✓ **Operational Controls – Users**
- ✓ **Technical Controls – Tools**

From Strategy to Reality!

Measuring a Successful IS Program

- Develop manageable Metrics
- Metrics could be used demonstrate how well the environment is protected against Information Security threats
- Metrics monitor the effectiveness of goals and objectives established for Information Security
- Start with a few useful key set of metrics
- Develop a dashboard/scorecard to track and communicate results

If it can't be measured, it can't be improved!



Testing your IS Program

Capability Maturity Model (CMM)

Level	Name	Description
1	Initial	Ad-hoc, reactive, “firefighting”
2	Repeatable	Proactive, trained people
3	Defined	Documented, standardized products and procedures
4	Managed	Metrics for deliverables and processes
5	Optimizing	Continuous improvement with feedback

Carnegie Mellon SEI

Best Practices

- Take a more proactive instead of a reactive posture!
- Develop, Communicate, and Enforce clear policies, processes, and procedures.
- Enhance an IS Risk Management program.
- Integrate InfoSec into the SDLC and business processes.
- Define security controls to safeguard data.
- Communicate - implement a strong awareness program.
- Create a culture of “doing the right thing.”
- Train your Information Security personnel.
- Develop a vendor management program (ask vendors to certify security practices.)
- Establish Patch Management program.
- Maintain a “sound” auditing and monitoring processes.

Support your Information Security teams

From Strategy to Reality!

Final Remarks & Takeaways

10 Secrets for Success :

1. Have a focus on the information security program as a whole
2. Identify and manage risk
3. Follow the data
4. Apply defense-in-depth measures
5. Align with business products, services and objectives
6. Anticipate, be innovative and adapt
7. Establish a culture of security
8. Measure your Security Program
9. Trust but verify
10. Build support

Thank You