Implementing a Data Security Program at UMass Amherst

Presented by:

Jake Cunningham

Lead Information Security Analyst

University of Massachusetts Amherst

Boston University Security Camp

August 2012

Summary

1. Introduction
2. Data Security Program:
   Goals, Background, Planning Phase, Pilot Phase
3. Data Protection Action Plan in Practice:
   Successes & Challenges
4. Data Security Program Next Steps
5. Measuring Success

Introduction: About UMass Amherst

- Large research university located in Western Massachusetts
- ~ 6,500 faculty and staff
- ~ 27,500 undergraduate & graduate students
- Largest of the 5 UMass campuses

Introduction: About UMass Amherst

- *Central IT*: the Office of Information Technologies (OIT)
- *Departmental IT*: many departments have their own IT staff and equipment
- Benefits & challenges of de-centralized IT on a large University campus

Data Security Program: Goals

- Protect University data
- Comply with relevant laws, regulations & policy
- Educate faculty & staff on the importance of data security & protection
- Reduce the impact of compromised computer systems & networks

Data Security Program: Goals

Increase Faculty/Staff awareness in specific areas:

- *Process* to classify University data
- University's *data classification* categories
- Awareness of *where* their data is stored
- The *consequences & risks* of accidental disclosure, unauthorized access, virus infections & physical loss of devices containing University data

Data Security Program: Background

Data Security Program as a collaborative effort

Project team:

- OIT Information Security Office
- OIT Communications Office
- OIT Help Desk & Software Support
- OIT IT Administrators

Collaboration with campus IT Administrators & other departmental representatives

Data Security Program: Planning Phase

1. Project plan
2. Documentation & reference materials
3. Staff allocation – for training & for assisting with locating, classifying and purging data
4. Pilot program with select departments

Data Security Program: Pilot

Pilot Goals

- Develop relevant documentation
- Identify support issues & gaps
- Test the process of installing and running Identity Finder & cleaning up University data
- Identify roadblocks during & post rollout
- Gather feedback about how to best integrate data scanning and cleanup in departments

Target: Departments with little or no formal IT support & departments with full IT support

Data Security Program: Pilot

Print & Online Documentation

- Overview of the Data Security Program
- Data Protection Action Plan
- Data classification instructions
- Data classification reference
- How to Install & Run Identity Finder (Windows & Mac)
- How to Interpret Identity Finder results
- Identity Finder FAQ
- Handling Recommendations for University data
- Data Security presentation

Data Security Program: Pilot

PHASE 1
Face-to-face-meeting with department head & IT staff (if relevant)

PHASE 2
Data Security presentation to the department as part of staff meeting.
Provide online reference documentation

PHASE 3

Install and run Identity Finder software, clean up or secure the data

Data Security Program: Pilot

Pilot Conclusion & Transition to Production

Pilot showed the project plan & process were successful

Documentation & workflow were refined based on feedback

No clear transition from pilot to production

- Engaged new departments in the process
- Advertised the program to more audiences
- One FTE allocated to provide assistance to departments as part of job responsibilities

Data Protection Action Plan in Practice

Data Security Program

Data Protection Action Plan

- KNOW how data is classified at UMass Amherst
- IDENTIFY: Have an accurate inventory of your data
- PURGE: Keep what's necessary, delete what's not
- SECURE: Handle, store & dispose of sensitive data securely
- DOCUMENT the business processes for the use of sensitive data
- RESPOND: Know how to respond to potential data security incidents
- UNDERSTAND the consequences of a security breach

KNOW How Data is Classified

Successes

- Data classifications are already defined in University policy (*unclassified, operational use only, confidential*)
- Online reference documents made the classifications more accessible

Challenges

- Data owners or custodians are responsible for classifying the data
- Data ownership is sometimes complicated
- The average computer user may still have trouble classifying data

IDENTIFY University Data

Using Identity Finder software to locate sensitive information

- Searches computer file systems for SSNs, credit card & bank account numbers, dates of birth, etc.
- Enterprise version supports scanning on Windows, Mac OS X & remote file shares (SMB, NFS)
- Central console to manage scan policies, schedules & collect search results
- Pushed the software through Active Directory to centrally managed systems
- Made software installers available online to all University employees

IDENTIFY University Data

Successes

- A number of departments installed and ran Identity Finder
- A full-time staff member to give a presentation and assist targeted departments with installing and running the software

Challenges

- Getting people to run the scans, review the results & repeat the process
- Identifying all the possible digital and physical locations where data may be stored
- Identity Finder does not identify data over the network

PURGE: Keep What is Necessary, Delete What is Not

- Using Identity Finder to securely delete (overwrite) files, or redact the sensitive information from files
- Manually deleting files
- Shredding paper and CDs, using file/disk overwriting software or a hard drive/tape de-gausser

PURGE: Keep What is Necessary, Delete What is Not

Successes

- Locating old, forgotten data that survived computer upgrades & other major hardware overhauls

Challenges

- Questions about how long sensitive data needs to be retained

SECURE: Handle, Store & Dispose of Sensitive Data Securely

Successes

- Guidelines on secure handling & storage
- Centralized secure fileserver storage to departments (at a cost)
- Some limited file/folder encryption options (RMS, PGP)

Challenges

- No good centrally managed, ubiquitous encryption solution
- Still difficult to keep data off the desktop, even with central storage
- “Cloud” backup solutions are still problematic

DOCUMENT Business Processes for Sensitive Data

Challenges

- *Intra-departmental coordination*: many departments are large and de-centralized and coordination within a department is tricky

RESPOND: Know How to Respond to Potential Incidents

- Properly responding to computer security or data security incidents is critical
- Proper response can be a factor in whether or not a breach needs to be reported

RESPOND: Know How to Respond to Potential Incidents

Successes

- Developed robust computer incident response procedures
- Provided documentation and presentations to IT Administrators, faculty, and staff on responding to computer security and data security incidents
- Some departments are successful in the initial triage of incidents

Challenges

- Disseminating incident response process information to campus IT administrators and other faculty and staff is time consuming

Data Security Program: Next Steps

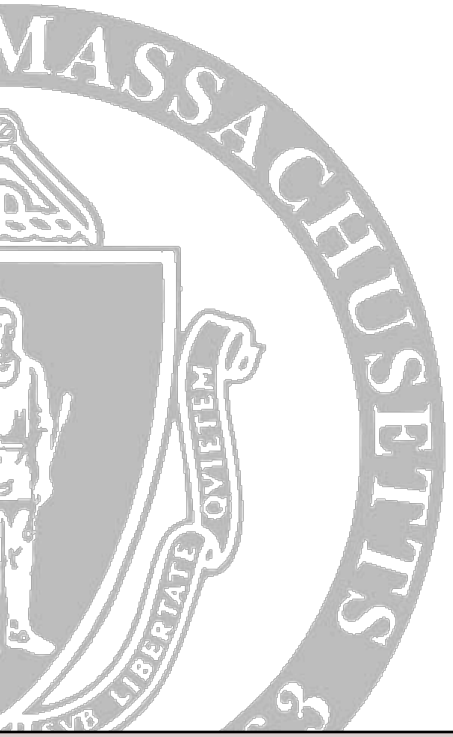
- Continue to encourage departments to go through the iterative process of detecting and securing data
- Continue to offer assistance with the process
- Update & refine documentation and processes as needed
- Focus on resolving process gaps, critical points & challenges
- Consider network-based DLP to complement existing process

Data Security Program: Measuring Success

Financial impact alone is a poor indicator of success
Data breach risks and their realization probabilities are hard to convert into realistic financial measurements

Success criteria

- Ongoing efforts to educate users
- Positively change attitudes & behavior around data security
- A large number of hosts with Identity Finder installed and running scans with no sensitive information found



Questions?

Thank you!

The Data Security Action Plan and associated documents are available at http://www.oit.umass.edu/security