



Confidentiality

Integrity

Availability

# Risky Business

Information Security & Business Success

Presented by:

John H. Rogers, Practice Director

InfoSecurus, Inc

October 20, 2011

Copyright © 2011, InfoSecurus, Inc.. All rights reserved





# Agenda

Confidentiality

Integrity

Availability

- The Environment, in which we find ourselves.
  - Protection from what?
  - Recent Data Breach Examples from Maine
- Key concepts
- Correcting some misconceptions
- The concept of Organizational Memory
- The Culture of Continuity
- Risk Management: Controls essential to business success





# Protection From What?

Confidentiality

Integrity

Availability

- Theft or loss of equipment
- Theft or loss of information in hard-copy
- Hardware failure
- Application/system failure due to patching, updates, upgrades
- Loss of Intellectual capital from turn-over
- 24/7 scanning of the internet
- Accidental Loss & Disclosure of Data
- Social Engineering attacks
- Disgruntled employees
- Natural disaster
- Directed hacking attacks





Confidentiality  
Integrity  
Availability

## Recent Data Breach Examples from Maine





# Recent Maine Data Breach Incidents

Confidentiality

Integrity

Availability

Who: Days Jewelers

What: 2,000 Credit/Debit Card #'s

When: February 2011

How: Outside Hack

Approx. Cost: \$428K

Hindsight: Penetration Testing, Intrusion Detection





# Recent Maine Data Breach Incidents

Confidentiality

Integrity

Availability

Who: ME Dept. of Education

What: Unknown # of Social Security Numbers

When: September 2010

How: Inside Job – Unauthorized Employee Access

Approx. Cost: Unknown (avg. cost per record = \$214)

Hindsight: Policies & Procedures, Awareness Training





# Recent Maine Data Breach Incidents

Confidentiality

Integrity

Availability

Who: ME Sec. of State

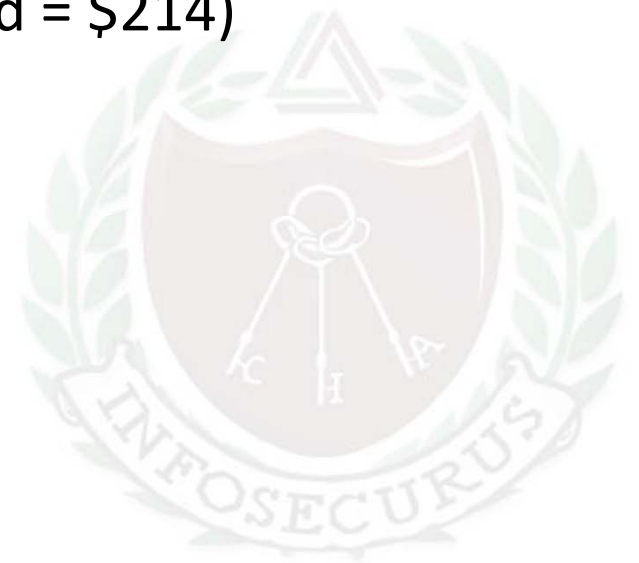
What: up to 700,000 Voter Registrations

When: August 2011

How: Malware Infection(remote computer used by Town Clerk)

Approx. Cost: Unknown (avg. cost per record = \$214)

Hindsight: Access Control Procedures





# Recent Maine Data Breach Incidents



Who: Hannaford Bros.

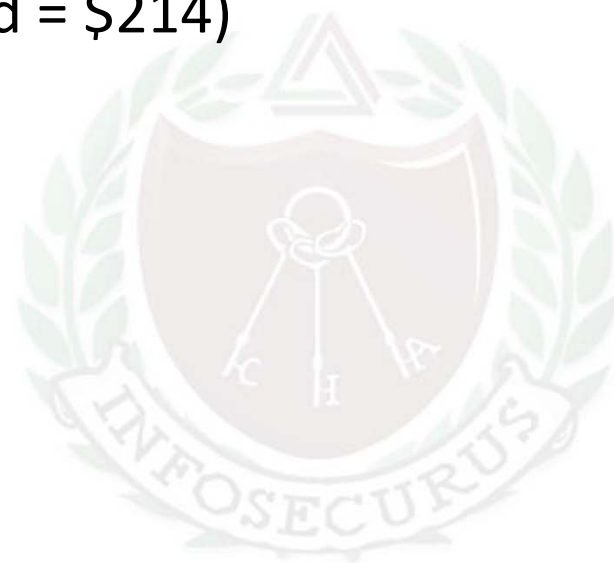
What: 4.2M credit/debit card #'s

When: March 2008

How: Outside Hack – Internet App Vulnerability

Approx. Cost: Unknown (avg. cost per record = \$214)

Hindsight: Application Penetration Test





# Key Concepts

Confidentiality

Integrity

Availability

## Information Security

- The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.





# Key Concepts

Confidentiality

Integrity

Availability

The CIA Triad: The founding concepts for understanding the scope of information security.

- **Confidentiality:** Is it private?
- **Integrity:** Is it accurate
- **Availability:** Is it there when you need it?





# Key Concepts

Confidentiality

Integrity

Availability

## Due Care:

- The duty to provide for information security to ensure that the type of control, the cost of the control, and the deployment of control are appropriate for the system being managed.





# Misconceptions

Confidentiality

Integrity

Availability

## Corrections: (These are all misconceptions)

- The idea that Information security is only about technology
  - People, Process, Technology
- The idea that IT Staff should be making the rules
  - Data Owners & Data Custodians
  - We are all end-users
- The idea that technology and security are separate from business
- The idea that Information Security and Risk Management are solely cost centers





# Organizational Memory

Confidentiality

Integrity

Availability

- The collective documented intelligence of the organization contained in:
  - Policies
  - Procedures
  - Guidelines
  - Plans
- Questions
  - How much of your organization's intellectual capital is memorized?
  - How much would your organization forget if key people left for any reason?
  - Can you quantify the costs of losing organizational intelligence?



# The Culture of Continuity

Confidentiality

Integrity

Availability

The strategically fostered, top-to-bottom company culture that supports:

- The business vision and mission of the organization
- The safeguarding of critical information
- The confidentiality, integrity and availability of that information
- Continuity of the organization, it's success, growth and fulfillment of the leadership vision.





# Strategic Goals & Information Security

Confidentiality

Integrity

Availability

## Strategic Business Goals Should Be Priority

A well conceived information security program must support these goals, not hinder them





# Controls Essential to Business Success

Confidentiality

Integrity

Availability

## Policies, Procedures, Plans

- Constitute organizational memory
- Describe the acceptable/required behavior
- Set boundaries
- Create an investment from all levels of the organization (If properly created and maintained)
- Support the business strategy by promoting consistency, raising the standard of performance and connection to the stated vision and mission.
- Minimize the effect of employee turn-over (If properly created and maintained)



# Controls Essential to Business Success

Confidentiality

Integrity

Availability

## Network Security Infrastructure

- Provide protection from outside threats
- Provide protection from inside threats
- Enable secure access from the inside-out to critical Internet resources
- Enable secure remote access for portable devices
- Monitor the “health” of critical servers and applications
- Protect digital information in when stored, processed and/or transmitted
- Provide organizational support for information use





# Controls Essential to Business Success

Confidentiality

Integrity

Availability

## Change Management

- Ensures that changes are approved by authorized personnel
- Provides a trail of accountability
- Provides back-out plans in the event of problems with patches, updates and upgrades
- Supports a strategy of planning and improvement in the organization
- Provides an accurate record of changes for analysis of business metrics
- Provides historical data that enables forecasting





# Controls Essential to Business Success

Confidentiality

Integrity

Availability

## Information Security Awareness Training

- Organization-wide training supports the Culture of Continuity
- Creates a common bond, shared experience and knowledge
- Increases performance and productivity
- Provides the opportunity to explain organizational rationale for policies
- Displays investment by the organization in its culture
- Works appropriately at all levels to advance security measures that support the core business strategy





# Controls Essential to Business Success

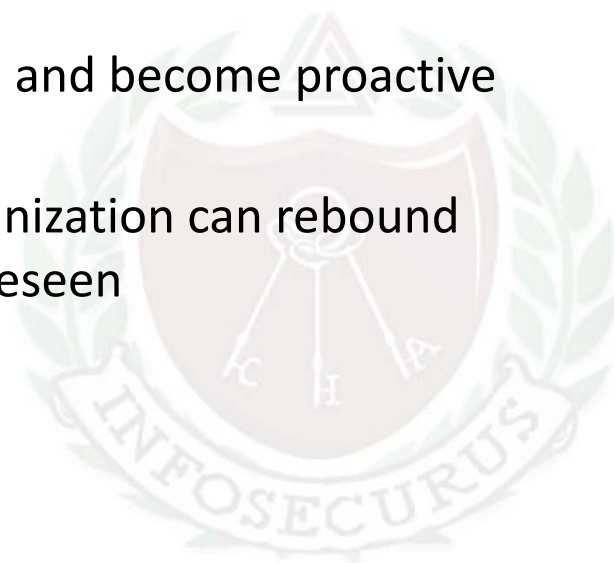
Confidentiality

Integrity

Availability

## Business Continuity & Disaster Recovery Plans

- Fosters the heightened awareness of the most critical business functions
- Provides a strategic initiative requiring detailed documentation of how different business functions interact and inter-operate
- Supports strategic planning for storage capacities, future technology needs
- Enables leadership to plan for foreseeable events and become proactive by enacting preventative control measures
- Most importantly: Is the guide to ensure the organization can rebound from a critical failure or event that can not be foreseen





Confidentiality

Integrity

Availability

# Thank you!

## Questions & Answers

**John H Rogers**

Practice Director

InfoSecurus, Inc

[jhr@infosecurus.com](mailto:jhr@infosecurus.com)

