Enterprise Security

Oversight using NIST CSF

November 2nd, 2017

About the speaker : VJ Rao

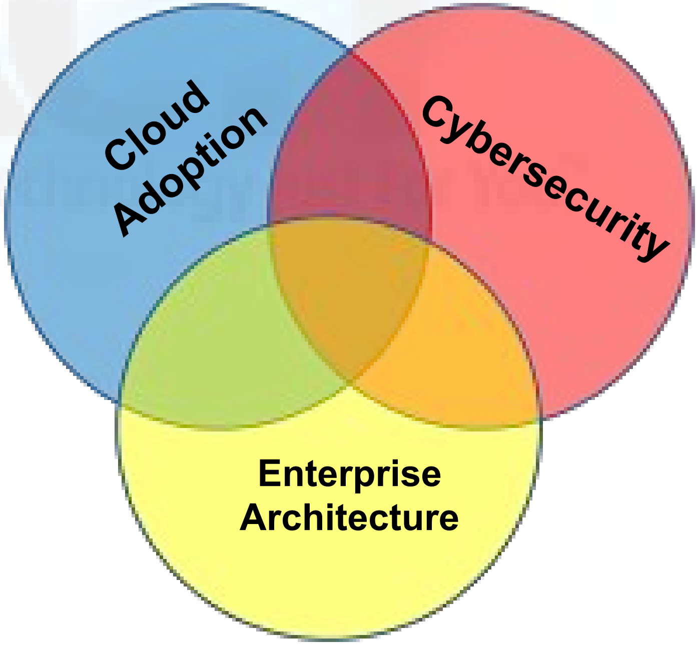
https://www.linkedin.com/in/vj-rao-51472a102

- CxO Advisor at Xykon
  - CISO for the Commission on Presidential Debates
  - Focus on Qualitative Risk and APT
  - Featured in numerous articles on cloud computing and cybersecurity

About the speaker : VJ Rao

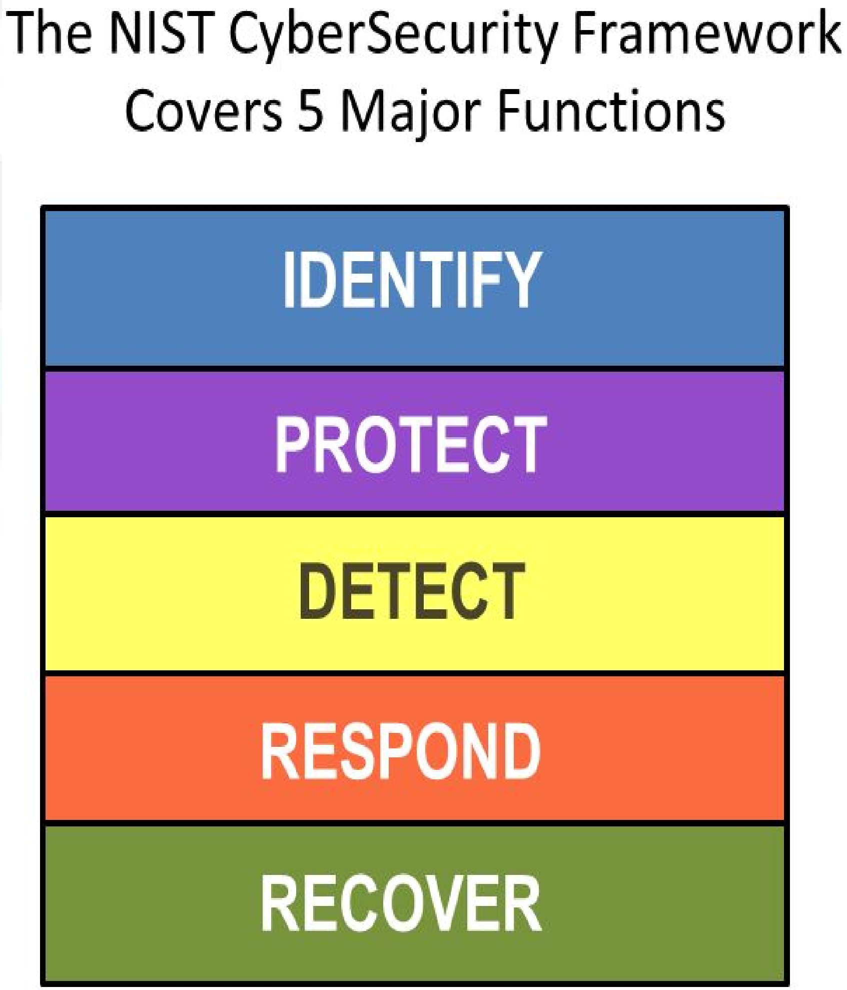
https://www.linkedin.com/in/vj-rao-51472a102

- CxO Advisor at Xykon
  - Numerous audits and assessments in Non-Profit, Financial, and Government Sectors.
  - Area of expertise: Intersection of Cybersecurity, Enterprise Architecture and Cloud Adoption



Focus

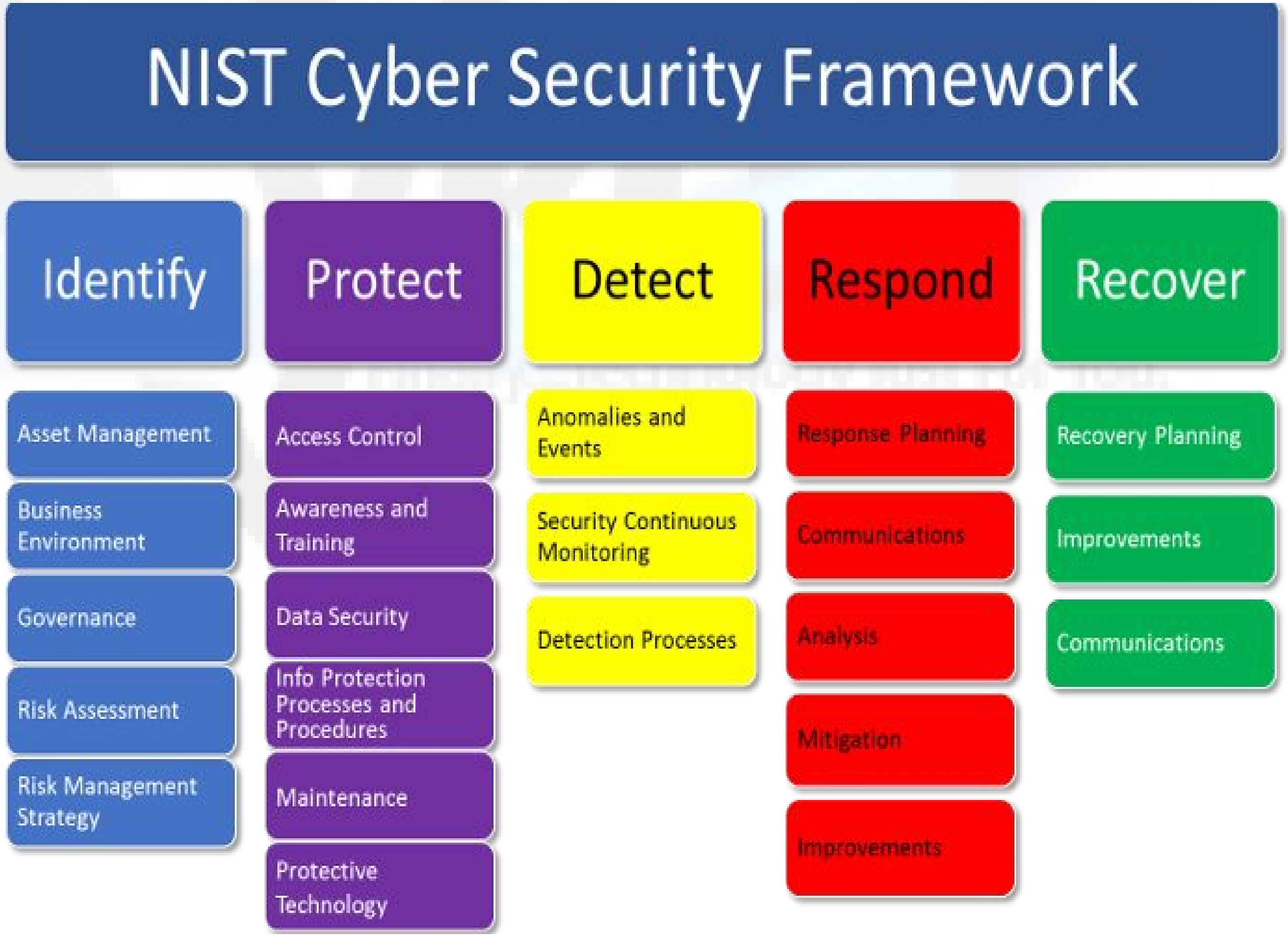
NIST CSF – an easy to adopt model for corporate oversight of IT security



The NIST CyberSecurity Framework Covers 5 Major Functions

Focus

- Broken down into 22 categories
- Further broken down into 98 subcategories
- It is a tool to get started



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Focus-Continued

Last year's talk – How NIST CSF can be mapped to IT controls such as CSC top 20, ISO 27001, NIST 800-53, etc.

This year's talk – How boards and executive leadership understand and participate in the process

© D.Fletcher for CloudTweaks.com

Focus-Continued

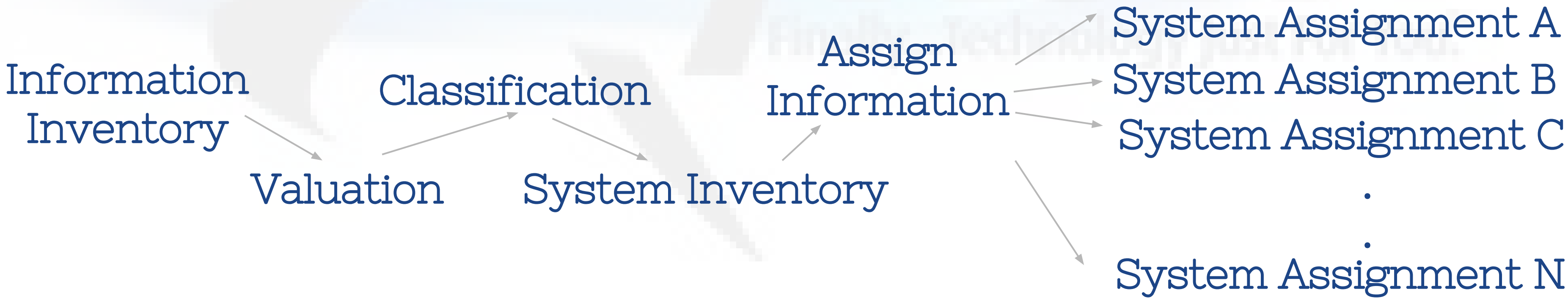
NIST CSF can be used for

- Organizational maturity (macro) and application or service level (micro) *oversight*

NIST CSF adoption is now a FEDERAL MANDATE based on an EO by President Trump on May 11, 2017

NIST CSF

- A traditional risk assessment requires the following information prior to commencement



Information Inventory

Valuation

Classification

System Inventory

Assign Information

System Assignment A

System Assignment B

System Assignment C

.

.

System Assignment N

- In contrast, an application centric assessment groups applications into groups.

NIST CSF

- Helps think of risk in terms of applications and services
  - These can be more easily linked to enterprise goals

NIST CSF

- Better protection against APTs and Ransomware
  - Easier to understand and counter reputational threats

NIST CSF

- An application based assessment is easier for business leaders to understand. They are typically grouped based on:
  - Categories – Dictates architectural investments needed for resiliency and security
  - Priorities – Dictates recovery order in a disaster scenario
  - Risk Type – Dictates types of risk that broadly apply to an application or system

NIST CSF

- Overarching goal of improving AIC does not change. However…
    - It allows for a formal risk management program to proceed in parallel with an inventory exercise
    - It is more likely to engage information with low risk systems than constantly gauge risk based on information contained

NIST CSF

- Target state
  - Partial
  - Informed
  - Repeatable
  - Adaptive

- Assess current state
- Create gap analysis and progress plan for desired maturity level
  - As we saw last year, controls to help improve maturity level map directly to Top 20 CSC, NIST and ISO

NIST CSF

- Partial
  - Risk Management Process – Not formalized
  - Integrated Risk Management Program – Nonexistent/Ad-hoc
  - External Participation – Nonexistent

NIST CSF

- Informed
  - Risk Management Process – Not formalized, but in tune with business
  - Integrated Risk Management Program – Informal, but management and users are more aware than at the ‘Partial’ level
  - External Participation – Stakeholders may generally be aware but have no clarity on how to interact or communicate with partners

NIST CSF

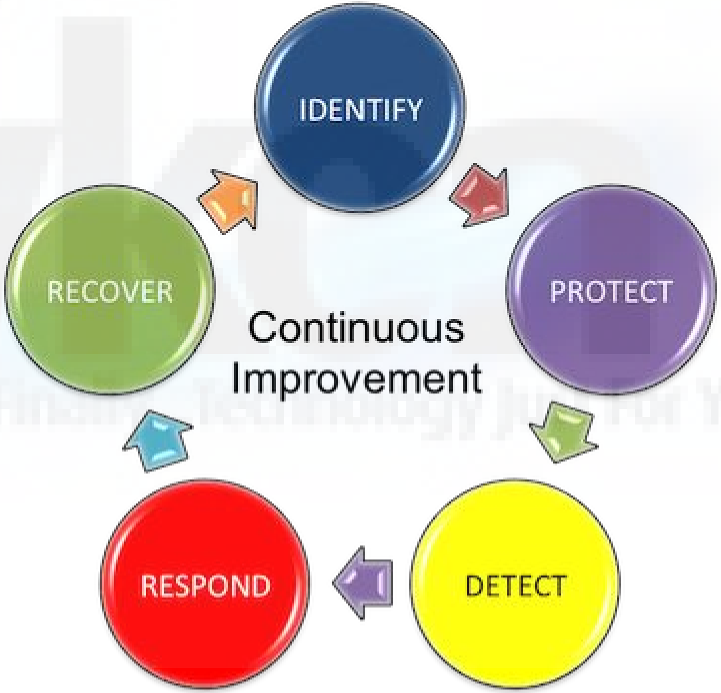
- Repeatable
  - Risk Management Process – Formal approval process exists where business leaders review and make decisions, as opposed to IT
  - Integrated Risk Management Program – Formal program exists and everyone is aware of their RACI roles (Responsible, Accountable, Consulted, Informed)
  - External Participation – Send and receive information to and from trusted partners

NIST CSF

- Adaptive
  - Risk Management Process – Equipped to handle advanced persistent threats through continuous improvements
  - Integrated Risk Management Program – Thinking about risk and cybersecurity is in every employee's DNA
  - External Participation – Proactive threat and information sharing to ensure community as a whole is better protected against advanced persistent threats

NIST CSF

- IDENTIFY
- PROTECT
- DETECT
- RESPOND
- RECOVER

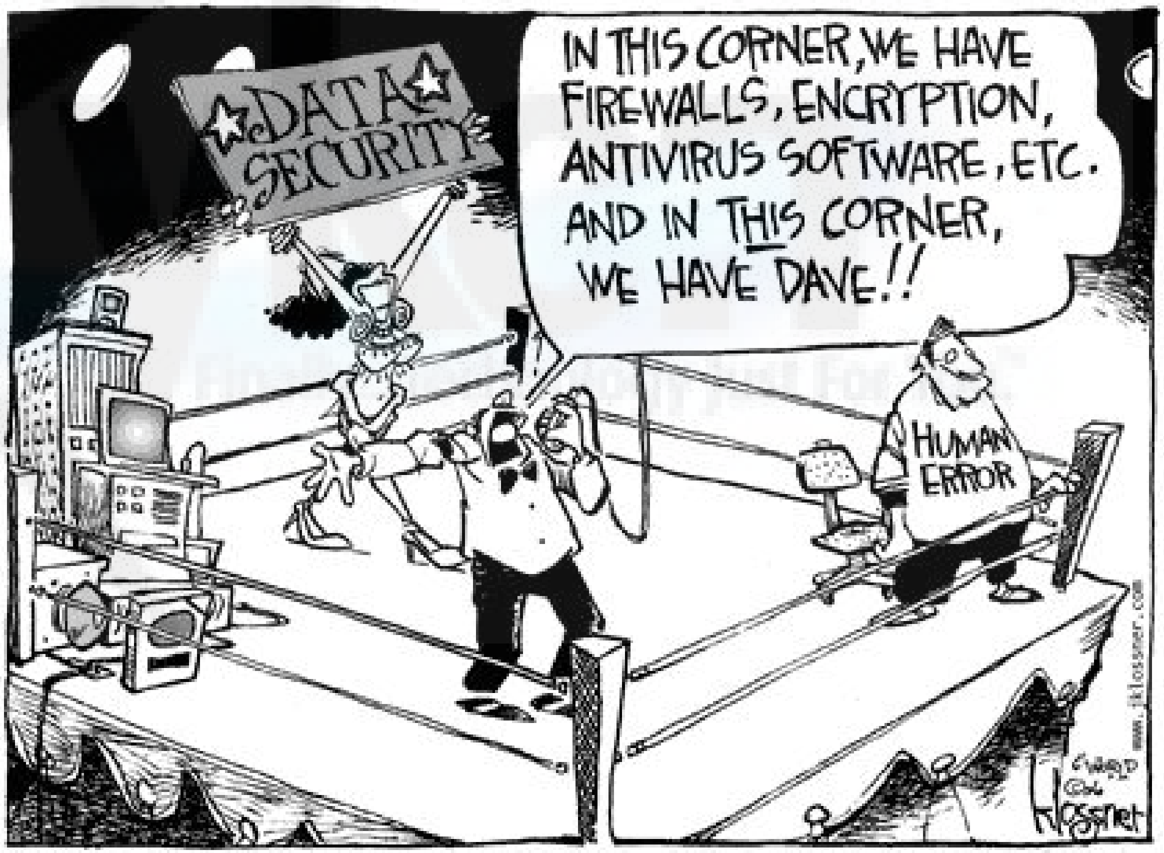


IDENTIFY

- ASSET MANAGEMENT
- BUSINESS ENVIRONMENT
- GOVERNANCE
- RISK ASSESSMENT
- RISK MANAGEMENT STRATEGY

PROTECT

- ACCESS CONTROL
- AWARENESS AND TRAINING
- DATA SECURITY
- INFORMATION SECURITY PROCESSES AND PROCEDURES
- MAINTENANCE
- PROTECTIVE TECHNOLOGY


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner

DETECT

- ANOMALIES AND EVENTS
- SECURITY CONTINUOUS MONITORING
- DETECTION PROCESSES

RESPOND

- RESPONSE PLANNING
- COMMUNICATIONS
- ANALYSIS
- MITIGATION
- IMPROVEMENTS

Disaster risk mitigation:
"alright, enough about me and my anti-human trafficking missions in Moldova: tell me something about yourself...
.... my husband just got here...
"i guess his full-contact tournament finished early"
MANU

RECOVER

- RECOVERY PLANNING
- IMPROVEMENTS
- COMMUNICATIONS

Example Subcategories: AWARENESS AND TRAINING (PROTECT)

- ALL USERS ARE TRAINED (PR.AT-1)
- PRIVILEGED USERS UNDERSTAND R&R (PR.AT-2)
- THIRD PARTY STAKEHOLDERS UNDERSTAND R&R (PR.AT-3)
- EXECUTIVE LEADERSHIP UNDERSTAND R&R (PR.AT-4)
- SECURITY PERSONNEL UNDERSTAND R&R (PR-AT-5)

Qualitative vs. Quantitative

- Quantitative
  - Dollar value
- Qualitative
  - Relative Rank

Qualitative

- Threat (1-4)*Vulnerability(1-4)*Impact(1-4)*Context(1-4)
  - Impact is set by business
  - Context is set by IT/Security

Risk Profiles

- High Risk- 128-256
- Medium Risk - 32-128
- Low Risk - < 32

Example - Public Website

- Threat 4 (APT 4, Poor High Availability 3. Choose highest)
- Vulnerability 4 (SQL Injection 4, Memory Leak 4, OS patch 2. Choose highest)

Example - Public Website

- Context 4 (APT 29/Fancy Bear currently targeting SQL Injection vulnerabilities on Drupal websites)
- Impact 3 (Public Facing->Reputational Impact)

Example - Public Website

- Score = 4*4*4*3
- 192
- HIGH RISK

Example - Internal Database

- Threat 4 (APT 4, Poor High Availability 3. Choose highest)
- Vulnerability 4 (SQL Injection 4, Memory Leak 4, OS patch 2. Choose highest)

Example - Internal Database

- Context 1 (System Offline – Physically Controlled Access)
- Impact 4 (Reputational 3 and Legal 4. Choose Highest)

Example - Internal Database

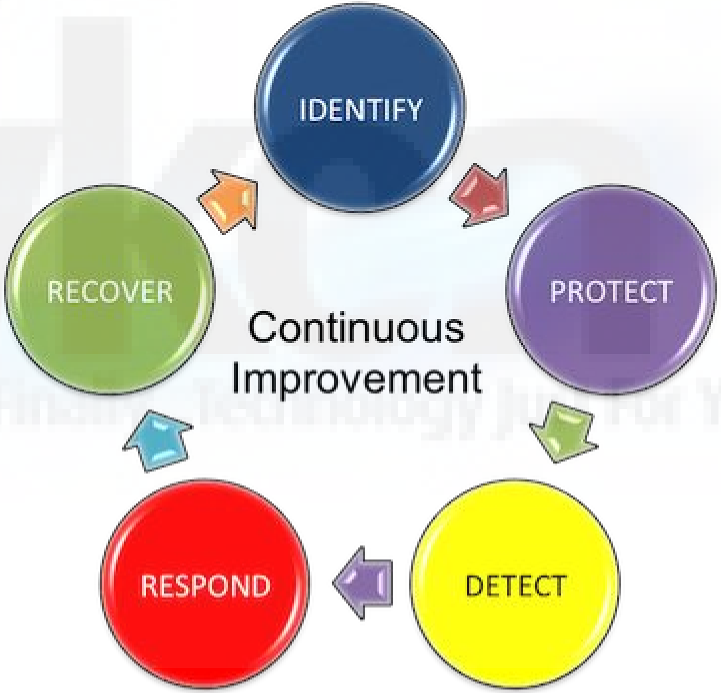
- Score = 4*4*4*1
- 64
- MEDIUM RISK

NIST CSF Risk Profiles

- Partial - 128-256
- Informed - 64-128
- Repeatable - 32-64
- Adaptive - < 32

EXAMPLE RISK PROFILE

- IDENTIFY – Partial
- PROTECT – Informed
- DETECT – Informed
- RESPOND – Informed
- RECOVER – Partial



RECOVER - Recovery Planning Deep Dive

- RECOVERY PLANNING
  - Recovery Planning is updated during an event (RC.RP.1)

Recovery Planning Score- Public Website - 192 (Informed)

- Impact 3
  - Priority 3 (4, 3, 2 and 1)
    - If the assessment is for Protect (Resiliency PR.PT-4), use ‘Categories’ instead of ‘Priorities’.
- Context 4
  - No DR site
    - If the assessment is for Protect (Resiliency PR.PT-4), use an architectural assessment.

Recovery Planning Score - Public Website - 192 (Informed)

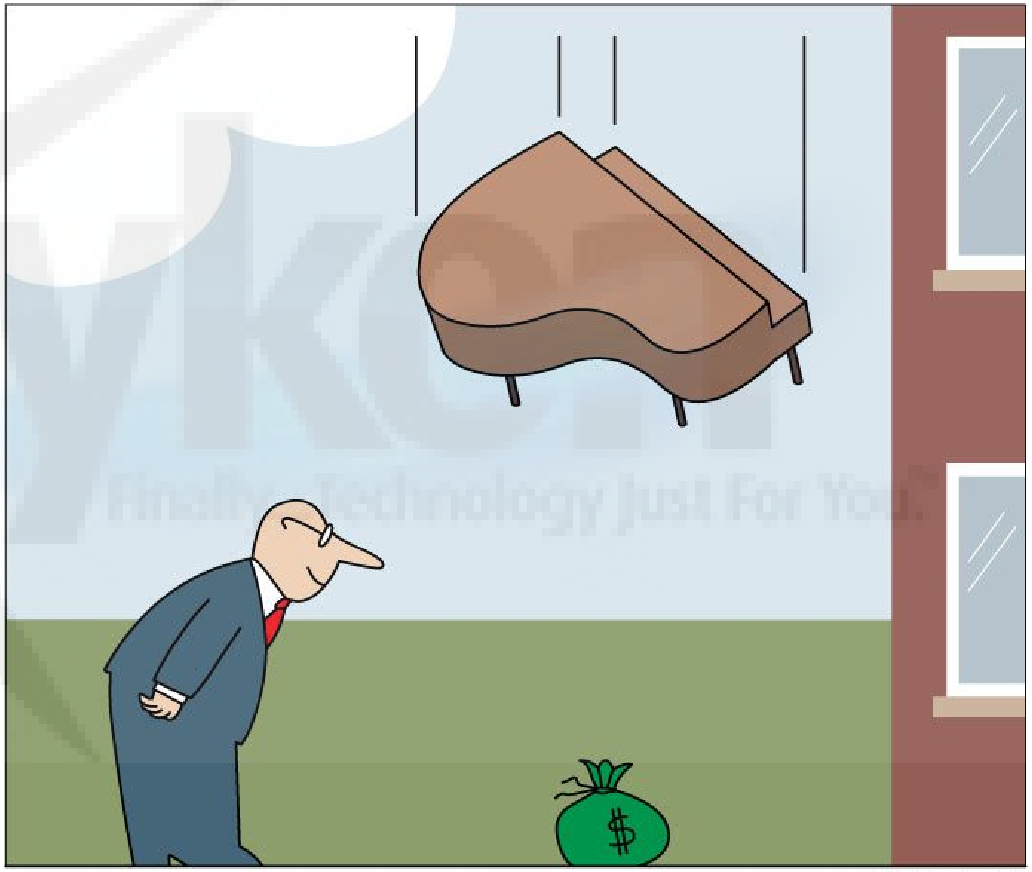
- Vulnerability 4
    - Documentation, Current State and Exercise Review – 4 (Choose Highest)
- Threat 4
    - Internal Threats, APT – 4 (Choose Highest)

Example Scores: RECOVER (Partial - If choosing the highest score)

- RECOVERY PLANNING 192 (Partial)
- IMPROVEMENTS 64 (Informed)
- COMMUNICATIONS   128 (Informed)

Conclusion

The primary advantage to organizations using NIST CSF is the ability to understand the current state from a *risk perspective*



Tracking performance without risk is... shortsighted

Conclusion

Think about IT security from a strategic (enterprise goals, maturity) and operational (ATO) perspective using a single framework.

It leads to better clarity of thought when it comes to overseeing risk.

"For security purposes, the information should make no sense at all to spies and hackers. We'll bring in someone later to figure out what you meant."

Softball Questions Allowed

Questions?