IPDR2
5-22-98

The NIST Cybersecurity Framework (CSF) Unlocking CSF - An Educational Session

Robert Smith
Systemwide IT Policy Director
Compliance & Audit Educational Series

Today's reality

There are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese.
- FBI Director James Comey

"Hackers have already breached Internet-connected camera systems, smart TVs, and even baby monitors."

Molly Wood, The New York Times

There are two types of companies in the world: those that know they've been hacked, and those that don't.
- British Journalist Misha Glenny

In a 2014 FireEye / Mandiant report,

97% of the organizations analyzed had been breached.

"There's no perfect security, and security isn't an endpoint — it's a never-ending journey."

John Klemens, Technical Director of IA Solutions, Telos Corporation

Incident patterns by industry minimum 25 incidents (only confirmed data breaches)

Crimeware	Cyber-espionage	Denial of Service	Everything Else	Stolen Assets	Misc. Errors	Card Skimmers	Point of Sale	Privilege Misuse	Web Apps
			1%	<1%	1%	<1%	95%	1%	1%
	7%		17%	17%	27%			3%	30%

Figure 22.

Incident patterns by industry minimum 25 incidents (only confirmed data breaches)

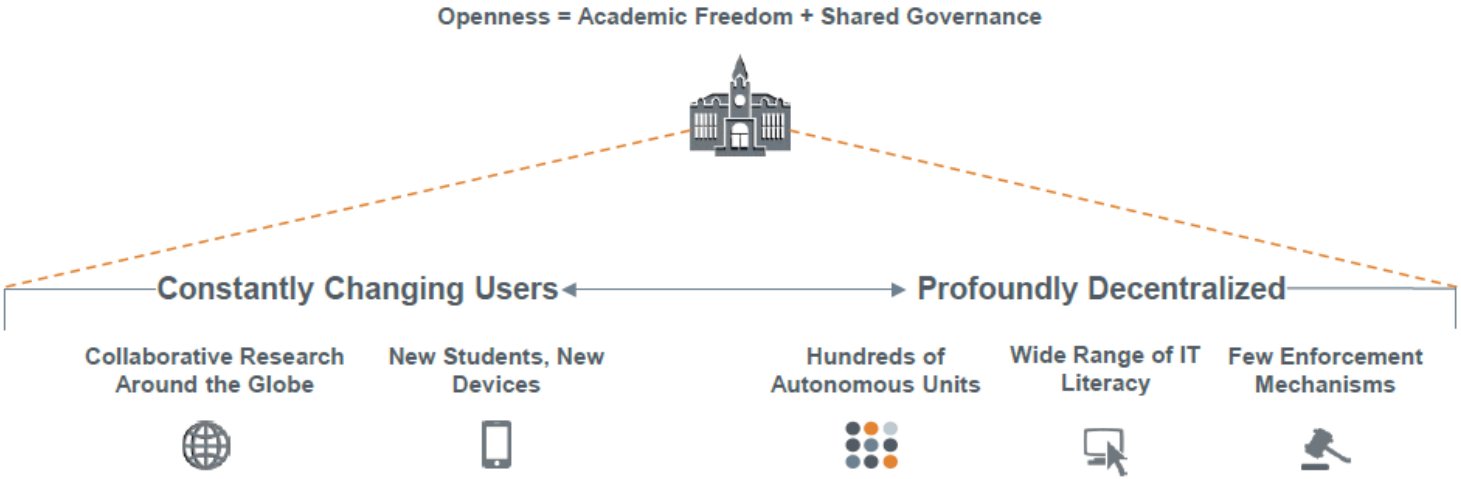
Accommodation (72), n=282

Educational (61), n=29

verizon

2016 Data Breach Investigations Report

How Do We Protect an Institution Designed for Openness?



Determined to Stay "Free"

"Higher Ed is by design focused on transparency, with as few restrictions as possible to information sharing. The bedrock mindset tilts toward academic freedom."

CIO, Regional Masters University

Uniquely Risky

"Higher education is one of the most heavily regulated industries in the U.S.- and it has more risk-producing constituencies than almost any other industry."

Leta Finch, Aon Risk Management Services

Source: EAB Interviews and Analysis

Threats are real, evolving, and sophisticated

- The “bad actors” are organized and coordinated
  - Nation-State
  - Criminal Syndicates
  - “Hacktivism” / politically driven

- They know how to get at what they want
  - Compromised devices (“hacked”)
  - Compromised passwords (“phished” or harvested)
  - Lost and stolen devices
  - Insider (accidental or nefarious)

Think Different

Old Thinking – "Keep Out"

- Security is IT's job
- Perimeter defense
- Plugging the holes
- "If only we had more…"
  - Money, Time, People
- More money = More defense = more security
- End state – "we are secure"

New Thinking – "Find and recover"

- Security is everyone's responsibility
- Asset inventory = new perimeter
  - Separate assets based on risk
- Resources allocated based on risk
- Assume you are breached
  - Threat detection and identification
  - Find intruders and kick them out
  - Limit the damage they can do
  - Recovery
  - These are different spending priorities
- End state – "managed risk"

Today's goal – unlock CSF

IPDR2

5-22-98

Takeaway

- **I**dentify – Know your assets
- **P**rotect – Limit the damage
- **D**etect – Find the bad actors
- **R**espond – Hunt the bad actors and expel
- **R**ecover – Get back to a normal state

The Five Functions of the NIST CSF

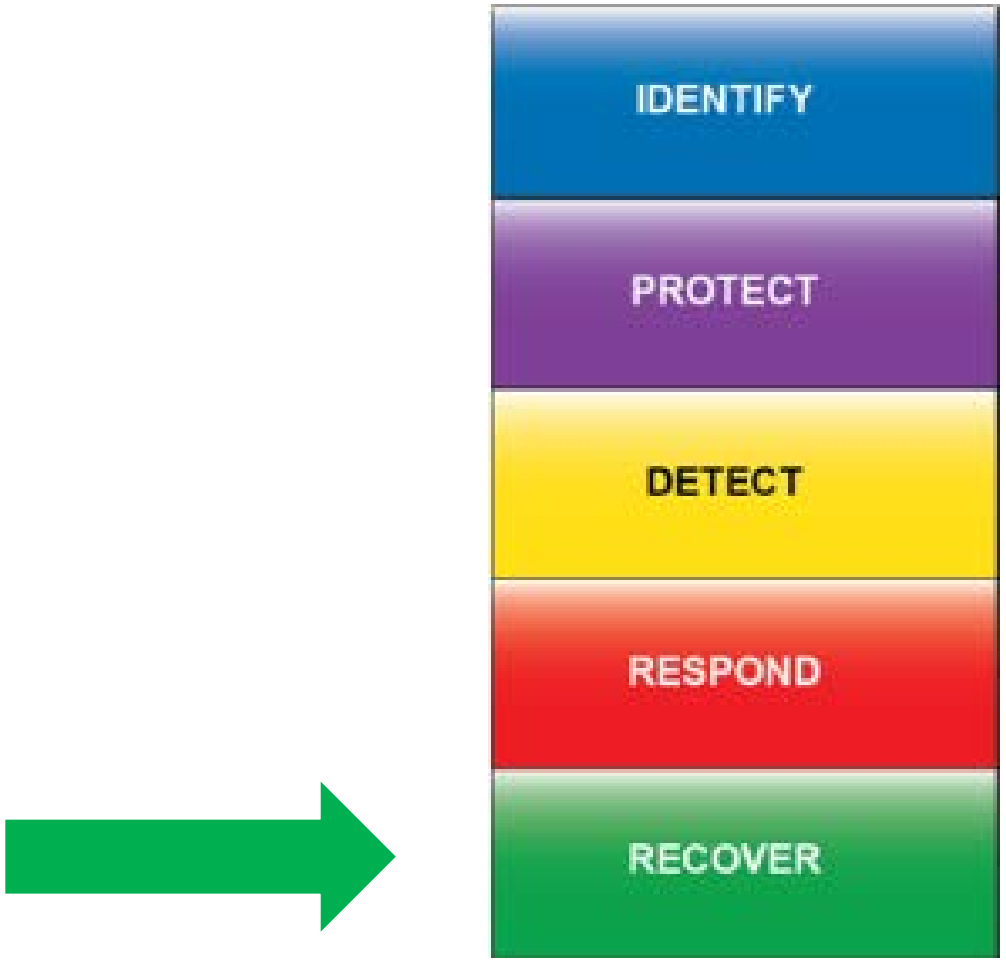
IPDR2

5-22-98

Case Study – Hollywood Presbyterian

- Ransomware
- Locked-up hospital for more than a week!
- $17K ransom paid!
  - But it could have been worse!
- Think different …

The most important control?



Introduction to the NIST CSF

NIST CSF

- NIST – National Institute of Standards and Technology
- CSF – Cybersecurity Framework – issued February 2014
- Why?
  - NIST 800-53 is 462 pages long
  - How can organizations apply a 462 page standard?
  - The CSF is guidance, based on standards, guidelines, and practices, for organizations to better manage and reduce cybersecurity risk
    - Avoid using a checklist and think about risk
  - Designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders, as well as managed and reduce risk

CSF Introduction

- Provide a common taxonomy and mechanism:
  1. Describe current cybersecurity posture
  2. Describe target state for cybersecurity
  3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
  4. Assess progress toward the target state
  5. Communicate among internal and external stakeholders about cybersecurity risk

CSF Overview

- Framework Implementation Tiers
  - Tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk
- Framework Core
  - Set of cybersecurity activities, desired outcomes, and applicable references that are common across sectors
- Framework Profile
  - Represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories
  - The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario.

IPDR2
5-22-98

Maturity model

IMPLEMENTATION TIERS

CSF Implementation Tiers - Maturity

- Tier 1 – Partial
  - Cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.
  - Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- Tier 2 – Risk Informed
  - Risk management practices are approved by management but may not be established as organizational-wide policy.
  - Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- Tier 3 – Repeatable
  - Risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
- Tier 4 – Adaptive
  - Adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.
  - Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner.

IPDR2

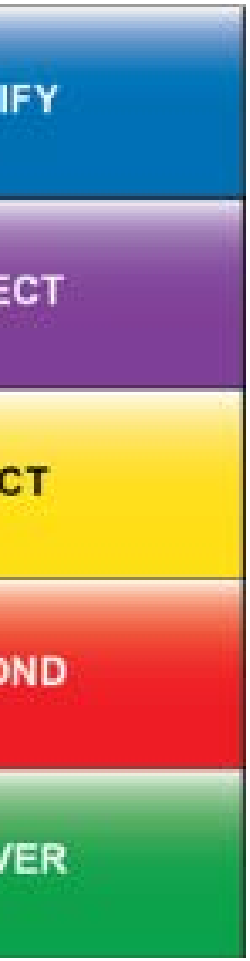
5-22-98

Talking about security controls relative to risk

FRAMEWORK CORE – IPDR2

CSF – 5 Functions

- **I**dentify
  - Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
- **P**rotect
  - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **D**etect
  - Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **R**espond
  - Develop and implement the appropriate activities to take action regarding a detected cyber security event.
- **R**ecover
  - Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event



IPDR2

5-22-98

It’s pretty easy

- A fairly straight forward way to ask and describe, here are the main activities in
  - Identify, Project, Detect, Respond and Recover.
  - 5 Buckets
- The next level, categories, is not bad at 22
  - 3 to 6 per function
  - See the next slide →

IPDR2

5-22-98

Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Functions, Categories, Subcategories

- **5** Functions
- **22** Categories
  - Cybersecurity outcomes closely tied to programmatic needs and particular activities
  - Examples:
    - Asset Management
    - Access Control
    - Detection Processes
- **98** Sub categories
  - Examples
    - External system cataloged
    - Mobile devices with ePHI identified

IPDR2

5-22-98

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	• **COBIT 5** APO01.02, DSS06.03 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1

IPDR2
5-22-98

Where are we and where are we going

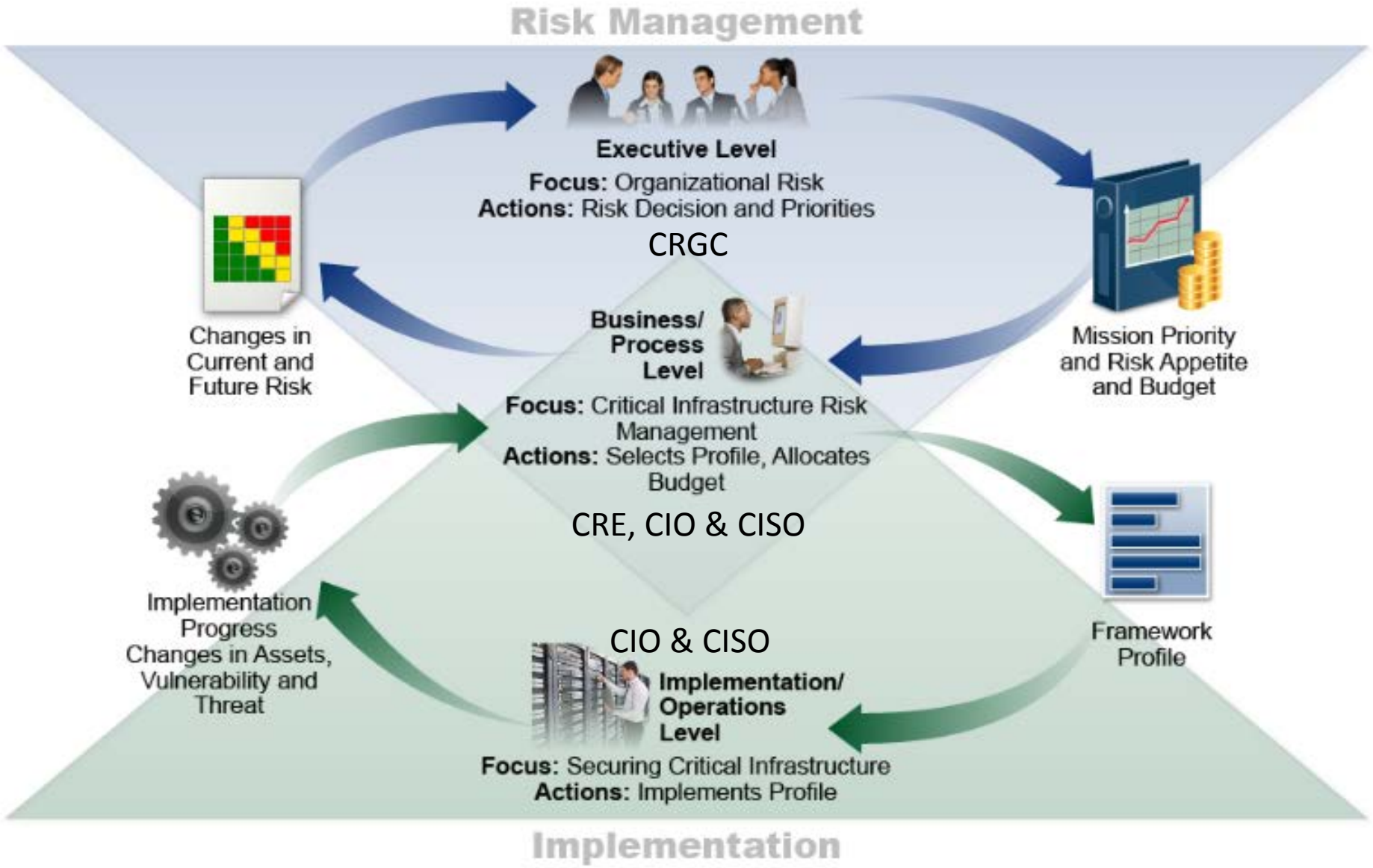
CREATING A PROFILE

Recommended 7 Step Process

- Step 1: Prioritize and Scope
  - Identify business/mission objectives and high-level organizational priorities
- Step 2: Orient
  - Identify related systems and assets, regulatory requirements, and overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets
- Step 3: Create a Current Profile
  - Which Category and Subcategory outcomes from the Framework Core are currently being achieved

Recommended 7 Step Process

- Step 4: Conduct a Risk Assessment
  - Analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization
- Step 5: Create a Target Profile
  - Framework Categories and Subcategories describing the desired cybersecurity outcome
- Step 6: Determine, Analyze, and Prioritize Gaps
  - Step 3 vs. Step 5
- Step 7: Implement Action Plan
  - Actions to take
  - Monitoring of the program


Risk Management
Executive Level
Focus: Organizational Risk
Actions: Risk Decision and Priorities
CRGC
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget
CRE, CIO & CISO
Implementation Progress Changes in Assets, Vulnerability and Threat
Framework Profile
CIO & CISO
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

Why is this important?

- UC is driving to adopt a common risk management framework
- NIST CSF provides the taxonomy and mechanisms to have the conversations across UC and with external consulting firms
  - Consistent
  - Auditable
- NIST 800-39 may drive the overall process flow
  - Managing electronic information security risk

Case Study
University of Central Florida

- Feb 4, 2016 - Student SSNs exposed in breach
  - 63,000 current and former students were accessed – class action lawsuit filed within days
  - Weakness in architecture cited
    - Local database

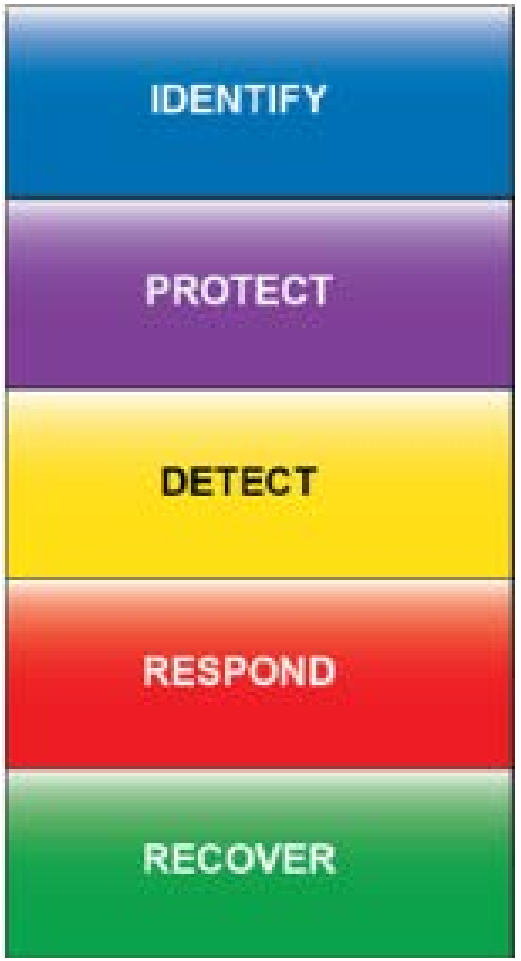
      The first group includes current student athletes, some former student athletes who last played for UCF in 2014-15 and some student staff members of UCF teams. Compromised personal information about these people includes first and last names, Social Security numbers, student ID numbers, sport, recruitment information and the number of credit hours taken and in progress.
- CSF
  - What do you think?

Case Study
University of Central Florida

ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes

Quick review

- CSF – Cybersecurity Framework
- Governance is key – investment decisions
- Taxonomy and mechanism to talk about cyber-risk
- 5 Functions
  - They are…?
- 22 Categories across the 5 Functions
- A 4-Tier Maturity Model
- A target profile process that maps where we are and where we **want** to be based on risk and governance
  - Continuous improvement and adjustment



IPDR2
5-22-98

Robert Smith
robert.smith@ucop.edu