LEVERAGING PROJECT MANAGEMENT TO MITIGATE DATA BREACH

Presented by

Francisco T. Avalos, MBA, PMP, CSM

Teissier Consulting Services, LLC

For

PMI – Orange County Chapter – Professional Development Day

Use Case

A newly hired PM contractor, walks into a Health Care IT company and while working on one of the assigned projects, the PM learned patient information being transmitted to a third party vendor through an unsecure FTP port.

- The PM diligently notes the risk because the PM recently completed a HIPAA training course.

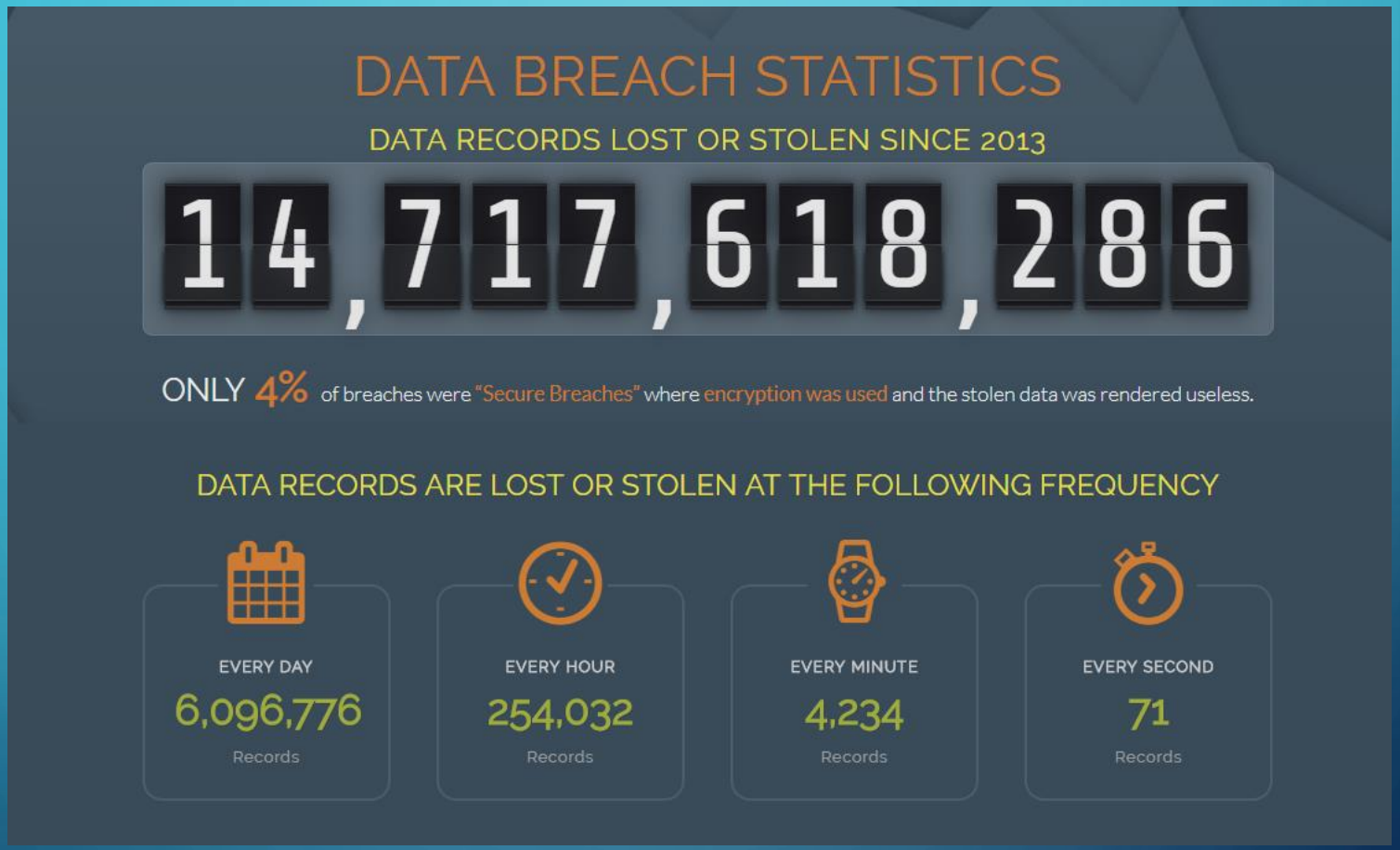
- The PM notifies compliance and stakeholders at the next meeting to highlight and discussed.

- What do you think happened next?

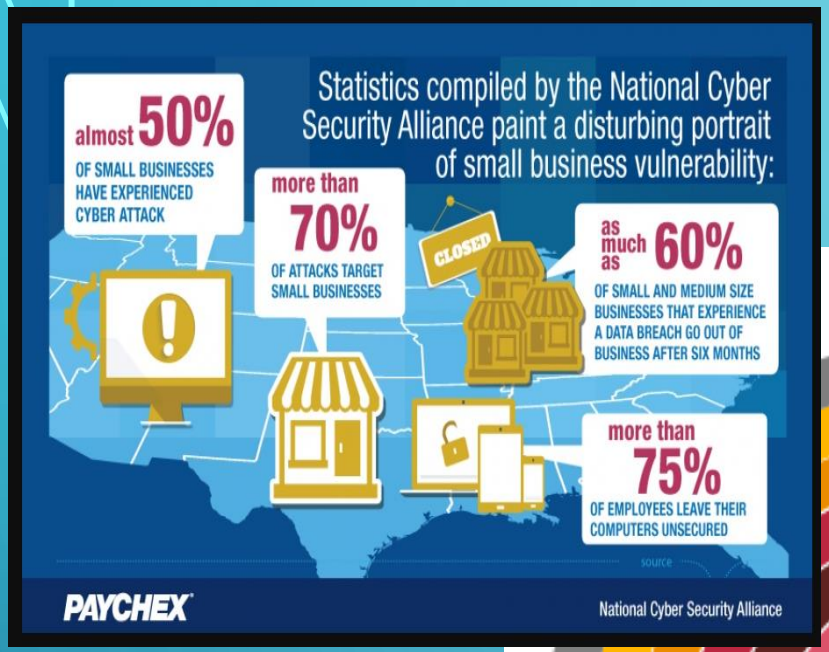
A Complex Market in Continuous Evolution…

	Major Hacks	Estimated Affected People
Financial	EQUIFAX	148 Million
Retail	Target	110 Million
Health Care	Anthem	79 Million
Financial	JP Morgan/BofA TD Banks	83 Million
	Total People Affected	420 Million
	US Population	*329 Million*
CHANCES ARE, YOU BEEN AFFECTED!!!!		
BreachLevelIndex.com* Data as of 10/2018		

Data as of August 8, 2019



Small Business Vulnerability



How can AI be Dangerous?

From SIRI to self-driving cars, artificial intelligence (AI) is progressing rapidly. It's Here!

"A computer algorithm failure in Britain's automated health services discovered in May prevented women from receiving a digital reminder to schedule their mammograms. As a result, 450,000 patients in England missed vital breast-cancer screenings and up to 270 patients might have died because of the oversight, according to an analysis. And project teams missed an opportunity to build a backup notification process into the system."

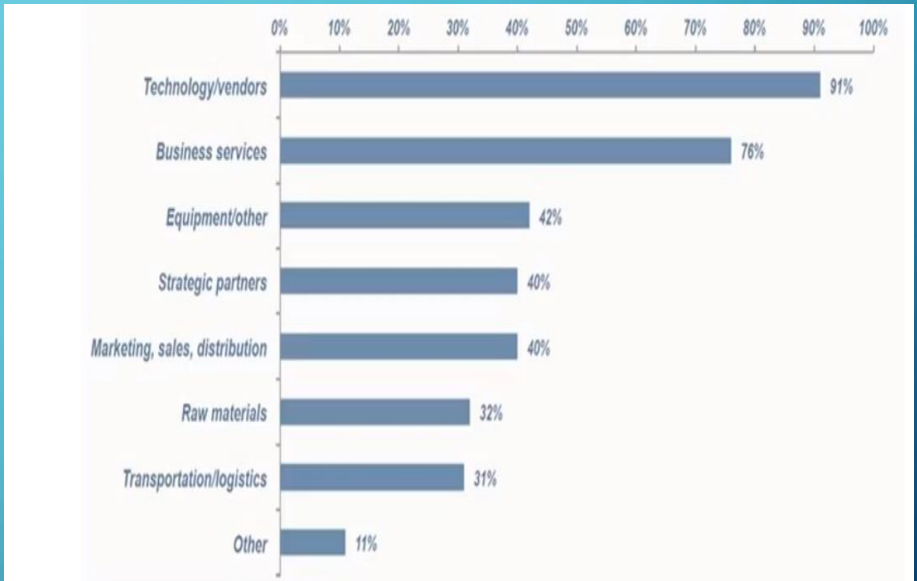
88% of men and 12% women contributed work to three leading machine learning conferences in 2017(2).

What about Third Party Vendors Risk Management

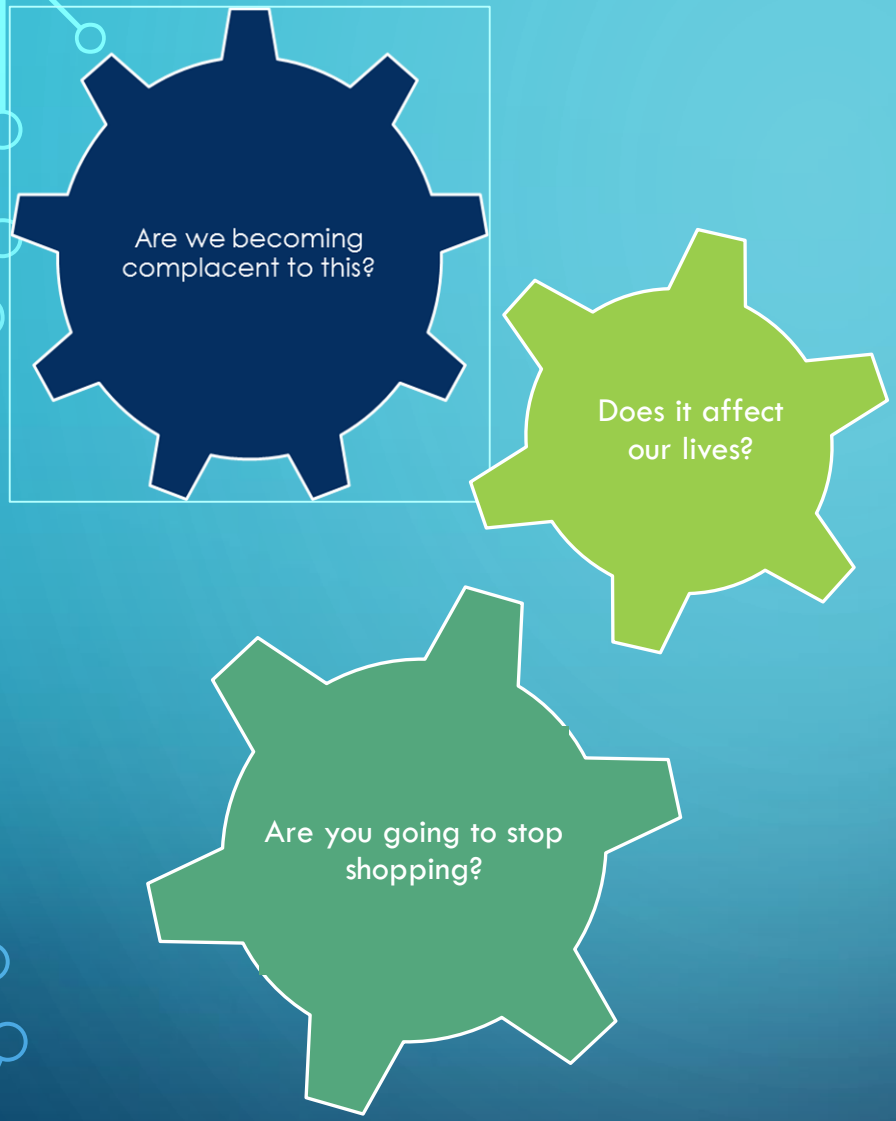
- Technology Services
- Financial Services
  - Accounting
  - Invoicing and Collection Agencies
- Healthcare Services
- Engineering Design
- Manufacturing

Survey Question

- Which type of third parties are significant in your business model?
  - Equipment Vendors
  - Business Services
  - Strategic Partners
  - Technology Vendors



Source: IIARF Research Report: Closing the Gaps in Third Party Risk Management



- Technology is used everywhere
- Technology is vulnerable
- Attackers use vulnerability that become threats

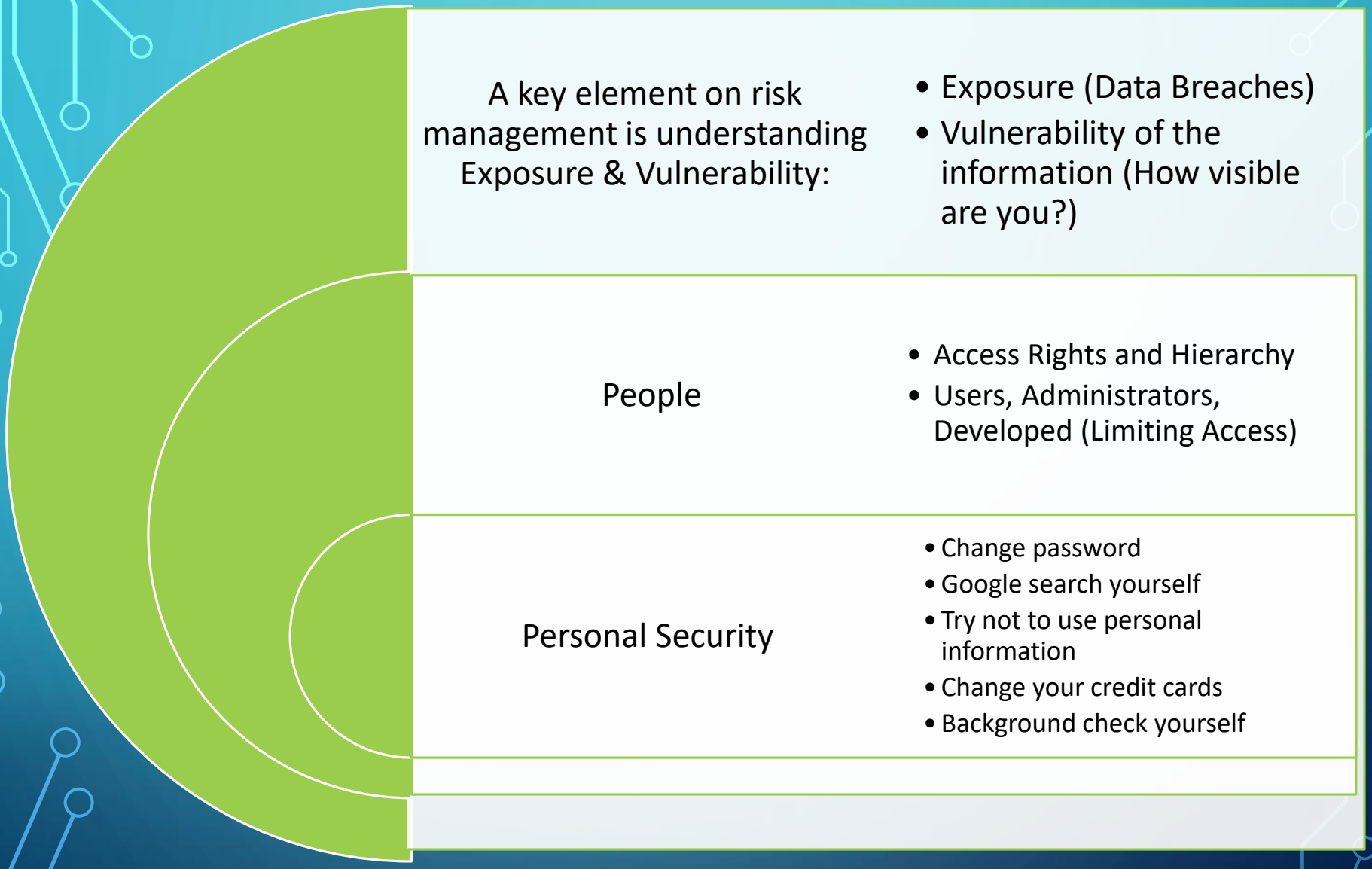
- Autonomous Automobiles
- Medical records
- Medical devices
- Electronics at Home

- Tactical & Cyber War:
  - Electrical Power Plants
  - Utilities
  - Products that use software
  - Financial Institutions
  - Infrastructure

Survey Question

- Majority of IT and security professionals believe that the risk of a breach from a third party is serious and is increasing…
  - Agree
  - Disagree
  - Unsure

Soha System's: "63% of all data breaches linked directly or indirectly to third party access, those contractors and suppliers who need to get access to corporate applications in order to get their job done represent risk to any organization." (2)


A key element on risk management is understanding Exposure & Vulnerability:
• Exposure (Data Breaches)
• Vulnerability of the information (How visible are you?)
People
• Access Rights and Hierarchy
• Users, Administrators, Developed (Limiting Access)
Personal Security
• Change password
• Google search yourself
• Try not to use personal information
• Change your credit cards
• Background check yourself

What is the common element?

Each of the technologies built started out as a

Project!

…And who is the main person responsible for the Project?

Project Manager

Survey Question

- Should Project Managers be concerned about Cyber Security on their assignments?
  - Yes
  - No
  - Not Sure?

Project Manager vs. Cyber Security Manager

Project Manager (PM)	Cyber Security Manager (CSM)
Project Managers identify success in the form of project success and stakeholder satisfaction	CMS identify success by identifying all the vulnerabilities and threats
PM ensure the scope of the plan is well understood	CMS determines the scope of the plan based on infrastructure needs
PM gather requirements to develop the application	CMS gather requirements to detect and prevent vulnerabilities
PM monitor projects using the triple constraints	CMS integrate tools to monitor the pulse of the infrastructure
PM are normally professional and organized to complete the project	CMS have identical traits and a “knack” to get information that is not privy to get the job done.

What about PMBOK® ?

Process Groups / PM Knowledge Area	Initiating	Planning	Executing	Monitoring and Controlling	Closing
4. Integration Mgmt	4.1 Develop Project Charter	4.2 Develop Project Management Plan	4.3 Direct & Manage Project Work	4.4 Monitor & Control Project Work	4.5 Close Project
5. Scope Mgmt		5.1 Plan Scope Management 5.2 Collect Requirements 5.3 Define Scope 5.4 Create WBS		5.5 Validate Scope 5.5 Control Scope	
6. Time Mgmt		6.1 Plan Schedule Management 6.2 Define Activities 6.3 Sequence Activities 6.4 Estimate Activity Resources 6.5 Estimate Activity Durations 6.6 Develop Schedule		6.7 Control Schedule	
7. Cost Mgmt		7.1 Plan Cost Management 7.2 Estimate Costs 7.3 Determine Budget		7.4 Control Costs	
8. Quality Mgmt		8.1 Plan Quality Management	8.2 Perform Quality Assurance	8.3 Control Quality	
9. Human Resource Mgmt		9.1 Plan Human Resource Management	9.2 Acquire Project Team 9.3 Develop Project Team 9.4 Manage Project Team		
10. Communications Mgmt		10.1 Plan Communications Management	10.2 Manage Communications	10.3 Control Communications	
11. Risk Mgmt		11.1 Plan Risk Management 11.2 Identify Risks 11.3 Perform Qualitative Risk Analysis 11.4 Perform Quantitative Risk		11.6 Control Risks	
12. Procurement Mgmt		12.1 Plan Procurement Management	12.2 Conduct Prourements	12.3 Control Procurements	12.4 Close Procurements
13. Stakeholder Mgmt	13.1 Identify Stakeholders	13.2 Plan Stakeholder Maangement	13.3 Manage Stakeholder Engagement	13.4 Control Stakeholder Engagement	
14. Security Mgmt	14.1 Analysis and Impact Assessment	14.2. Plan Security Management	14.3 Perform Security Assurance	14.4 Monitor and Control Security Vulnerabilities	

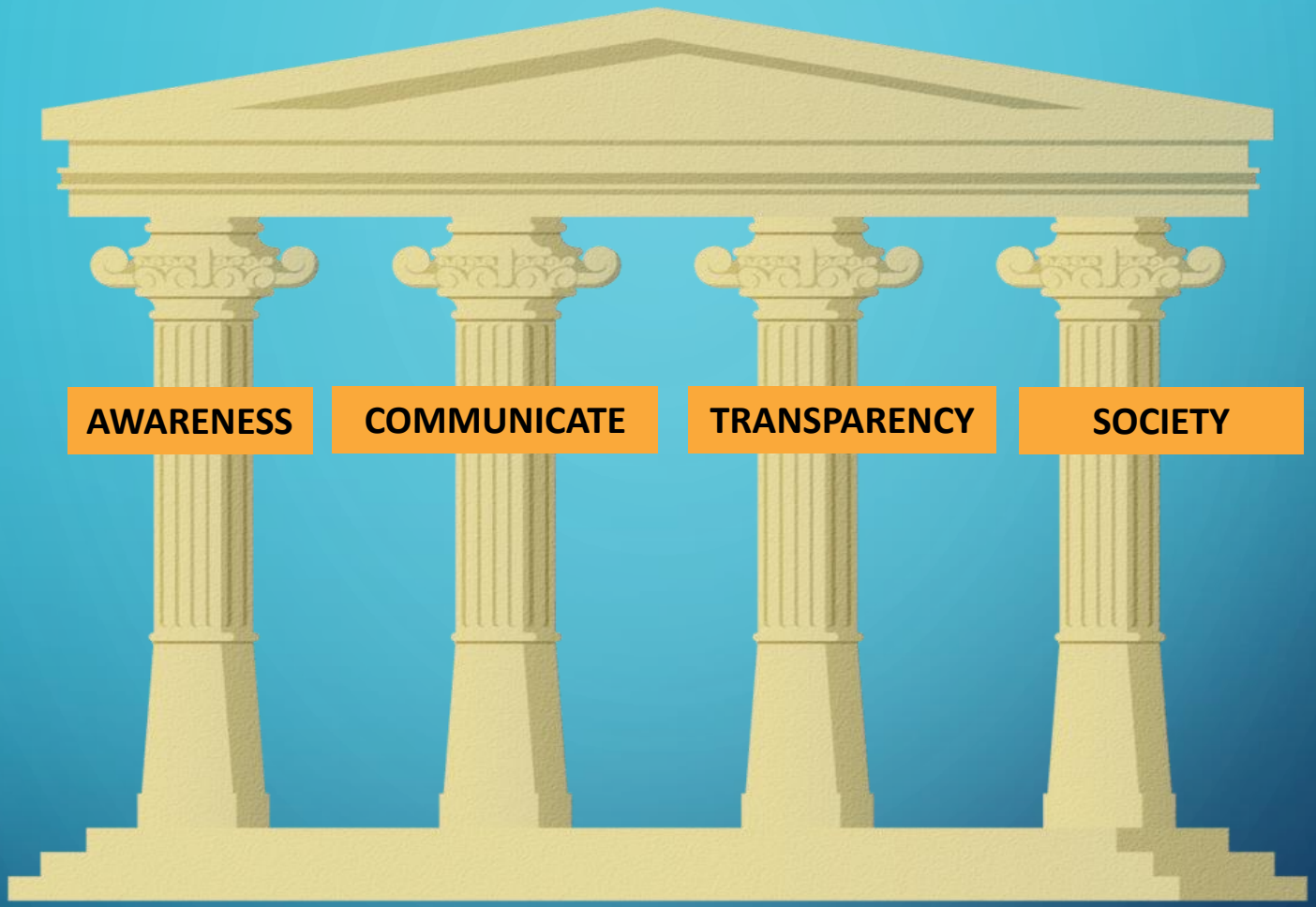
A proposed revision to the *PMBOK® Guide's* list of Knowledge Areas and Process Groups. By Nilanjan Kar, PMP

Project Manager – What Not To Do

- Lack of experience as a project manager – If something doesn't feel right, ask and document
- Don't talk too much – Listen more
- Too much focus on the triple constraints - Often overshadows security risks
- Poor communications, motivators are not self assured

Guard Your Projects

- Load up your risk register log
- Do not upset your IT staff!
- Understand the Information Data Risks For your Project
  - Transmission, Confidentiality, Physical Security, Device Security
- Produce Evidence: Rely on Sarbanes-Oxley Compliance, HIPAA, etc. for guidance
- Get compliance/Data Security involved! How? Project Charter & Project Plan
- Audit Frequently or Walk-through Processes.
- Understand your risk for each of your implementations
- Third Party Vendors: What is the contract like? Incident Reporting



Tune your Radar to People and Situations

Whole Body Decision

THANK YOU

QUESTIONS

?

Teissier Consulting Services, LLC
Francisco T. Avalos

- References:

- Project Management.com. Information Systems 2015: PMP and Security – A necessary Union?
  - By Lisa Woffinden, and Marina Syprou.
- BreachlevelIndex.com
- Paychex.com/National Cyber Security Alliance.
- Element AI
- The Institute of Internal Auditors (North America)
- (1) Soha system's Third Party Advisory Group online survey conducted in April 2016
- (2) Source: AI