

DASU– Security Risk Management

December 2013



Introduction

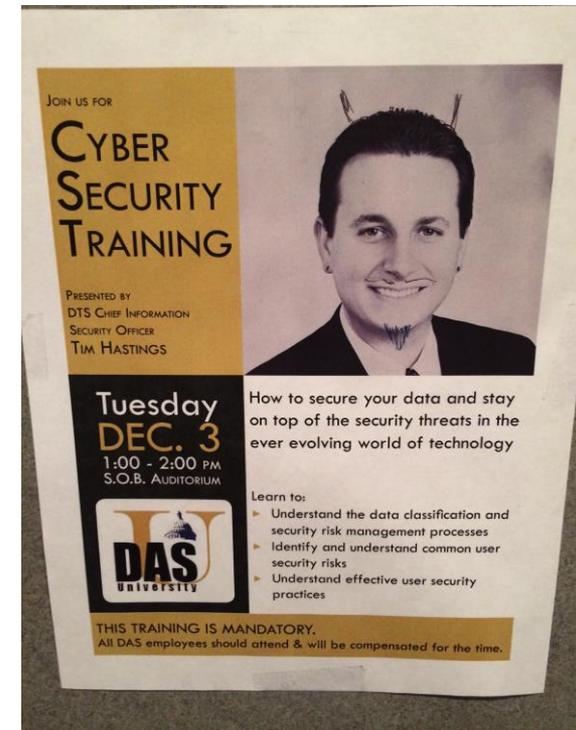
Tim Hastings, Chief Information Security Officer

State of Utah - Department of Technology Services

- Tim Hastings has more than 15 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

- ❑ Understand the data classification and security risk management processes
- ❑ Identify and understand common user security risks
- ❑ Understand effective user security practices



Agenda

3

Data classification

Security risk assessment

Common user security risks & mitigating techniques

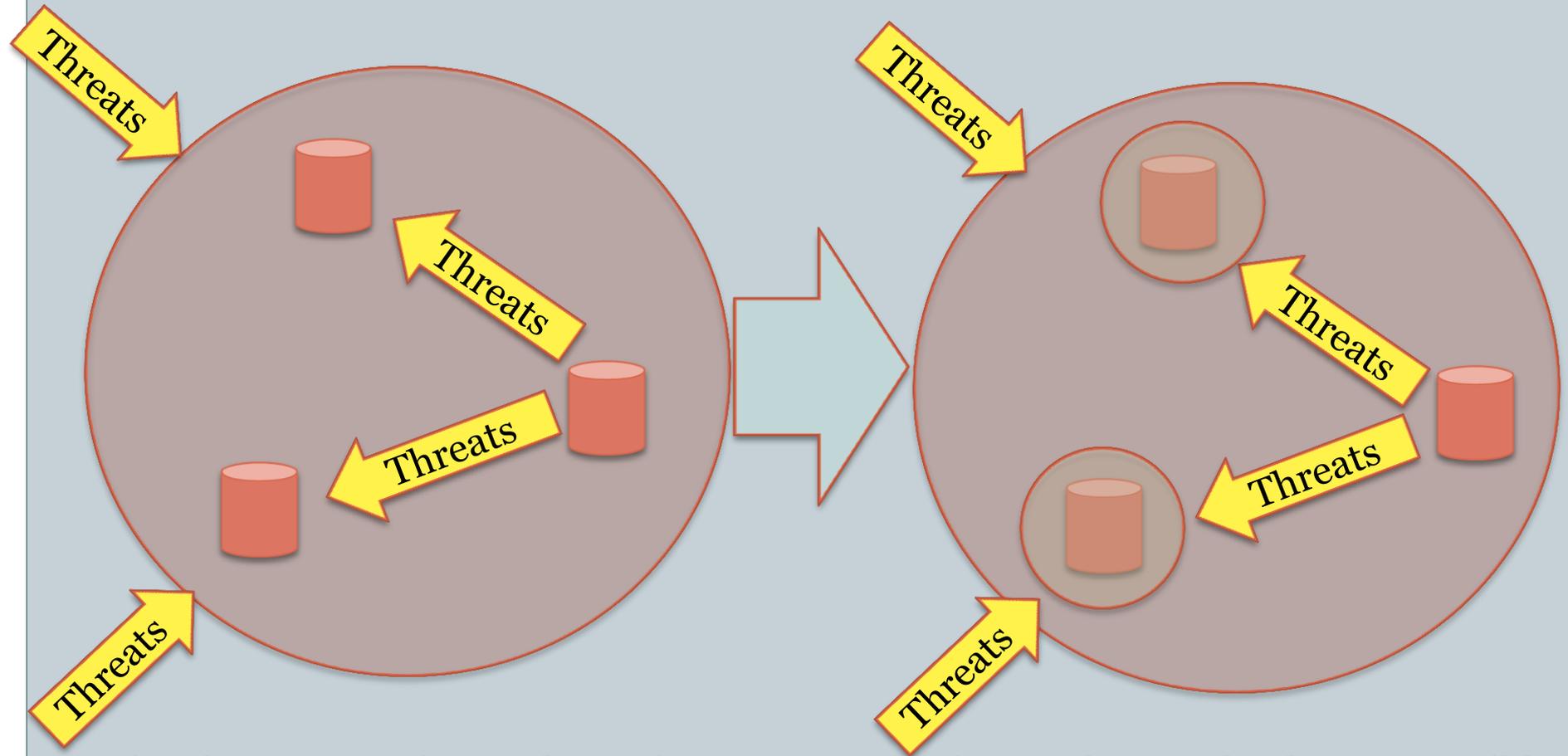
- Physical security
 - Social threats
 - Logical security
 - Mobile devices
-

A call to action

Data classification & Security risk assessment

Protecting data stores

5



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

How do we implement this?

6

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

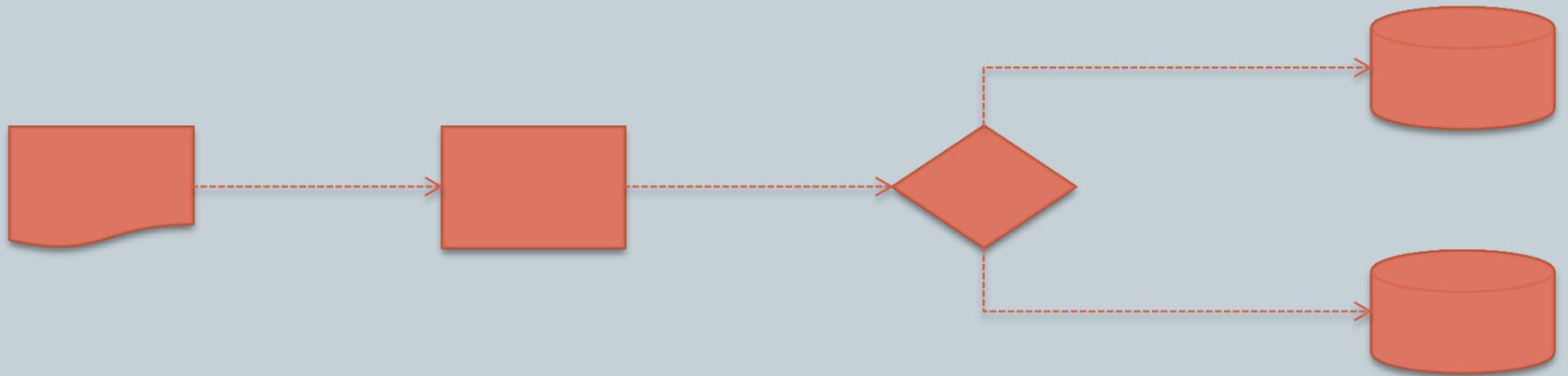
Implement Protection

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

Data store identification

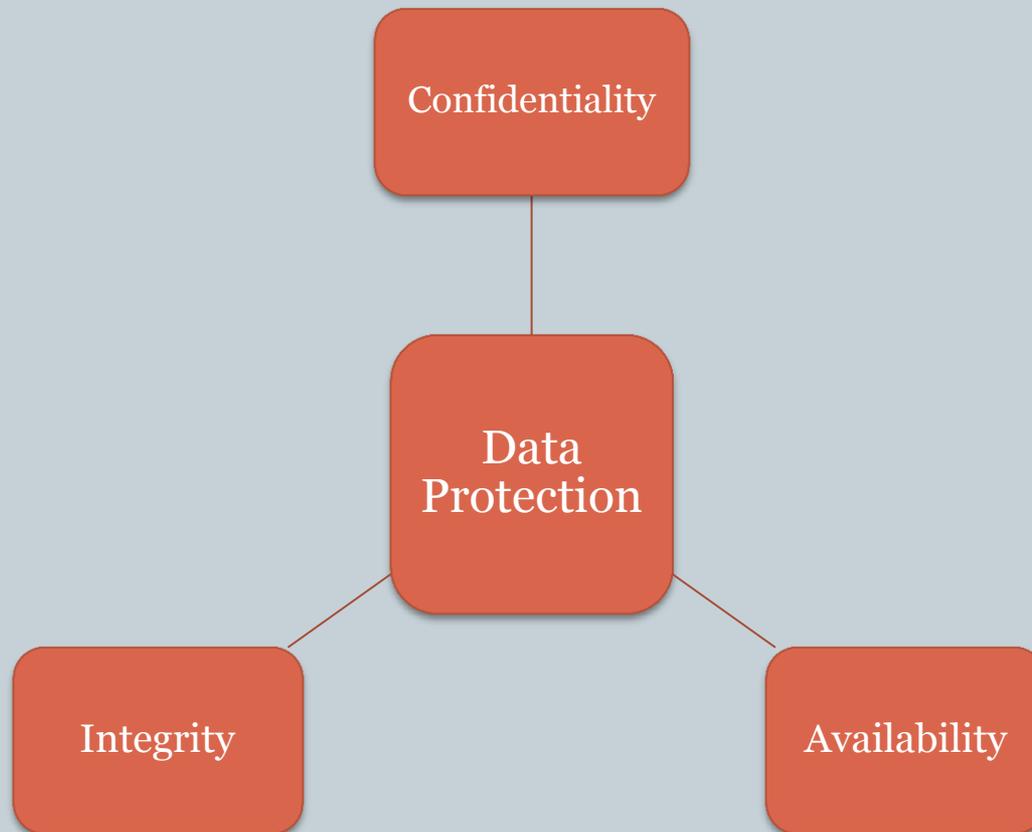
7

- 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

8



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

Identify classes

9

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

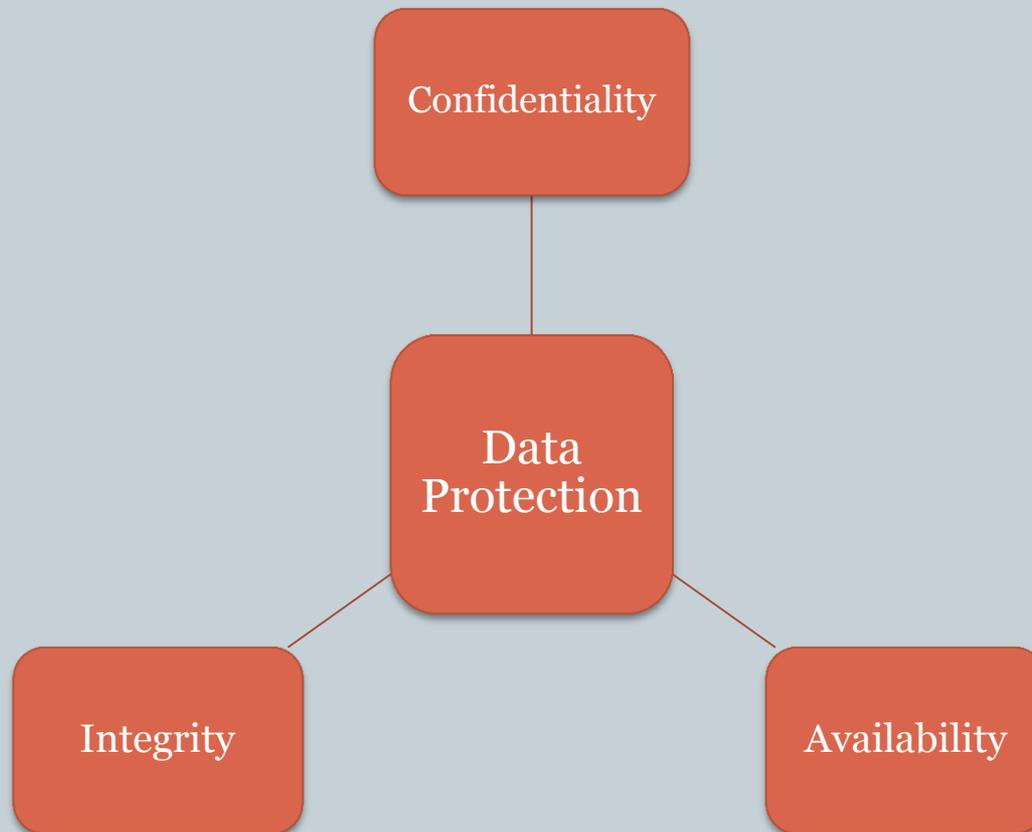
10

- 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

Common security pitfalls and vulnerabilities

Common User Security Vulnerabilities

12



Considering these guiding principles in any given security scenario. The following items give some of the most common pitfalls.

Common User Security Vulnerabilities (cont)

13

Physical security for your workspace:

Item	Description	Solution
Shoulder surfing	Unauthorized individuals viewing the screen while an authorized user has an active session	Be cognizant of who is around you and can view your screen; choose to view sensitive material in a private environment
Unlocked computers	Computer left unattended with an active user session	Lock your computer when you walk away (hit ctrl-alt-del and select “lock this computer” option)
Clean desks	Sensitive papers left on desk after hours	File papers in a locked desk or place them in the locked shred bin
Laptop security	Devices are stolen from home/car	When leaving your laptop unattended, use a locking cable

Common User Security Vulnerabilities (cont)

14

Social threats:

Item	Description	Solution
Social engineering	Attempting to obtain user credentials from a legitimate user (via phone call, email, texting, etc.)	Never share your password with anybody unless you are sure who you are working with
Phishing	Email version of social engineering; these appear to be legitimate, but ask for your credentials	Be cautious of any emails from a user you don't know; Don't click on links in emails unless you are familiar with them
Email attachments	Email attachments are known to have viruses	Don't open attachments you aren't familiar with and/or came from an unknown person

Web page links

15

- Sometimes it hard to know if a web page's link is valid or not! We can't always see what behind the link..
- How do we know when or if to click on a link



Things to consider first:

- Do I know the sender?
- Do I usually get emails from this person or organization with attachments?
- Why would I be asked to log into Gmail when I am already logged into my e-mail?
- Place your cursor over the link in the email. The link name and the pop-up URL should be the same. If not **DO NOT** open the link

Common User Security Vulnerabilities (cont)

16

Logical security vulnerabilities to your data:

Item	Description	Solution
Open-ended user sessions	User who does not log off of an online service	Make sure you log off every session that you initiate and don't just close the browser window
Weak passwords	Passwords with few characters or ones that contain dictionary words	Choose hard to guess passwords to make it harder on the attackers
Unencrypted files	Information which can be read in clear text	Encrypt sensitive information so that it cannot be viewed with out proper authentication
Information sharing	Sharing information that you have access to with those that don't	Consider who you share information with and if they are authorized to see it

Common User Security Vulnerabilities (cont)

17

Mobile device vulnerabilities:

Item	Description	Solution
Unlocked devices	Devices with no Password challenge to use (Smartphone's, IPADS, Etc)	Place a password on any device to enter before it can be used
Anti-virus	Programs which scan inbound email, Web pages for malicious software	Make sure you have Anti-virus program install and the signature file is current (needed for Android devices)
Location services	Many apps you locations services including your camera	Review your devices location permissions and make sure you approve
Device encryption	Unencrypted devices can be viewed by unauthorized users	Encrypt all devices that contain sensitive information

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. Consider the sensitivity of information when sharing with others.
4. How should I share information with others.
5. Be cautious of any unusual activity (emails, websites, people, etc.)

Questions?



Rick Johnson
Capitol Campus Security Analyst,
State of Utah
1 State Office Building, 1st Floor
Salt Lake City, UT 84114
Phone: 801.538.3516
Rickjohn@utah.gov

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