Cyber Security Disclosures

The SPARK Institute

Presenters

GROOM LAW GROUP
CHARTERED

Allison Itami

Callan

Ben Taylor

Contents

Today's Measure of Cyber Security Adequacy

Behind Closed Doors

Evaluators Traditionally Not Trained as Experts

Destructive Information Cycle

Regulatory Environment

PROTECTING AMERICA'S CONSUMERS

Gramm Leach Bliley

ERISA

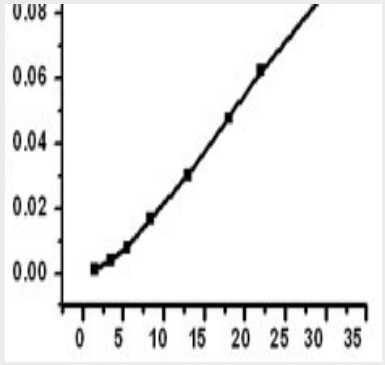
International Regulations

Governmental Plans

State Statutes

NCSL
NATIONAL CONFERENCE of STATE LEGISLATURES

Background & History



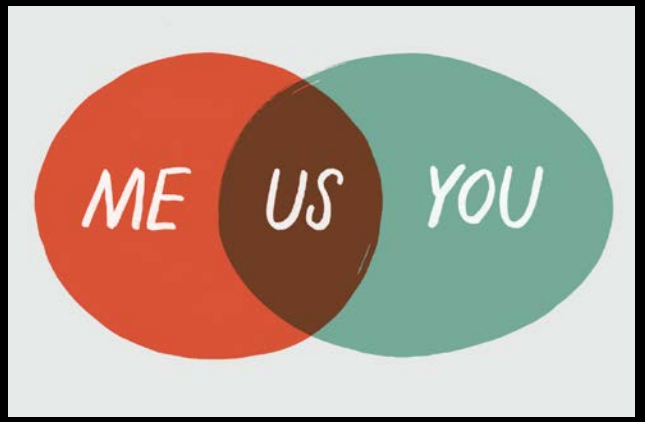
Proliferation of Questions

Intimacy of Questions & Secrecy of Answers

Refusal to Answer to Protect Other Clients

Development Process

SPARK Data Security Oversight Board



Collaborated

Examined Possibilities

Decided on an Approach

First Priority

Third Party Attestations

Flexibility

Security Framework Flexibility

- Agreement on a single framework is not possible
- A single framework is NOT Desirable
- Diverse Frameworks make a stronger defense

NIST National Institute of Standards and Technology U.S. Department of Commerce

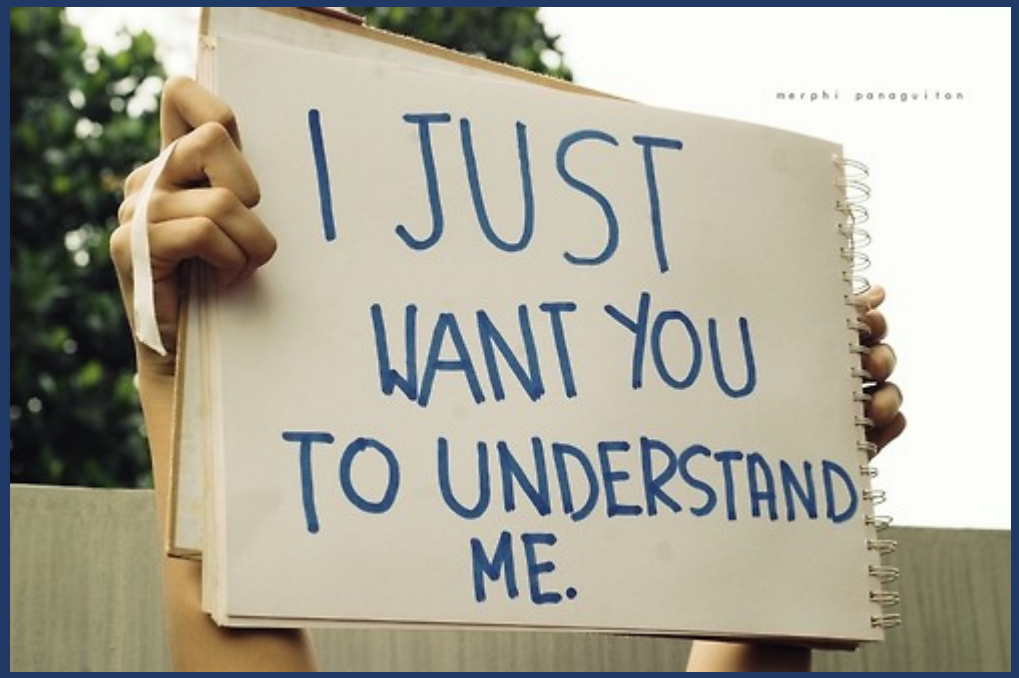
CISQ Consortium for IT Software Quality

Founded by: Software Engineering Institute Carnegie Mellon; OMG Object Management Group

IASME Consortium + CYBER ESSENTIALS

HITRUST CSF Certified

Easily Understood



SPARK's 16 Control Objectives

1. Risk Assessment and Treatment
2. Security Policy
3. Organizational Security
4. Asset Management
5. Human Resource Security
6. Physical and Environmental Security
7. Communications & Operations Management
8. Access Control
9. Information Systems Acquisition Development
10. Incident & Event Management
11. Business Resiliency
12. Compliance
13. Mobile
14. Encryption
15. Supplier Risk
16. Cloud Security

Record Keeper Hires Third Party Independent Auditor

Auditor Uses SPARK's 16 Control Objectives

Auditor Creates a SOC2 or AUP Report for Consultants and Plan Sponsors

Plan Consultant or Plan Sponsor Uses Report to Grade Record Keepers

How It Works

Next Steps

Communicate to Plan Sponsors, Consultants and Attorneys

Implement New Best Practice Disclosures for Cyber Security & Data Protection

Share with Retirement Community, Learn and Continually Improve the Process

Questions