

(More) Lessons Learned

Steve Romig
April 2008

Agenda

- House Bill 104 and OSU: a brief chronology
- OSU's Institutional Data Policy and Data Disclosure Policy
- OSU's Computer Security Standards
- Our Progress So Far
- Other Issues

A Brief Chronology

A Brief Chronology

- February 2006: House Bill 104 goes into effect, mandating that businesses contact individuals if certain personal information is exposed.
- OSU suffers from a series of relatively small disclosure incidents and near-misses, refines its procedures and policies, starts thinking (more) about prevention.
- April 2007: OSU suffers its largest data breach to date - 14,000 names and SSNs exposed through a SQL injection attack on a web server.
- May 2007: I spoke at the ISACA meeting and talked about some of our lessons learned. Hey, deja vu :-)

A Brief Chronology

- April 2007: we start drafting our “Computer Security Standards”.
- Minimum standard posted at the end of the summer, 2007
- Units start reporting monthly status regarding compliance with the Minimum Standard and the Institutional Data Policy in the fall of 2007
- March 2008: initial CC&E requests for the Minimum Standard are due
- April 2008: Critical, Database and Web Standards go into effect

Institutional Data Policy, Data Breach Policy

Institutional Data Policy

- Defines data classifications:
 - Restricted - e.g. SSN, FERPA, PCI
 - Limited Access - e.g. date of birth, purchasing data
 - Public - everything else
- Defines roles: Trustee, Steward, Custodian, User
- Defines mandatory security practices for different data classes
 - e.g. Restricted Data must be encrypted if stored on portable devices

Data Breach Policy

- This defines how OSU intends to comply with HB 104 when “personal information” is potentially exposed.
- Our definitions of “personal information” and “potentially exposed” and “notification” are broader than required by HB 104.
- The policy basically defines the situations it applies to, the people who need to be involved in the investigation, and the procedures for conducting the investigation (at a high level).
- Potential breaches must be reported, investigation performed as directed by the committee, results reviewed by the committee, notification carried out and paid for by the organization(s) involved.

Computer Security Standards

Computer Security Standards

- There are currently 4 standards.
- Minimum Computer Security Standard (MCSS): applies to all computers owned by OSU and all computers attached to the OSU network.
- Critical Computer Security Standard (CCSS): applies to “critical computers”
- Web Server Security Standard (WSSS): applies to critical web servers.
- Database Server Security Standard (DSSS): applies to critical database servers.

Development Process

- These were drafted in April/May 2007
- They were based on NIST's Special Publications 800 series.
- The minimum standard was “fast tracked” and approved with an aggressive implementation plan by the end of the summer (2007)
- The critical, database and web standards have gone through a slower development process, including thorough review by focus groups drawn from IT groups around campus.

How the Standards “Work”

- The standards build on each other:
 - “Everything” must comply with the minimum standard.
 - “Critical” servers must comply with the minimum standard and the critical standard.
 - Critical web and database servers must comply with the minimum and critical standards and also the web/database standard.
- “Critical” means that it contains Restricted Data, or loss of service carries a significant financial liability (or other impact, e.g. loss of reputation), or the owning unit has decided to call it critical.

Includes an Appeals Process

- If you can't comply with one of the standards you can request approval for a Compensating Control or an Exception (similar to what the PCI requirements allow).
- For example, consider a network attached electron microscope. The Minimum Standard requires that it have a host-based firewall but the vendor doesn't support one. So you might request approval for using a small network-based firewall as a compensating control for that element of the MCSS.
- Exceptions can also be requested/granted - this is for cases where there is no suitable compensating control.
- We've created "blanket" compensating controls and exceptions that cover common cases: copiers and printers, switches, routers, etc.

Minimum Standard

- Applies to all computers owned by OSU and to all computers attached to the OSU network
- It contains 4 requirements: use a host-based firewall, use anti-virus and anti-spyware software, keep up-to-date with security patches, and use good passwords.
- It is **not** very specific: no details on how the firewall should be configured, what anti-virus software to use, how soon patches need to be installed, password complexity, etc.
- Upper-management inserted the stipulation that compliance must be automatically audited and enforced.
- We've adopted an aggressive implementation schedule.

Critical Server Standard

- Register critical servers with the security group.
- Use appropriate physical security.
- Backup and recovery requirements.
- Data destruction/surplus requirements.
- Intrusion detection and incident response requirements.
- Logging and monitoring.
- Account and password security requirements.
- Change control procedures.
- Secure SDLC.
- Network and firewall security.

Database Server Standard

- Network and firewall requirements.
- Accounts, passwords, principle of least privilege.
- Installation, configuration.
- Not co-hosted with web server.
- Specifically requires compliance with the IDP regarding Restricted Data.
- Specific logging and monitoring requirements.

Web Server Standard

- Not co-hosted with a database server.
- Installation and configuration.
- Logging and monitoring.
- Encryption, certificates.
- SDLC.

Progress

Progress

- About 70% of the faculty and staff, 24% of the grad students and 33% of the undergrads know about the MCSS.
- After all that effort, only 70% know about it? Yow.
- We have a long way to go with the students.
- About 80% of faculty, staff and undergrads and 73% of the grad students have the host-based firewall turned on. Great!
- About 87% of faculty and the students and 83% of the staff use automatic updates. Also great!
- Between 81 and 84% of the people use anti-malware. Fantastic!
- 63% of the faculty, staff and undergrads require a password to login. Only 48% of the grad students do. Help!!

Problems

Problems

- The 80-20 rule - we're spending 80% of our effort (currently) on 20% of the problem.
- A lot of effort University-wide is going into the implementation of the MCSS.
- The MCSS alone would not have prevented any of the data breaches (or near-breaches) that we've had to date.
- Automating the auditing and enforcement of security policy on devices that you don't own or directly manage is **very** difficult in a large, heterogenous environment.
- NAC is a possible solution for unmanaged devices
- NAC isn't ready for our environment (or visa versa)

Problems

- It is a learning process - people don't understand how the Compensating Controls and Exception request process works.
- We get a lot of requests for compensating controls for cases where they're actually compliant.
- And we get requests for CCs that make no sense: "we have a firewall (that allows access to tcp/80) so we don't need to install patches on the web server because it might break things".
- Searching for Restricted Data is difficult. It might be better to assume that its there and just encrypt portable devices regardless. That's the policy in the Office of the CIO now.

Problems

- The transition to whole disk encryption is difficult. You need good disaster recovery procedures when you make the conversion!
- We got special pricing for PGP.
- The state got special pricing on SafeBoot shortly thereafter.
- Some people at OSU use SafeBoot, some people use PGP. Both products have issues.
- Lack of focused attention is bad, but given the problems with both products maybe allowing for diversity is good?

Problems

- User awareness, training and education is a formidable problem.
- We're having *huge* problems now with webmail spam. Attackers send us "phish" asking for passwords. Some of our users give them their passwords. The attackers use these to login to our webmail system and send spam. This causes operational problems for the mail servers and is a huge security risk for the account owners and for the University.
- The CMU phish study...

Problems

- “Responsive Standard Creation”
 - The usual workflow is slow, slow, slow
 - That’s usually good
 - The security “problem space” changes very rapidly
 - How can we quickly adapt/create standards and policies and get them into the ATE workflow ASAP?

Questions

What Else Are You Doing?

- 2-factor authentication rollout (Office of the CIO, Student Information Systems - 3500+ users)
- Online Institutional Data Policy training
- SSN Reduction efforts
- Whole disk encryption (PGP, SafeBoot, etc.)
- User awareness, training and education efforts

Why Not...

- Why didn't you frame your standards using ITIL/COBIT/FISMA/ISO/XYZZY?
- Simple answer: I don't know anything about ITIL, COBIT, FISMA, or ISO.
- ITIL and ISO cost \$\$ to access. I didn't have access.
- I was already quite familiar with the NIST SP-800 series (the base for FISMA) and they're very available.
- "Revised Draft Ohio Administrative Rule on Sensitive Data Security" requires policy/standards based on the state standards, FISMA, COBIT or ISO.
- OSU is apparently going the ISO route.

References

- Draft Interim University Policy on Disclosure or Exposure of Personal Information: <http://cio.osu.edu/policies/disclosure.html>
- Policy on Institutional Data: http://cio.osu.edu/policies/institutional_data
- University Computer Security Standards: <http://buckeyesecure.osu.edu/Policy/UCSS>
- NIST SP 800 series: <http://csrc.nist.gov/publications/PubsSPs.html>