Cybersecurity Regulations for Higher Education and Research

Matt Morton, CISSP, CISM, CGEIT

Executive Director & Chief Information Security Officer

University of Nebraska

matt.morton@nebraska.edu

Overview

- History
- Key cyber regulations for IHE’s
- Calculating the cost of compliance
- Communicating compliance risk to leadership
- Developing a plan to compliance
- Compliance is not security

Key Regulations in Higher Education

Family Educational Rights and Privacy Act (FERPA).

- Prevents institutions from disclosing education records or student PII without written consent;

Federal Information Security Modernization Act of 2014 (FISMA 2014).

- Requires Federal data to be secure;

Gramm-Leach-Bliley Act (GLBA) (1999).

- Requires "financial institutions," including colleges and universities, to ensure the security and confidentiality of customer PII;

Health Insurance Portability and Accountability Act (HIPAA).

- Requires institutions to protect health records and other identifiable health information via privacy safeguards and by limiting use and disclosures without authorization;

Higher Education Act (HEA)

- Requires IHEs with Title IV programs to have policies, safeguards, monitoring, and management practices related to information security;
- Recent Memos tie Title IV programs to GLBA and NIST 800-171.

Student Aid Internet Gateway (SAIG) Enrollment Agreement.

- Requires IHEs with Title IV programs to ensure that all Federal Student Aid applicant information is protected.

NIST 800-171	• Standards for controlled Unclassified Information
Missouri § 407.1500 RSMo.	• Breach/Privacy notification for State of Missouri residents

Key Regulations in Higher Education (cont'd)

Family Educational Rights and Privacy Act (FERPA)

- Data can be shared with:
  - School officials with legitimate educational interest;
  - Other schools to which a student is transferring;
  - Specified officials for audit or evaluation purposes;
  - Appropriate parties in connection with financial aid to a student;
  - Organizations conducting certain studies for or on behalf of the school;
  - Accrediting organizations;
  - To comply with a judicial order or lawfully issued subpoena;
  - Appropriate officials in cases of health and safety emergencies; and
  - State and local authorities, within a juvenile justice system, pursuant to specific State law.

Gramm Leach Bliley Act (GLBA) Safeguards Rule (1999)

- Requires **financial institutions** to explain their information-sharing practices to their customers and to safeguard sensitive data
  - Organizations that offer consumers financial products or services like loans, financial or investment advice, or insurance.
- Create an **information security program** based on a risk level relevant to your institution's size and complexity and that accounts for the sensitivity of data you use?
- Do a risk assessment and **mitigate the risks** that you identify?
  - *This is a foundational methodology of information security practice.*
- Designate an **official responsible** for the program?
- Include **training and awareness** as part of the program?
- Pay attention to what **service providers** are doing with your data?

Dear Colleague

Protect student financial aid information under the Program Participation Agreement (PPA) and GLBA

all users are aware of and comply with all of the requirements to protect and secure data from Departmental sources using SAIG.

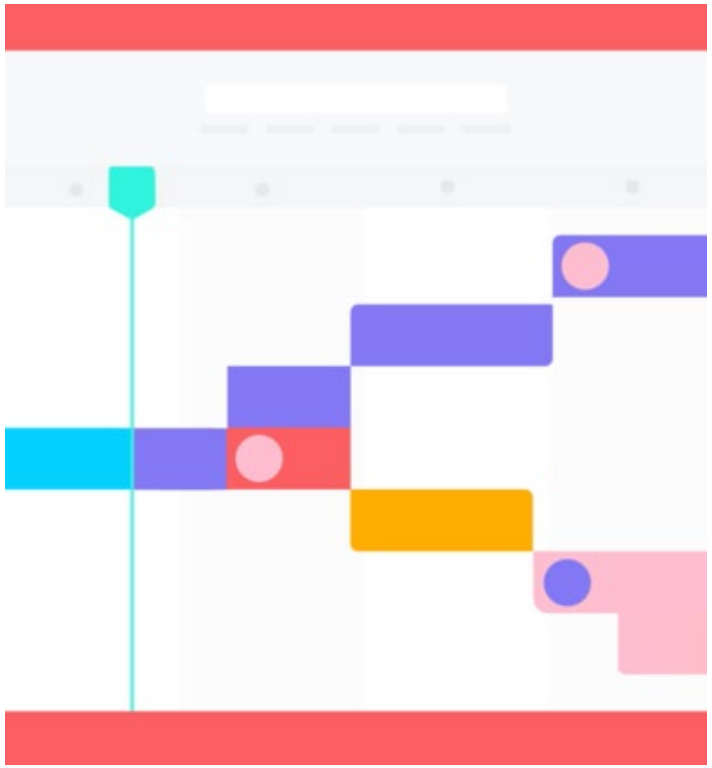
We also advise institutions that important information related to cybersecurity protection is included in the National Institute of Standards and Technology (NIST) Special Publication 800-171 (NIST SP 800-171). Specifically, the NIST SP 800-171 identifies recommended requirements for ensuring the appropriate long-term security of certain Federal information in the possession of institutions.

Draft Audit Language

- Starting in 2018, GLBA information security safeguards will be audited to ensure administrative capability. Draft audit language:
- Audit Objectives – Determine whether the IHE designated an individual to coordinate the information security program; performed a risk assessment that addresses the three areas noted in 16 CFR 314.4 (b) and documented safeguards for identified risks.
- Suggested Audit Procedures
  - Verify that the IHE has designated an individual to coordinate the information security program.
  - Obtain the IHE risk assessment and verify that it addresses the three required areas noted in 16 CFR 314.4 (b).
  - Obtain the documentation created by the IHE that aligns each safeguard with each risk identified from step b above, verifying that the IHE has identified a safeguard for each risk.

Recent Events (Potential delay)

- Educause statement (2018)
  - *Again, the good news is that institutions may have more time to prepare for an eventual audit of their GLBA Safeguards Rule compliance along the lines indicated in FSA's draft objective. But until FSA and/or OMB provide final confirmation, EDUCAUSE members should take this opportunity to conduct a compliance "dry run" to ensure they are ready regardless of whether the objective emerges in the FY18 or FY19 federal single audit.*
- From GAO
  - ***According to an FSA official, the anticipated update to the OMB Compliance Supplement is planned for 2019.***
- https://er.educause.edu/blogs/2018/3/gao-safeguards-rule-audit-objective-may-wait-until-2019
- *The likelihood that FY19 will see the introduction of auditing for college and university compliance with the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule makes this a great time to review the Rule's history, requirements, and institutional next steps. – Jarrett Cummings*



Timeline

- Title IV schools are financial institutions per *Gramm-Leach-Bliley Act* (GLBA, 2002)
  - Per FSA PPA & SAIG agreements, these schools must have GLBA safeguards in place. Schools without GLBA safeguards may be found administratively incapable (unable to properly administer Title IV funds).
- Reminder to protect student data
  - https://ifap.ed.gov/dpcletters/GEN1518.html
- Letter that added NIST 800-171 (July 1 2016)
  - https://ifap.ed.gov/dpcletters/GEN1612.html
- March 1, 2018 (apparent delay)
- October 9, 2018
  - *"The likelihood that FY19 will see the introduction of auditing for college and university compliance with the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule makes this a great time to review the Rule's history, requirements, and institutional next steps."*
  - Jarret Cummings, EDUCAUSE Senior Advisor, Policy and Government Relations

Addition of NIST 800-171

NIST has provided non-FISMA guidelines (800-171) that are recommended by FSA & Education in GEN 16-12 which gives specific technical standards to prove GLBA compliance:

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment Requirements
- Security Assessment Requirements
- System and Communications Protection
- System and Information Integrity

NIST Cybersecurity Framework

- Consists of three fundamental components:
  - Framework core: set of information security activities an organization is expected to perform and their desired results
  - Framework tiers: help relate the maturity of security programs and implement corresponding measures and functions
  - Framework profile: used to perform a gap analysis between the current and a desired state of information security/risk management

NIST Cybersecurity Framework

- Seven-step approach to implementing/improving programs:
  - Prioritize and scope
  - Orient
  - Create current profile
  - Conduct risk assessment
  - Create target profile
  - Determine, analyze, prioritize gaps
  - Implement action plan

NIST 800-171a

Who does this affect?

- A DOD contractor operates two types of information systems
- Federal Information System
  - An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
- Non-federal Information System
  - An information system that does not meet the criteria for a federal information system.
- Contractor information system:
  - An information system belonging to, or operated by or for, the Contractor.
- Anyone with whom federal data is shared under a contract or agreement

NIST 800-171 Goals

- Security supports the mission of the organization and is an integral element of sound management.
- Security should be cost effective; owners have security responsibilities outside their own organizations.
- Security responsibilities and accountability should be made explicit; security requires a comprehensive and integrated approach.
- Security should be periodically reassessed; security is constrained by societal factors.

Purpose of 800-171

- *set of recommended security requirements for protecting the confidentiality of CUI when such information is resident in nonfederal systems and organizations; when the nonfederal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government wide policy for the CUI category or subcategory listed in the CUI Registry.*
    - NIST Document

Definitions

- CUI – Controlled Unclassified Information
  - shared by the federal government with a nonfederal entity and when no other federal law or regulation (e.g., FISMA) addresses how to protect the underlying data

Federal Data – what is CUI?

- NIST 800-60 – PDF contains outline
- https://www.archives.gov/cui

Types

Table 4: Mission-Based Information Types and Delivery Mechanisms[14]

Mission Areas and Information Types [Services for Citizens]

D.1 Defense & National Security
Strategic National & Theater Defense
Operational Defense
Tactical Defense

D.2 Homeland Security
Border and Transportation Security
Key Asset and Critical Infrastructure Protection
Catastrophic Defense
Executive Functions of the Executive Office of the President (EOP)

D.3 Intelligence Operations
Intelligence Planning
Intelligence Collection
Intelligence Analysis & Production
Intelligence Dissemination
Intelligence Processing

D.4 Disaster Management
Disaster Monitoring and Prediction
Disaster Preparedness and Planning
Disaster Repair and Restoration
Emergency Response

D.5 International Affairs & Commerce
Foreign Affairs
International Development and Humanitarian Aid
Global Trade

D.6 Natural Resources
Water Resource Management
Conservation, Marine and Land Management
Recreational Resource Management and Tourism
Agricultural Innovation and Services

D.7 Energy
Energy Supply
Energy Conservation and Preparedness
Energy Resource Management
Energy Production

D.8 Environmental Management
Environmental Monitoring and Forecasting
Environmental Remediation
Pollution Prevention and Control

D.9 Economic Development
Business and Industry Development
Intellectual Property Protection
Financial Sector Oversight
Industry Sector Income Stabilization

D.10 Community & Social Services
Homeownership Promotion
Community and Regional Development
Social Services
Postal Services

D.11 Transportation
Ground Transportation
Water Transportation
Air Transportation
Space Operations

D.12 Education
Elementary, Secondary, and Vocational Education
Higher Education
Cultural and Historic Preservation
Cultural and Historic Exhibition

D.13 Workforce Management
Training and Employment
Labor Rights Management
Worker Safety

D.14 Health
Access to Care
Population Health Mgmt & Consumer Safety
Health Care Administration
Health Care Delivery Services
Health Care Research and Practitioner Education

D.15 Income Security
General Retirement and Disability
Unemployment Compensation
Housing Assistance
Food and Nutrition Assistance
Survivor Compensation

D.16 Law Enforcement
Criminal Apprehension
Criminal Investigation and Surveillance
Citizen Protection
Leadership Protection
Property Protection
Substance Control
Crime Prevention
Trade Law Enforcement

D.17 Litigation & Judicial Activities
Judicial Hearings
Legal Defense
Legal Investigation
Legal Prosecution and Litigation
Resolution Facilitation

D.18 Federal Correctional Activities
Criminal Incarceration
Criminal Rehabilitation

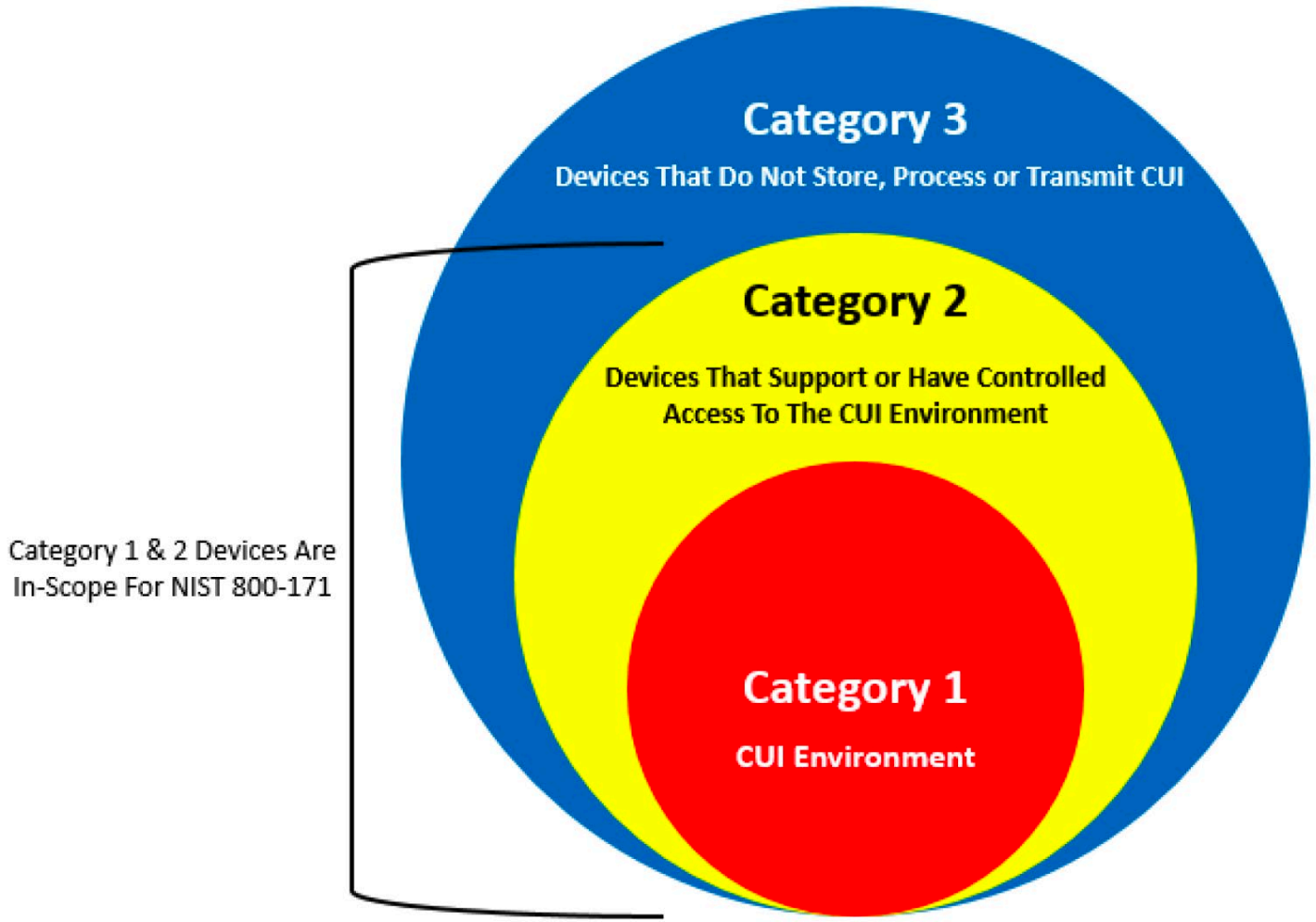
D.19 General Sciences & Innovation
Scientific and Technological Research and Innovation
Space Exploration and Innovation

Types

Table 4: Mission-Based Information Types and Delivery Mechanisms[14]

Services Delivery Mechanisms and Information Types [Mode of Delivery]		
D.20 Knowledge Creation & Management	**D.22 Public Goods Creation & Management**	**D.24 Credit and Insurance**
Research and Development	Manufacturing	Direct Loans
General Purpose Data and Statistics	Construction	Loan Guarantees
Advising and Consulting	Public Resources, Facility and Infrastructure Management	General Insurance
Knowledge Dissemination	Information Infrastructure Management	**D.25 Transfers to State/ Local Governments**
D.21 Regulatory Compliance & Enforcement	**D.23 Federal Financial Assistance**	Formula Grants
Inspections and Auditing	Federal Grants (Non-State)	Project/Competitive Grants
Standards Setting/Reporting Guideline Development	Direct Transfers to Individuals	Earmarked Grants
Permits and Licensing	Subsidies	State Loans
	Tax Credits	**D.26 Direct Services for Citizens**
		Military Operations
		Civilian Operations

NIST 800-171a Scoping



GDPR – Adopted April 2016

- **Increased Territorial Scope (extraterritorial applicability)**
- **Penalties**
- **Consent**
- **Breach Notification**

In force May 25th 2018

- **Right to Access**
- **Right to be Forgotten**
- **Data Portability**
- **Privacy by Design**
- **Data Protection Officers**

GDPR Rules

- Article 15
  - grants the "right of access” requiring the RCB to detail what (and how) personal data is being processed
- Article 17
  - grants the "right to be forgotten” to ensure personal data is deleted when requested
- Article 20
  - grants the "right of portability” to enable individuals transfer personal data between companies upon request
- Articles 25 & 32
  - requires companies to implement reasonable data protection measures to protect individuals data and privacy

GDPR Rules cont’d

- Articles 33 & 34
  - requires companies to report data breaches to supervisory authorities and individuals affected within 72 hours
- Article 35
  - requires companies to perform data impact assessments to identify risks; and develop plans to remedy risks
- Article 37
  - requires the appointment of a data protection officer to oversee GDPR compliance (not in IT)

Personal Data

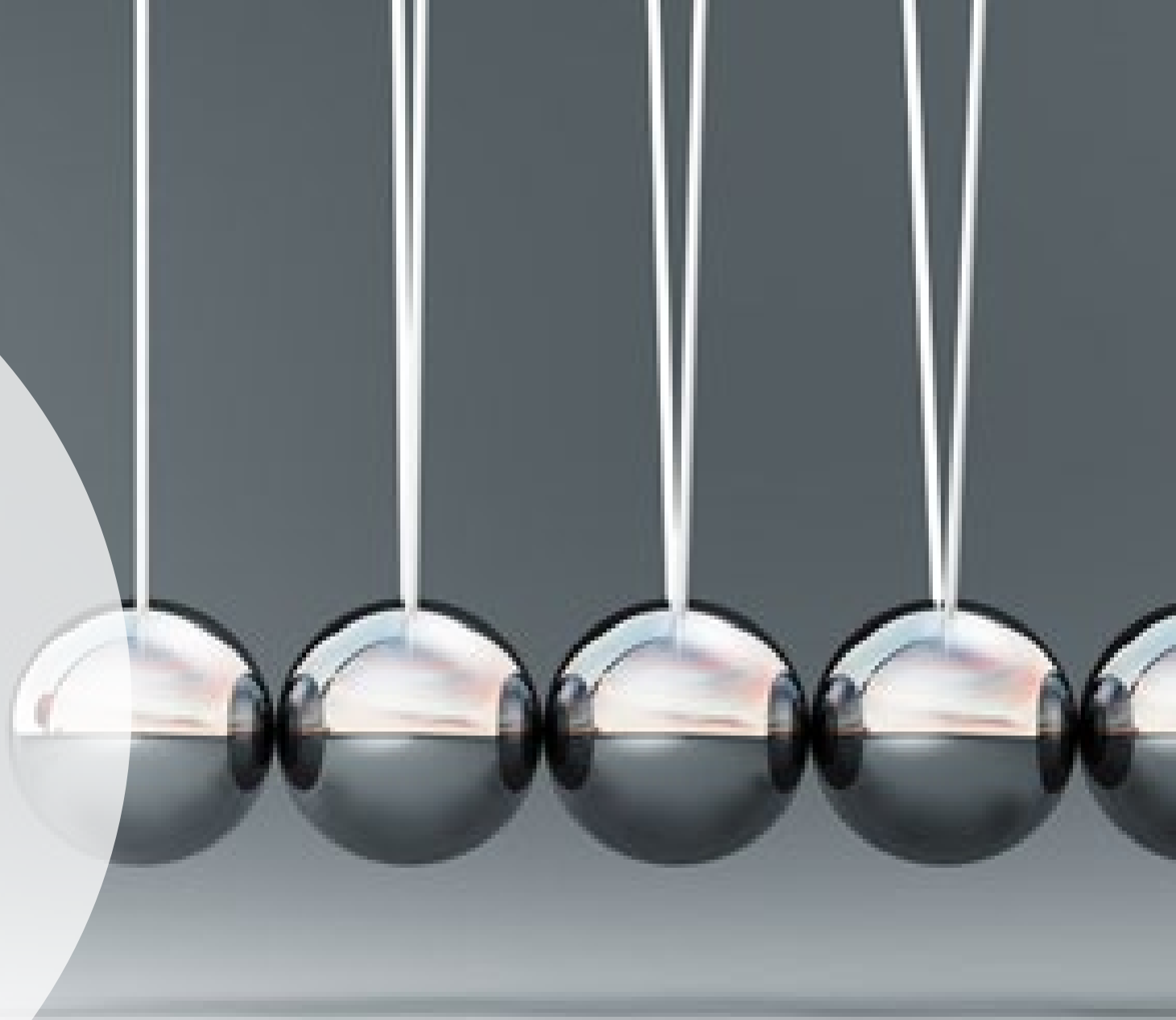
- Name
- Address
- Date of Birth
- ID Numbers
- Health Information
- Income
- Religious Preference
- Family Status
- Race
- Sexual Orientation

Action

- Review all personal data that you hold and, if consent is relied upon, check that it has been obtained correctly
- Review all policies and procedures. Ensure they cover all the rights individuals are entitled to
- Plan how you will access requests for data
- Security
  - check what security systems are in place to protect personal data. Know what to do if there is a security breach
- Communication
  - Become informed; tell your staff, committees, etc.

Impact

- New Technologies
- Effort around SIS to develop required use cases
  - “Right to be forgotten”
  - “Where is the data”
- Financial Cost for EU startup operations
- Fines for non-compliance
  - 4% of annual revenue
  - Or 20 million euros which is greatest
- 8.8 billion dollar lawsuits on Facebook & Google on “day one”
- Latest Facebook breach will be subject to this as well



Survey of R1 Universities

- 6% have not started
- 55% just getting started
- 39% actively working on it
- Primary roles engaged
  - General Counsel
  - CISO
  - Compliance

Cost of regulation

- 2011 – 3.5 million on average 9.4 million to be non-compliant
- 2017 – 5.47 million - 14.82 million to be non-compliant
- Key 45% increase in organizational cost
- Education – 6.8 million to 9.8 million

Gauging risk

Communicating risk to leadership

- Build a profile of each member.
- Consider backgrounds when developing your presentation.
- Ask about questions about priorities, risk, tolerance, and reputation.
- Have facts ready
  - How many apps impacted
  - Where are our operations?
  - How many students are in “scope”
  - How many vendors are in scope?
  - How many employees are in scope?

GDPR RISK

Developing the plan

- 5 easy steps
  - Identify highest risk compliance requirements
  - Have a gap assessment done
  - Map gaps to other compliance requirements
  - Prioritize based upon the # of matrixed objectives
  - Develop a timeline for compliance based upon priorities and gaps
  - Track Progress

GDPR Gap Assessment

Sheet


Questions?

Resources

- Research Security Plan Development
  - http://www1.udel.edu/security/research/
- **The GLBA Safeguards Rule at 15**
  - https://er.educause.edu/articles/2018/10/the-glba-safeguards-rule-at-15
- https://library.educause.edu/resources/2014/5/information-security-guide-effective-practices-and-solutions-for-higher-education
- https://ifap.ed.gov/eannouncements/Cyber.html
- https://www.networkworld.com/article/2199260/compliance/cost-of-regulatory-security-compliance--on-average---3-5m.html