



MBA Information Security Overview

May 2008

Harry Gardner

VP Industry Technology



MBA Security Initiatives

- Legislation, Regulation and Advocacy
 - Government & Legal Affairs
- MBA Technology Committees
 - Board of Directors Technology Steering Committee
 - Residential Technology Steering Committee
- Education
 - CampusMBA
- MISMO
 - Information Security Work Group
- Identity Management
 - Secure Identity Services Accreditation Corporation

MBA Security Assets

- BoDTech Security White Papers
 - CXO Security Good, Bad & Ugly (10/2005)
 - Risk Mitigation 5 Step Model (10/2006)
- ResTech Security Subgroup white papers
 - Strong Authentication (10/2007)
 - Basic Security Program (05/2008)
- MISMO Information Security Workgroup
 - Identifying and Safeguarding Guidelines (10/2007)
 - Remote Authentication (11/2008)
 - Appraisal Risk Assessment (05/2008)



Advocacy/Policy Support

- MBA Red Flag Comment Letter
 - MBA position on identity theft and regulation
- Data Security Task Force Recommendations
- Monitor Federal and State legislation



SISAC – Identity Management

- Define standards for credential providers
- Common requirements & obligations to build trust and reliance of credentials
- Advance MISMO XML records with authentication and tamper-evident seals to achieve legal framework (backed by E-SIGN and UETA)
- Accreditation:
 - SISAC does not issue credentials, rather SISAC accredits Credential Service Providers (CSP)
 - Independent 3rd party audit or attestation



Broad Perspective



Information Security Drivers

- Federal privacy and ID theft legislation and regulations
- State breach notification legislation
- Liability and reputation risks
- Mitigation of fraud

Legislation and Regulations

- PATRIOT Act (Section 326)
 - Verify identity, maintain records, and consult government list of known terrorists
 - Customer Identification Programs (CIPs)
- FFIEC Guidance
 - The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for *high-risk* transactions
 - Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation.
 - *High Risk Transactions*
 - Finance transfer
 - Transfer of Personal Information



State Breach Disclosure Laws

- 42 states have breach disclosure laws
- Over 225 million sensitive personal information involved in security breaches
- ChoicePoint –
 - FTC settlement for \$10m in civil penalties and \$5m for consumer redress. Additional \$10m to settle a class action lawsuit
- \$182/record & \$4.8 million/incident
 - A 2007 survey by Ponemon Institute



Increased Fraud Risks

- Financial Crimes Enforcement Network (FinCEN); Mortgage Suspicious Activity Reports (SARs) April 2006 – March 2007
 - 44% increase from 2006 to 2007 in Mortgage SARS (52,868),
 - Mortgage Loan Fraud was the third most prevalent
 - Identity fraud and identity theft associated with mortgage fraud increased over 95% from the previous study
 - Fraudulent appraisals were at nearly 13%, an increase of 2%.

Suspicious Activity Reports

Activity	No. of SARs	% of Sampled SARs
Misrepresentation of income/assets/debts	761	43.02%
Forged/fraudulent documents	496	28.04%
Occupancy fraud	255	14.41%
Appraisal fraud	232	13.11%
ID fraud	180	10.18%
Straw buyers	100	5.65%
ID theft	61	3.45%
Flipping	48	2.71%

Identity fraud is defined as the unauthorized use of a social security number.

Identity theft involved an attempt to obtain credit using another person's identity.



Commercial

- Most firms do not differentiate in policies
 - Whatever baseline security for consumer also applies to commercial mortgages
 - Whatever baseline access management for consumer also applies to commercial mortgages
 - Definition of confidential versus non-public

Commercial (Continued)

■ Trends in International versus US

- No differentiation in commercial mortgages
- Expectation of privacy is a human right
- For example, transfers of personal data outside the EU are prohibited (unless the transfers are to a country which offers an adequate level of protection)
- Issue –The US is not considered by the EU as providing an adequate level of data protection
- Issue –Data transfers initiated inside the EU (data sent from France to US) are covered by EU regulations



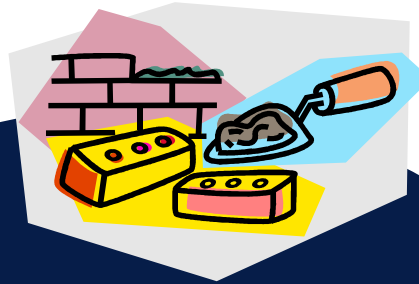
Proactive, not Reactive

Think Comprehensive

Information Assurance Model

(Plan, build, run, monitor and educate)

5. Education
(Initial and Continual)



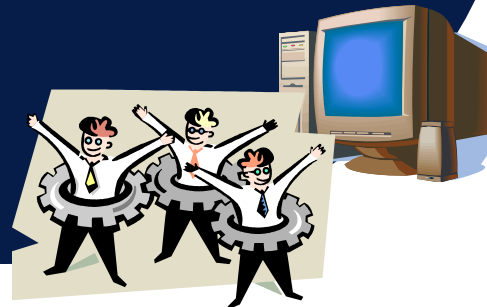
1. Business & Risk
Description (Foundation)

2. Policy and
Architecture
(Framework)

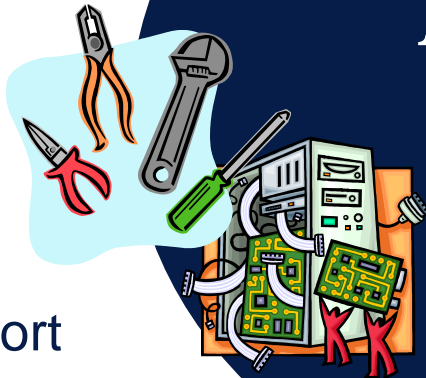


*Information
Security
Model*

3. Solution
Specification
(People, Processes
& Technology)



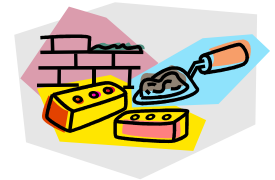
4. Support
(Testing,
Maintenance &
Sustainability)



Information Security Model

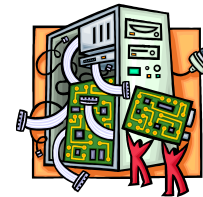
- Business & Risk Description (Plan)
 - Overall description
 - Identify assets, users, and systems
 - Risks associated with information assets

- Framework (Build)
 - Definition of an information security policy
 - “what is allowed / not allowed”
 - Definition of an information security architecture
 - Big picture
 - Tie together resources and protection
 - Identify interconnectivity between those systems



Information Security Model

- Solution (Run)
 - Detailed specifications
 - Technology
 - Procedures
 - Personnel
 - Implementation planning and testing
 - Certification & accreditation
- Support Program (Monitor)
 - Maintenance, Monitoring, & Reporting
 - Insurance & Contingency Planning
- Awareness Program
 - General security literature
 - Specific “How to...” guides
 - Periodic “refresher” courses





Basic Security Program

1. Acceptable Use Policy
2. User Access Control
3. Physical Security
4. Personnel Security
5. Business Contingency Planning
6. Compliance and Enforcement
7. Third Party Provider Management
8. Technology Security



Summary

- Information Security is a key risk function of any business
- Multiple facets make up the process of information security
- Information Security is an on-going process, not a one time inspection
- Increased regulation demands that more controls are put into place and monitored
- Business are mandated to ensure proper controls regardless of in-house or outsourced services
- Keeping up to date with the latest information security is a daunting task if not done within a framework



Thank You!

Harry Gardner

VP Industry Technology

MBA

202-557-2839

hgardner@mortgagebankers.org