

Data Minimization: Don't Keep It All Forever!

Brian Davis, Director

Director, Information Security, Policy, and Access

Information Security, Policy, and Records Office (ISPRO)
University of Virginia

Problem: Culture of Keeping It All, Forever

- Think you can never get in trouble for keeping things but you can get in trouble if you get rid of something
- Like to fulfill every request for data
- Electronic storage is cheap
- No one knows what they have
- Data accumulation is easy; data management is hard

Drivers of Change: Effect of Breaches

- Growth of identity theft
- Cost of data exposures
- Bad publicity from data exposures



Drivers of Change: Legal Compliance

- Breach notification
- HIPAA, GLBA, FISMA, PCI
- FERPA, FDA, DFARS
- Research grants
- SSN Remediation
- Retention and Disposition
- Freedom of Information Act
- E-Discovery
- New ones every day...



Drivers of Change: Loss of Internal Control

- Dependence on vendors
 - Who's responsible for data protection?
- Cloud
 - Easy “self-procurement” means we can't track it
- Proliferation of web applications
 - Web app vulnerabilities pose major security threat



GOAL: Data Minimization

- **If you don't use it, you can't lose it!**
- Understand information cycle from birth to death
- Get rid of the toxic waste
- Be released from compliance
- Focus security efforts on remaining stores
 - Identify the critical stuff, consolidate it, protect it
- Security as key stakeholder at each step

CONTEXT: Risk-Based

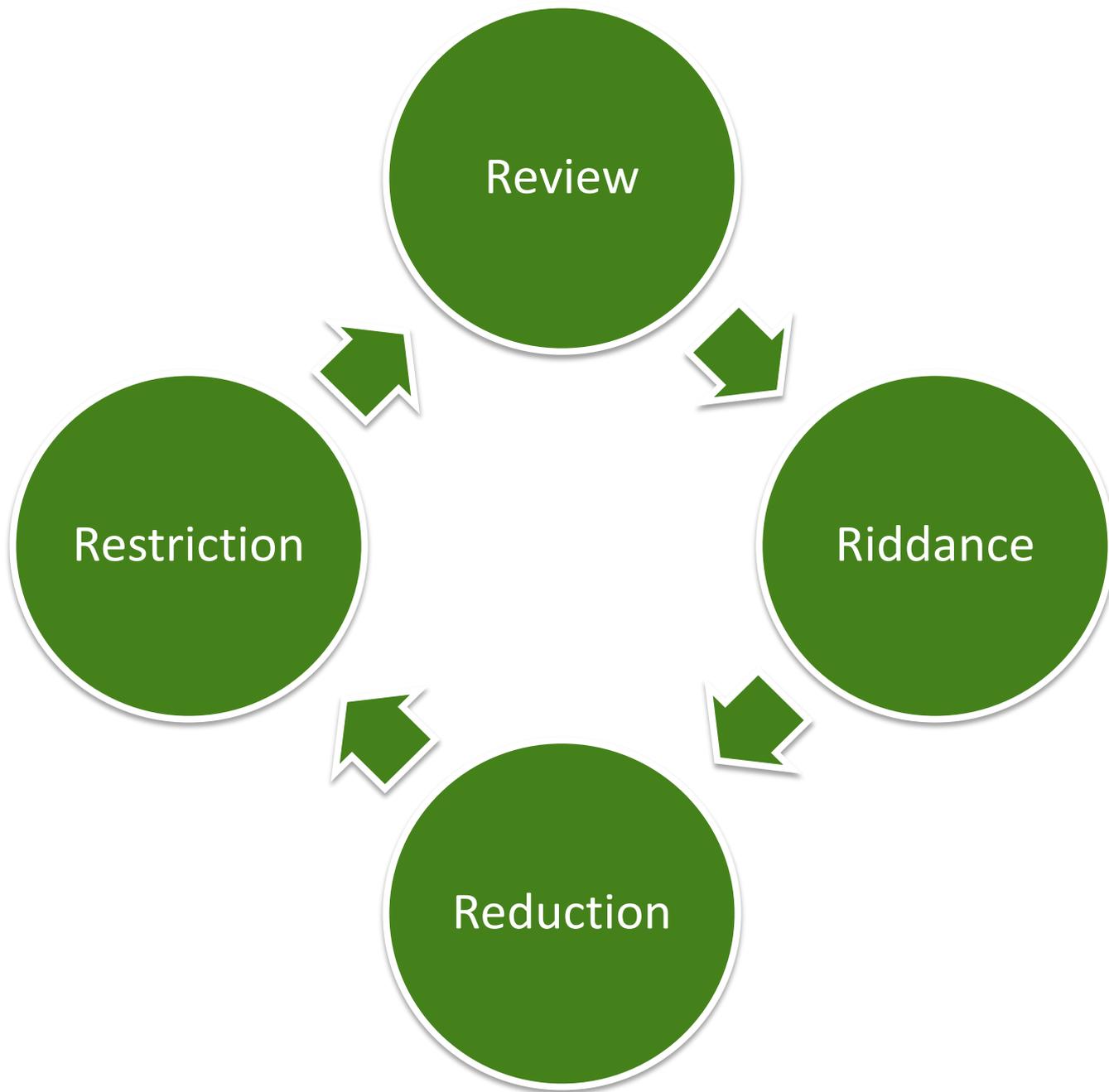
- Understand that no security is absolute
- Greater sensitivity requires higher level of protection
- Focus on effectiveness of controls within context rather than all-inclusive list of thou-shalt-nots
- Balance between security and ability to get necessary work done



PROCESS: Data Minimization



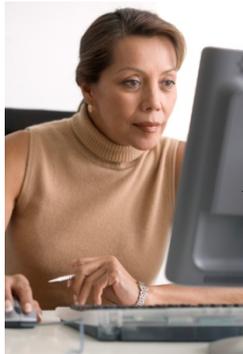
- Review
 - Identify what you have, why you have it, how you use it
- Riddance
 - Don't have to protect what you don't have
 - No legal liability if you don't have covered data
- Reduction
 - If you must have, reduce quantities retained, reproduced, reused, duplicated, displayed, distributed
- Restriction
 - If you must have, restrict access to only those with justified need to use



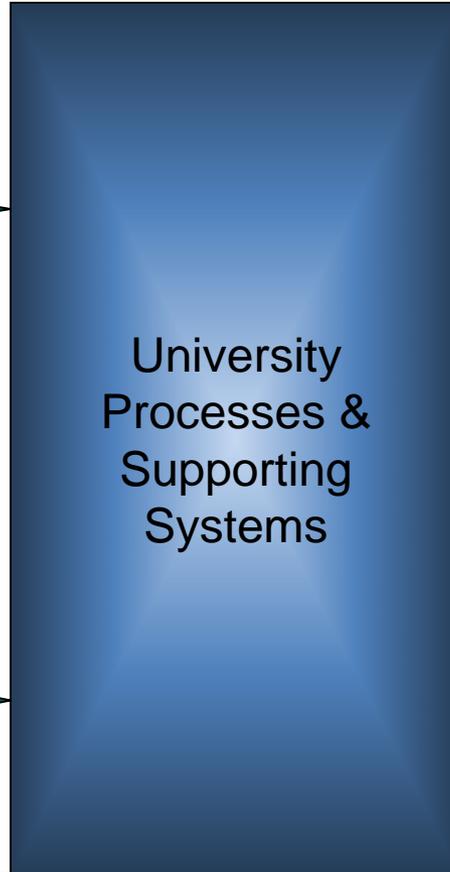
Data Minimization Goals



Confidential data requested only when essential



Confidential data access authorized to least # of people



- Clear confidential data use policy exists
- Responsibilities for data protection well communicated
- Compliance verification processes in place



Confidential data provided only when essential



Confidential data stored only in highly secured devices and file cabinets

A Comprehensive Approach

- [Step 1](#): Create a security risk-aware culture that includes an information security risk management program
- [Step 2](#): Define institutional data types
- [Step 3](#): Clarify responsibilities and accountability for safeguarding confidential data
- [Step 4](#): Reduce access to confidential data not absolutely essential to institutional processes
- [Step 5](#): Establish and implement stricter controls for safeguarding confidential data
- [Step 6](#): Provide awareness and training
- [Step 7](#): Verify compliance routinely with your policies and procedures

Highlights

- Minimized collection and use of SSNs, credit card numbers, HIPAA data, etc.
- Implemented new SSN Protection and Use Policy and Electronic Storage of Highly Sensitive Data Policy
- Scanned individual and shared storage records using Identity Finder
- Intensified University data protection education program
- Revamped data classification and stewardship policy
- Established stricter, mandatory standards for protection data in each classification
- Established significantly enhanced university-wide Records Management Program
- Updated IT Security Risk Management Program

Information Technology Security Risk Management Program

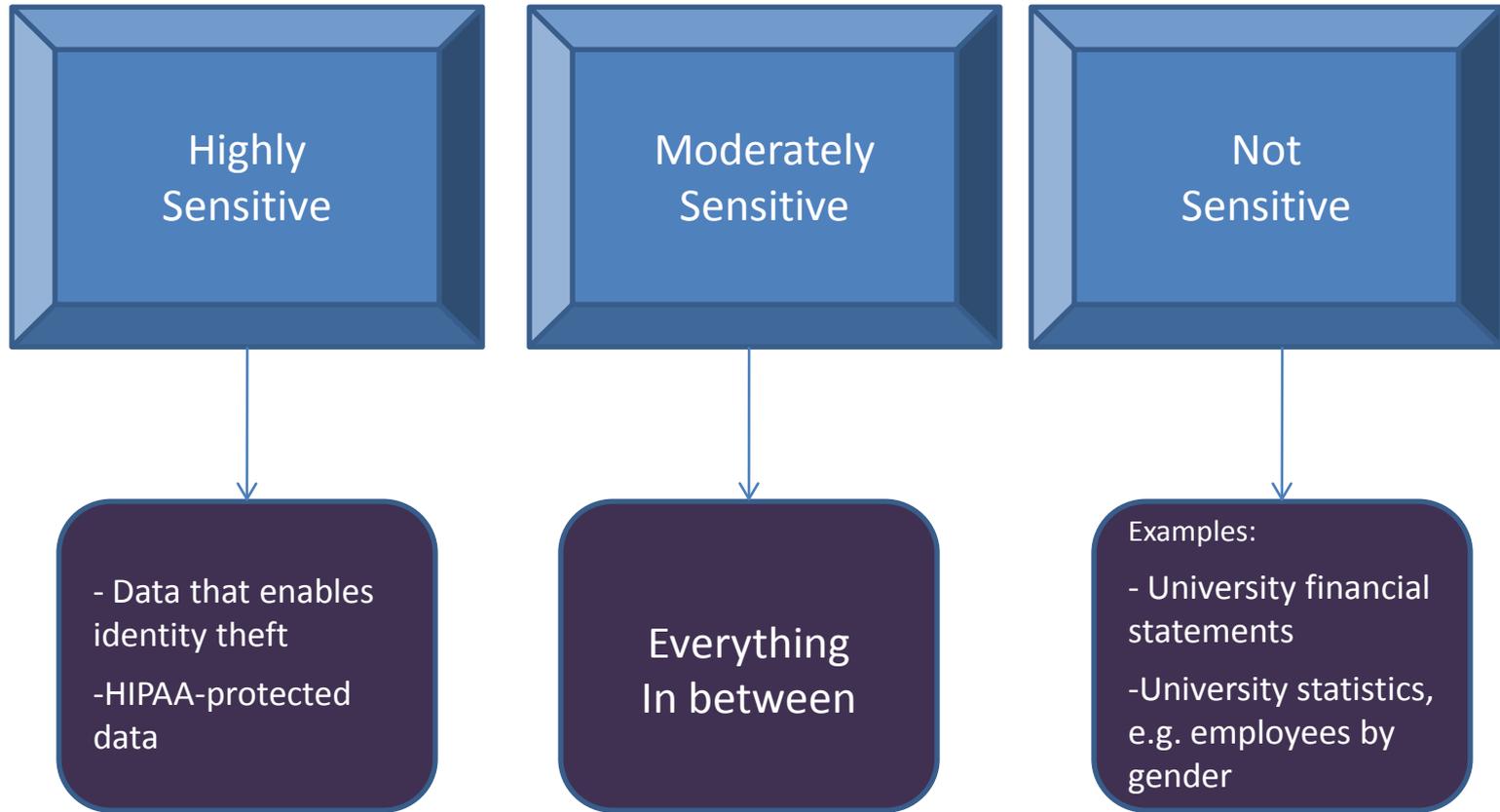
- Includes
 - IT Mission Impact Analysis
 - IT Risk Assessment
 - IT Mission Continuity Planning
 - Evaluation and Reassessment
- Not just equipment and disaster recovery: data and processes
- Repeat every three years; annually if store highly sensitive data; or when you have a significant technology change
- Key initial review and iterative review step



Information Technology Security Risk Management Program

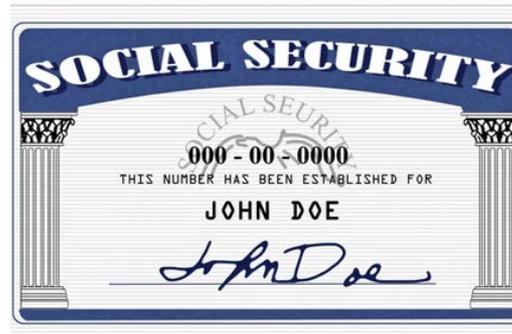
- Although the program includes instructions, templates and guidance, the department needs to own the risk management process
- Departments have to do the work of risk management
- Only departments know their mission, what assets are critical to that mission, how to prioritize resources to address those assets and how best to get back up and functioning following a disaster

Redefined Data Classifications



Social Security Number Remediation

- Comprehensive initiative to phase out use of SSNs wherever possible
- Although SSNs collected where legally required(e.g. W-2 tax forms and financial aid reporting), altered other business functions to use University ID numbers wherever possible
- Need approval before using SSNs in any new way



Social Security Number Remediation

- All departments identified all records and records systems within their purview that use SSNs and developed a remediation plan; once approved, implemented
- Secure remaining SSN stores and sustain continual efforts to rid, reduce and restrict



Electronic Storage of Highly Sensitive Data

- Highly sensitive data (HSD) defined
- HSD can only reside on individual-use devices and media with the approval of the responsible vice president or dean, and then only if the data are encrypted and the device and/or media are protected by strict security requirements



Electronic Storage of Highly Sensitive Data

- Applies to all faculty, staff, and others who electronically store HSD collected on behalf of the University
- Applies to all HSD stored on individual-use electronic devices or electronic media, regardless of whether those devices or media are owned by the University or the individual
- Incentive to keep HSD in central stores
 - Stronger access controls
 - Supervisor approval, two-factor authentication

University Data Protection Standards

- Standards outline requirements for handling and protecting all institutional data
- Determine the sensitivity of the data involved: highly sensitive, moderately sensitive or not sensitive



University Data Protection Standards

- For data of different sensitivities, the standards for the most sensitive data on the system or device should be followed for the entire system or device
- For any standard labeled “recommended, not required,” the standard should be followed unless there is a strong, documented justification for not doing so

Data Protection Standards

Responsibility

- VPs and Deans
- Department Managers & Chairs
- Faculty, staff, student workers, contractors

Transmission

- Email and other messaging services
- Fax
- FTP, HTTP, and other transmission protocols

Storage & Destruction

- General purpose storage and workspaces
- Physical media production and storage
- Destruction of electronic and physical media

Why the “R” in ISPRO?



Data Minimization – With the “R” in ISPRO

- The Role Records Management Plays:
 - Retention and Disposition
 - SSN Remediation
 - Destruction Documentation
 - Electronic Records Management System
 - University Physical Storage Standards



Tools

- Identity Finder
 - Can't deal with data you don't know you have
 - Too much data for humans to parse
- WebApp Scanner
 - Web applications are constantly facing the Internet, they are common targets for attacks
- Templates
 - IT Security Risk Management question sets and plans
 - SSN Inventory and Remediation

Tools

- University Records Management System (URMA)
 - Inventory tool for electronic and paper records
 - Presentation of UVA specific records retention and disposition schedules
 - Electronic version of the Certificate of Records Destruction
 - Identification of historical records and documents

Review

- Information Security Review for Projects Questionnaire
- Data Protection Contractual Language Tool
- Working with Institutional Review Board, Office of Sponsored Projects and other stakeholders
- Annual Security Architecture Reviews
 - Future (dependent on additional resourcing)
 - For those using highly sensitive data
 - Reinforces seriousness of issue and effort required
 - If we don't build in checkups, won't happen

Questions?

Brian Davis

bdavis@virginia.edu

<http://www.virginia.edu/ispro/>