UIIPA - Security Risk Management

June 2015

Introduction

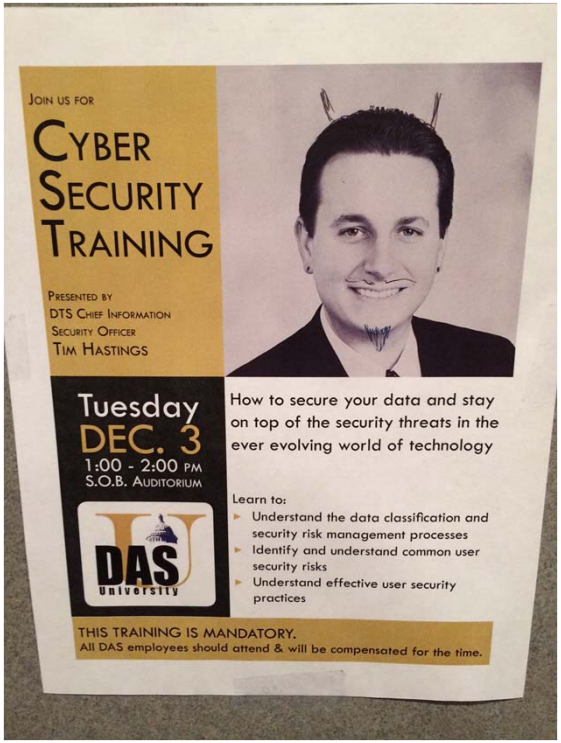
Tim Hastings, Chief Information Security Officer

State of Utah - Department of Technology Services

- Tim Hastings has more than 16 years of experience in assessing and developing information technology, security and privacy processes and controls. Tim specializes in security risk and compliance, working with his clients to build security management programs aimed at achieving compliance, reducing risk and providing enterprise value.
- Tim also understands the importance of evaluating business drivers when incorporating technology and security enablers into the enterprise structure. This understanding comes from a diverse background of services including financial internal and external auditing, performance auditing, quality assurance reviews and data analytics for clients in a variety of industries including technology, telecommunications, public sector, health care, insurance, oil & gas, manufacturing, higher education and consumer business.

Session Objectives

- ❑ **Security risk management strategies**
- ❑ **Secure development lifecycle**
- ❑ **Secure development principles**



Agenda

Data classification

Security risk assessment

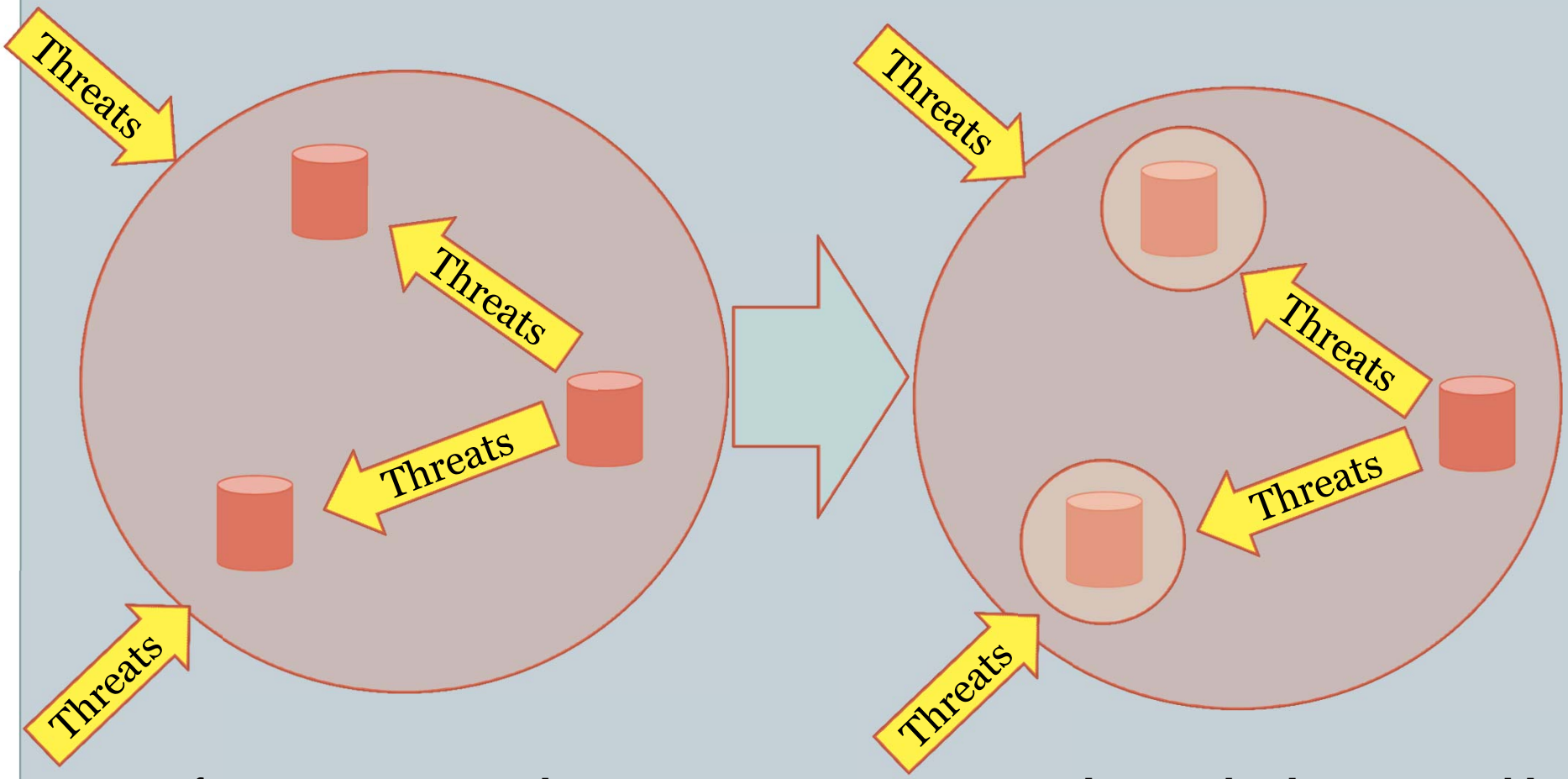
Common user security risks & mitigating techniques

- Physical security
- Social threats
- Logical security
- Mobile devices

A call to action

Data classification
&
Security risk assessment

Protecting data stores



Moving from protection at the perimeter to protection as close to the data as possible.

How do we implement this?

Locate Data

- What data do I have?
- Where is it?
  - In an application
  - On a file share
  - In email
  - Paper copies
  - 3rd parties

Assess Risk

- Is it confidential?
- What would happen if I lose it?
- How hard would it be to recreate?
- Is it regulated?
- How would we continue to operate?

Identify Classes

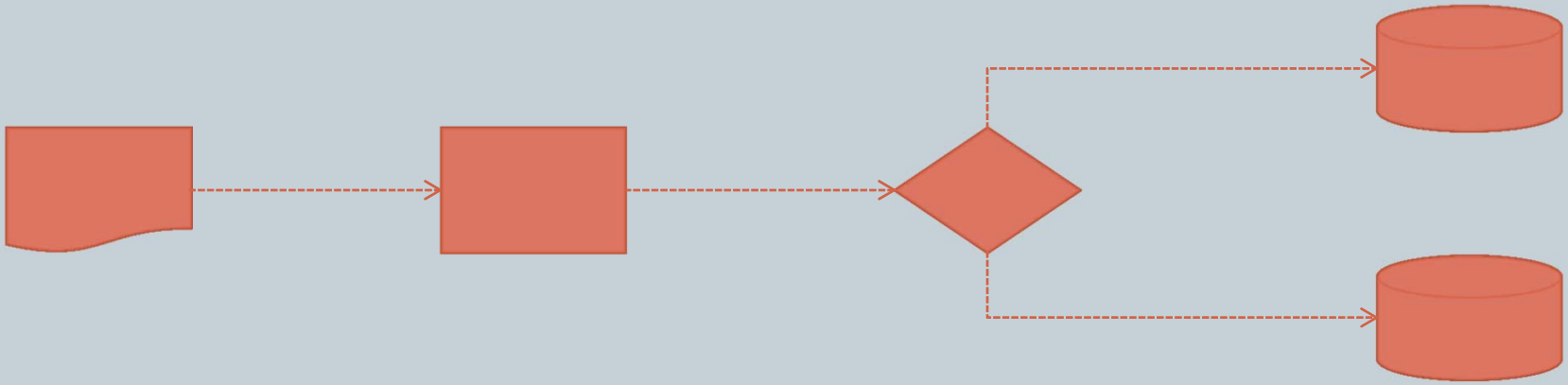
- Based on confidentiality
- Based on business criticality
- Based on regulations
- Make your list meaningful, but brief

Implement Protection

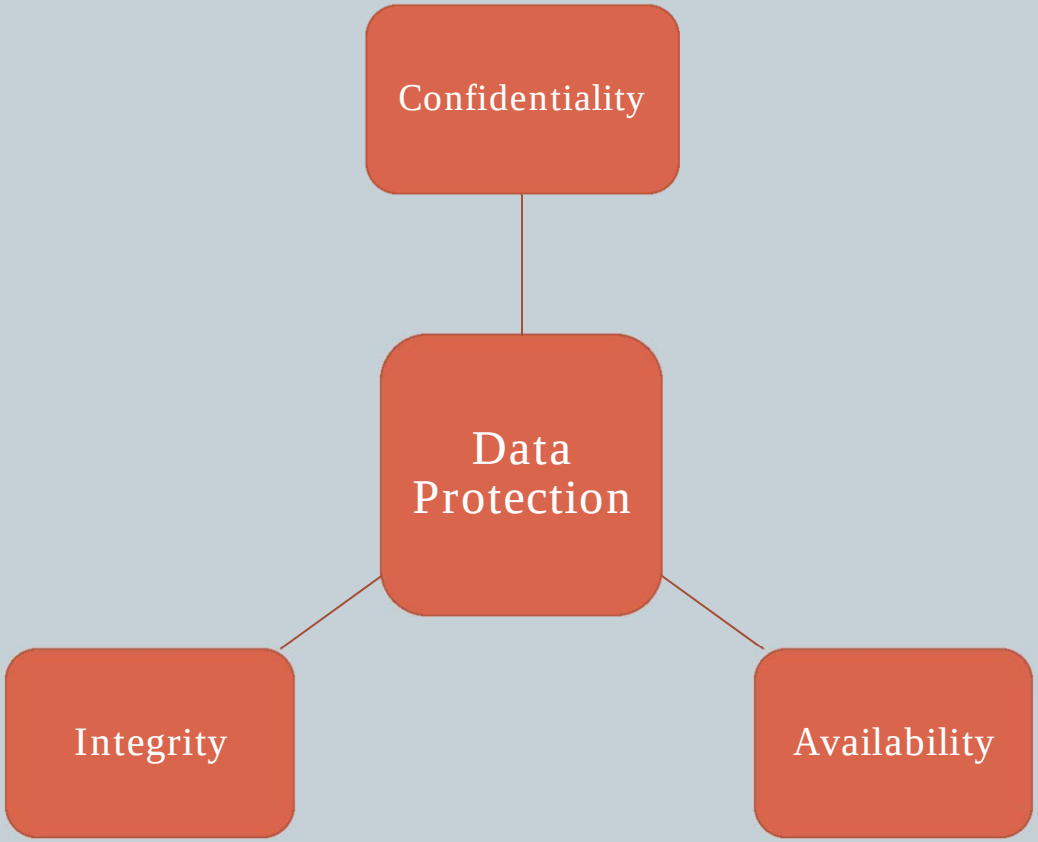
- Protection required for each class
- Enterprise-wide versus system specific

Data store identification

- Work with IT and business leadership to identify data stores used in operations
- For more complex processes, use flow charts
- Identify and limit rogue data stores



Assess risk



- All 3 should be balanced for a strong security program
- Remember that all data sources do not have the same criticality

Identify classes

Example classification:

Highly Confidential	• Personal data combined with health or financial data • Regulated data(FTI, HIPPA, Etc)
Confidential	• Intellectual property
Sensitive	• Names and addresses of customers
Private	• Enterprise financial data
Public	• Public website content

Implement security protection

- Decide on needed security controls based on classification (i.e. should all “highly confidential” classified data be encrypted?)
- Decide which controls should be enterprise wide and which should be application specific
- Track risks and corrective controls for completion
- Revisit classifications and risks identified periodically

Secure Development Lifecycle

Secure SDLC

Source: http://www.cisco.com/web/about/security/cspo/csdl/index.html

Guiding Principles

Domain	Principle
Security foundation	Security policy
	Integrate security into technology SDLC
	Delineate physical and logical boundaries
	Developer training
Risk based	Identify and reduce risk
	Assume external systems are insecure
	Implement tailored security controls
	Consider controls while processing, transmitting and storing data
	Consider custom development

Source: Summarized from http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

Guiding Principles

Domain	Principle
Ease of use	Consider security standards (even open source)
	Develop security requirement with common business language
	Consider designs open for new technology
	Strive for operational ease of use
Increase resilience	Implement layers of security
	Design controls to limit damage and recover quickly
	Plan for expected threats
	Identify and respond to vulnerabilities
	Segment systems based on classification/function
	Design monitoring controls
	Exercise resilience controls

Source: Summarized from http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

Guiding Principles

Domain	Principle
Reduce Vulnerabilities	Strive for simplicity
	Minimize trusted elements
	Implement least privilege
	Secure disposal
	Test for vulnerabilities and flaws
Network	Consider physical and logical controls
	Authenticate users and processes
	Use unique identities

Source: Summarized from http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

Vulnerability Identification Example

Current Scan
Old Scan

Last Scan:
>= 60 days
32 to 60 days
<= 31 days

Score Status: >= 7,001 between 5,001 and 7,000 < 5,000

Agency	Host	Score Status	Risk Score	Last Scan	Incident Number	Risk Acceptance	Risk Acceptance Exp. Date
Technology Services	itas02sat		1,302.23	2014-09-21	INC0215137		
			2,596.40	2014-09-21	INC0215137		
			847.34	2014-09-21	INC0215137		
			5,723.30	2014-09-21	INC0215137		
			847.34	2014-09-21	INC0215137		
			1,664.23	2014-09-21	INC0215137		
			1,664.23	2014-09-21	INC0215137		
			1,664.23	2014-09-21	INC0215137		

A call to action

What should we do?

1. Identify and understand your data sources
2. Create a risk-based approach to your information security program
3. Integrate security into SDLC
4. Formalize security requirements, development and testing

Questions?

Tim Hastings
Chief Information Security Officer, State of Utah
1 State Office Building, 6th Floor
Salt Lake City, UT 84114
Phone: 801.538.3298
thastings@utah.gov