



Security of personal and financial data

An integrated approach



Introduction

- Enterprise Security Office (ESO)
 - Theresa Masse, CISSP – State CISO
- Technical Team
 - John Ritchie, CISSP
 - Richard Woodford, CISSP
 - Shaun Gatherum, CISSP



Purpose

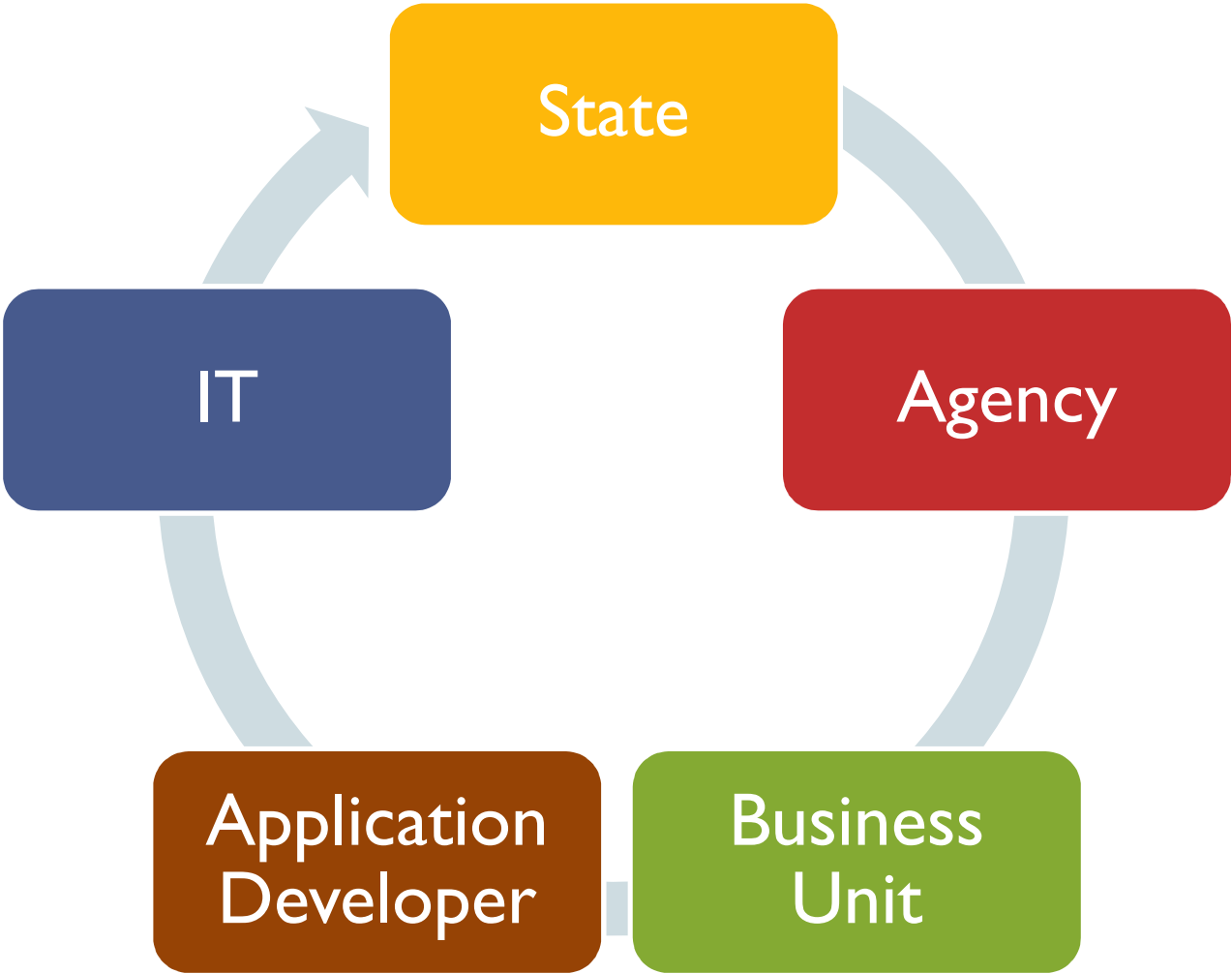
- We are here to...



Outline

- Beyond Compliance
- Know your data
- Application Simulation
- Incident Response
- White Paper
- Questions

Who's responsible





 **The problem with being compliance focused**



Compliant With What

- Payment Card Industry
- NACHA The Electronic Payments Association
- SB583/ Oregon Consumer Identity Theft Protection Act
- State policies
- Federal legislation
 - Federal Information Security Management Act
 - Health Insurance Portability and Accountability Act ...



Compliance and Beyond

- The purpose of compliance
- Security goes further than being compliant
- Security is a business Issue



**BREACHES
BREACHES
BREACHES**





Vermont ski area reports Hannaford-like theft of payment card data

- Okemo says card info was stolen as cards were swiped, as in breach at grocery chain. In a security breach that sounds similar to the one disclosed by Hannaford Bros. Co. last month, the Okemo Mountain Resort ski area in Vermont announced this week that data from more than 46,000 credit and debit card transactions may have been compromised during a system intrusion over a 16-day period in February.

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9074339&source=NLT_VVR&nid=37



Advance Auto says thousands of customers jeopardized in network hack

Advance Auto Parts announced yesterday that its computer network had been hacked, jeopardizing customer information at 14 stores nationwide - The Roanoke-based company says the network intrusion may have compromised the financial information of up to 56,000 American customers. The company is sending out letters directly to customers it has identified as being part of the breach.

<http://www.nbc12.com/news/state/17184761.html>



Hannaford breach illustrates dangerous compliance mentality

By Dennis Fisher Searchsecurity.techtargets.com

- “...The decline in emphasis on security in favor of a sometimes maniacal focus on compliance with various standards and regulations has created a climate in which passing an audit or satisfying a regulator is deemed more important than actually doing what's necessary to protect critical assets...”
- “...It's an easy way of saying, Hey, we did everything we could to protect your data. We met the standard implemented by the credit-card companies themselves. What else could we do?...”



continued

- “...Compliance with PCI, HIPAA, Sarbanes-Oxley or any other regulation simply means that at the time of the most recent audit, the organization met the guidelines set out in the regulation. It does not mean that the organization monitors its compliance with those rules on a continuous basis. It is simply a snapshot of the company's state at one moment in time...”
- http://searchsecurity.techtarget.com/news/column/0,294698,sid|4_gci|308040,00.html



What is security

- **Information security** means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
 - Availability
 - Integrity
 - Confidentiality

 - Authentication
 - Authorization
 - Auditing



Starting points

- Know your information

State Policy Information Asset Classification #107-004-050

- Requires information classification
- Protection is based upon classification

- Know where your information resides/stored, transported etc...

State Policy Transporting Information Assets #107-004-100

- Transporting Information Assets

State Policy Controlling Portable and Removable Storage Devices #107-004-051

- Controlling Portable and Removable Storage Devices



APPLICATION DEVELOPMENT SIMULATION



Banking application requirements

- **Transfer Funds:** The application allows users of the applications to transfer funds from one account to another. The users can transfer funds from one internal account to any other internal account. The application also allows a user to transfer funds from any internal account to an external account. This external account could be an account belonging to any other user of the application.
- **Request a Loan:** The users will be able to request a loan from the application to any of their internal accounts. The interest rates are preset and vary with the loan period of the loan requested. The comments section allows users to add notes and comments while requesting the loan. All valid loan requests are immediately approved.



Banking application requirements

- **Post Messages:** *Posted Messages can be used by the users of the bank to post on messages for all users of the application to view.* This can be used to post ideas, forum discussions or give feedback. Some safe default messages can be viewed by the users of the application
- **Change Password:** The application allows its users to change the password associated with the username. The user needs to provide the old password, the new password and confirm the new password.
- **My Accounts:** As discussed before, the application is preconfigured with default accounts with different account types and cash balances. Every user is assigned at least 2 accounts and can have at most 4 different accounts. More accounts can be added using the Admin interface.



Banking application requirements

- **View Transactions:** Associated with each account is an historical list of transactions. This allows the user to audit the account as required. Associated with all default accounts are some fake transactions.
- **Admin Interface:** The admin interface of the application allows the user to manage, control and configure the application. The access to Admin interface is provided after an authenticated user provides the response to the challenge. This feature is provided to emulate the two factor authentication as closely as possible. The assumption is that only administrator will be able to calculate the response to the challenge officered. For Hackme Bank users the response key is embedded in the web page for ease of use. The response to the challenge is on the upper left corner as displayed in the screen shot.



BANKING DEMONSTRATION



Lessons Learned

- Where in the development life cycle does security belong?
- What controls could have been used in this application?



So you have had a breach

- Incident response
 - Stay calm
 - Have a plan
 - Know who to call
 - How to investigate
 - Verify the breach and exposure
 - Control communication



Where to go from here

- Security program
 - Incident response
 - Business risk assessment
 - Vulnerability / penetration testing
 - Conduct base line analysis
 - Training
 - Policies & procedures
 - Monitor for compliance
 - Audits



Who to contact

- **Theresa Masse (503)378-4896**
Theresa.A.Masse@state.or.us
- **John Dufrene (503)378-3156x254**
Jonathan.E.Dufrene@state.or.us
- **Teresa Pullen (503)378-3156x275**
Teresa.L.Pullen@state.or.us
- **Shaun Gatherum (503)378-5373**
Shaun.A.Gatherum@state.or.us
- **Web site <http://oregon.gov/das/eispd/eso>**