Building a Cybersecurity Strategy in a Hospital

Session #154, February 13, 2019

Susan D. Villaquiral, CISO, Fundación Valle del Lili

FUNDACIÓN VALLE DEL LILI

Excelencia en Salud al servicio de la comunidad

Conflict of Interest

Susan D. Villaquiral,

Has no real or apparent conflicts of interest to report.

Agenda

- Who is Fundación Valle del Lili
- Definition of Cybersecurity
- Building a Cybersecurity Strategy
- Choosing HITRUST CSF
- HITRUST CSF and NIST CSF
- Organization Profile
- People, Process and Technology
- Tactics as part of the strategy
- Conclusions
- Questions

Learning Objectives

- Identify the main components during the implementation of a Cybersecurity strategy in a hospital
- Design a working plan for the implementation of a Cybersecurity strategy in a hospital
- Discuss the differences between the NIST Cybersecurity Framework and the HITRUST CSF
- Share the experience of a hospital in the process of implement a Cybersecurity strategy
- Classify the processes, people and technology that apply for each category of the Cybersecurity Framework

Fundación Valle del Lili

602 Doctors, Physicians and scientists

100 Specialties

5.329 Staff

514 Beds

12 Surgeon rooms

10 Endoscopy rooms

236 Consultories

3 Vascular intervention rooms

103.000 Mts^2

637 Students

#HIMSS19

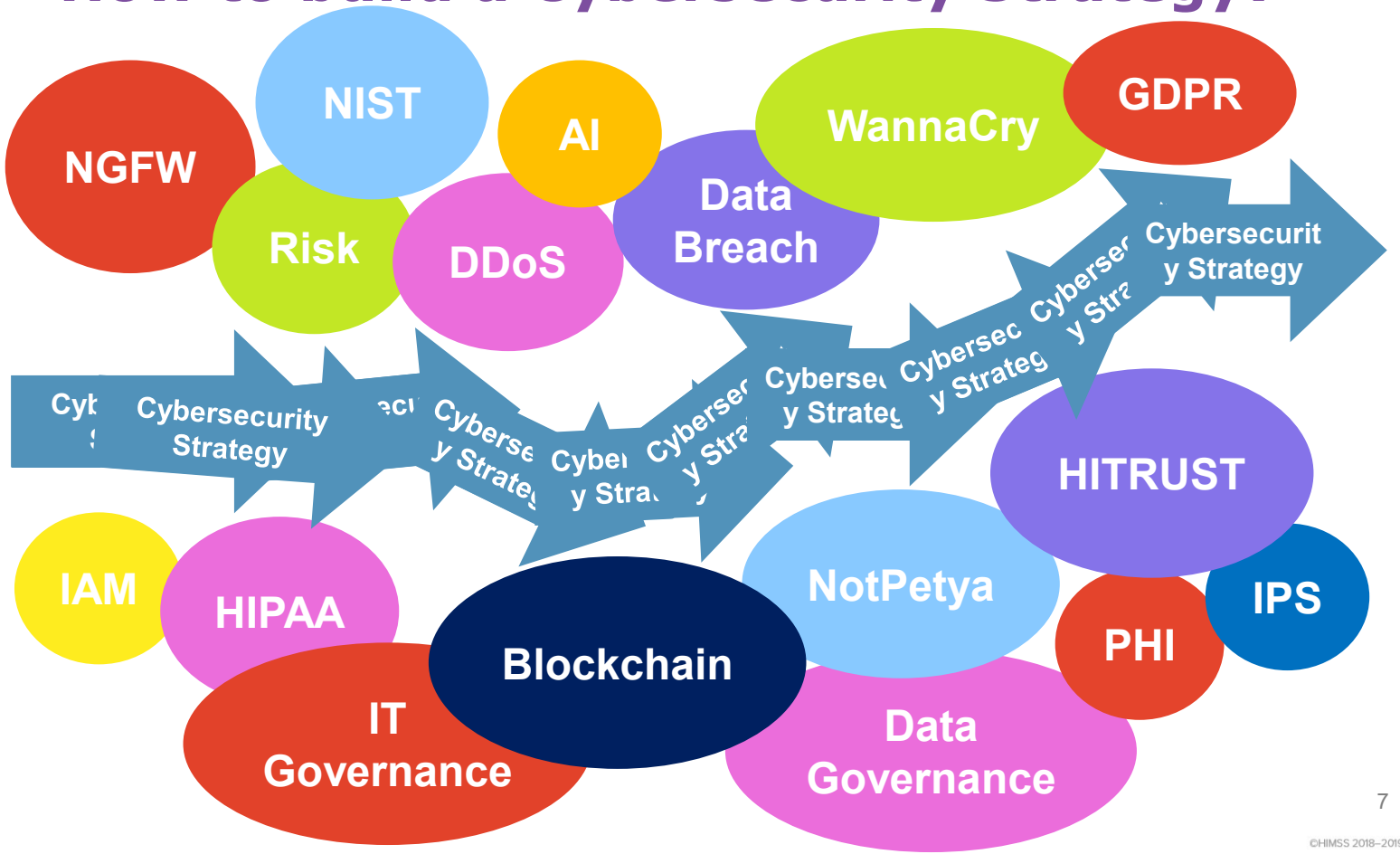
What is Cybersecurity?

- Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks.

- Elements of cybersecurity:
  - Application security
  - Information security
  - Network security
  - Disaster recover / business continuity planning
  - Operational security
  - End-user education

https://searchsecurity.techtarget.com/definition/cybersecurity?src=5822709&asrc=EM_ERU_103766138&utm_content=eru-rd2-rcpB&utm_medium=EM&utm_source=ERU&utm_campaign=20181120_ERU%20Transmission%20for%2011/20/2018%20(UserUniverse:%20455413)

How to build a Cybersecurity Strategy?

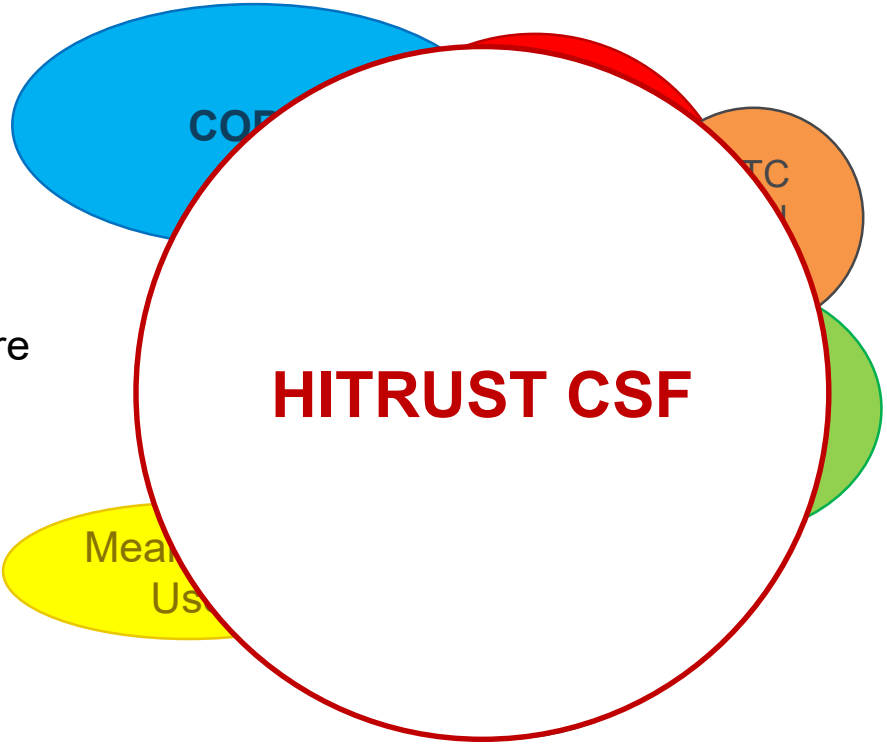


Building a Cybersecurity Strategy

Cybersecurity Framework

Choosing HITRUST CSF

- It is specific for healthcare organizations
- It has a cross reference with frameworks and laws like NIST CSF, ISO 27001, JCI, HIPAA, COBIT, GDPR
- The levels of implementation are according to features like number of beds and number of physicians
- Has a cross reference with JCI that is a short-term goal for the hospital



"Healthcare Sector Cybersecurity Framework Implementation Guide" https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf

Adoption of CSF

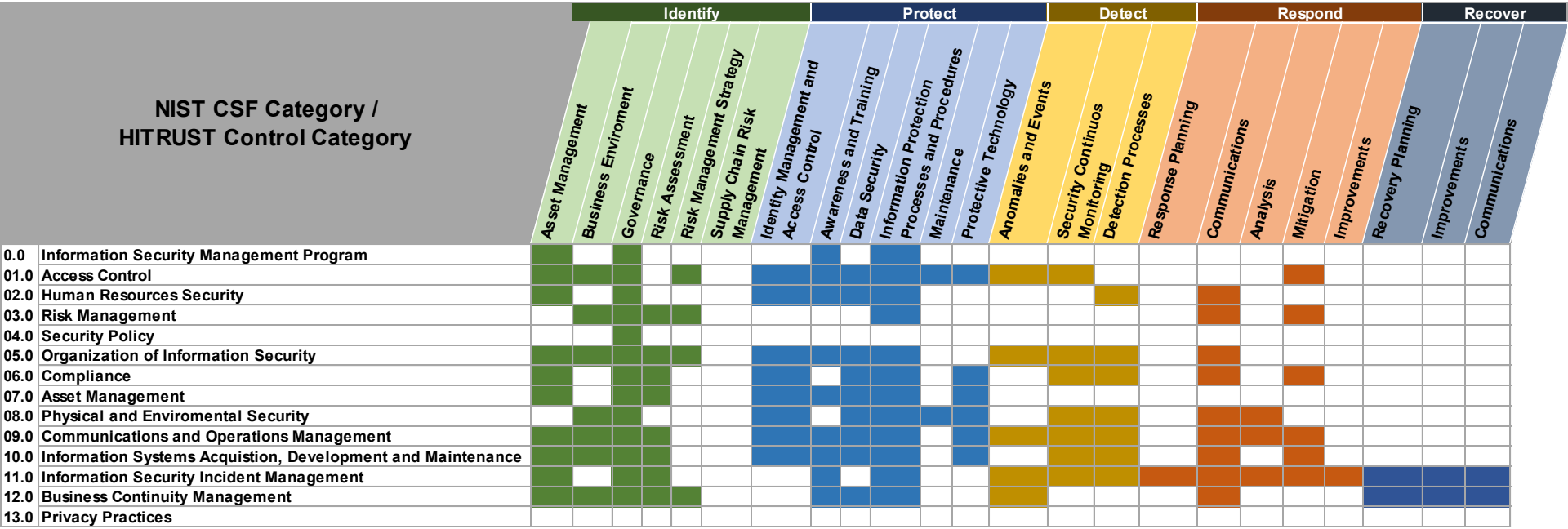
Table 17: Security Frameworks

Framework	N	percent
NIST	**103**	**57.9%**
HITRUST	47	26.4%
Critical Security Controls	44	24.7%
ISO	7	18.5%
COBIT	13	7.3%
Other	9	5.1%
No security framework has been implemented at my organization	30	16.9%
Don't know	15	8.4%

Q. Which of the following security framework(s) does your organization use? Please select all that apply.

"2018 HIMSS Cybersecurity Survey" https://www.himss.org/2018-himss-cybersecurity-survey

NIST CSF and HITRUST CSF



Building a Cybersecurity Strategy

Organization Profile

Cybersecurity Framework

Organization Profile

- Who is your Organization?
  - Mission, Vision and Strategy
  - Organizational culture and employees
  - Regulatory requirements
  - Main stakeholders
  - Environment
- Financial strategy
- Main constraints
- IT Budget
- Patient Safety as a main concern
- Baldrige Excellence Framework for Healthcare could be a good guide to perform this assessment

"About the Baldrige Excellence Framework (Health Care)" https://www.nist.gov/baldrige/about-baldrige-excellence-framework-health-care

"Suited" Cybersecurity Framework

Organizational Factors	Level 1	Level 2	Level 3
Beds	Applicable to all organizations	Between 200 and 750 Beds	Greater than 750 Beds
Health Plan/Insurance/PBM		Between 1 million to 7.5 Million Lives	Greater than 7.5 Million Lives
HIE Transactions		Between 1 and 6 Million Transactions	More than 6 Million Transactions
Hospital Admissions		Between 7.5k and 20k Patients	More than 20k Patients
IT Service Provider		Between 15 and 60 Terabytes(TB)	More than 60 Terabytes(TB)
Non-IT Service Provider		Between 25 and 100 Megabytes(MB)	More than 100 Megabytes(MB)
Pharmacy Companies		Between 10 million to 60 million Prescriptions	Greater than 60 million Prescriptions
Physician Count		Between 11 and 25 Physicians	Greater than 25 Physicians
Physician Encounters		Between 60k to 180k Encounters	Greater than 180k Encounters
Record Count Annual		Between 180k and 725k Records	More than 725k Records
Record Total		Between 10 and 60 Million Records	More than 60 Million Records
Geographic scope		Multi-State	Off-shore (outside U.S.)

Process, People and Technology

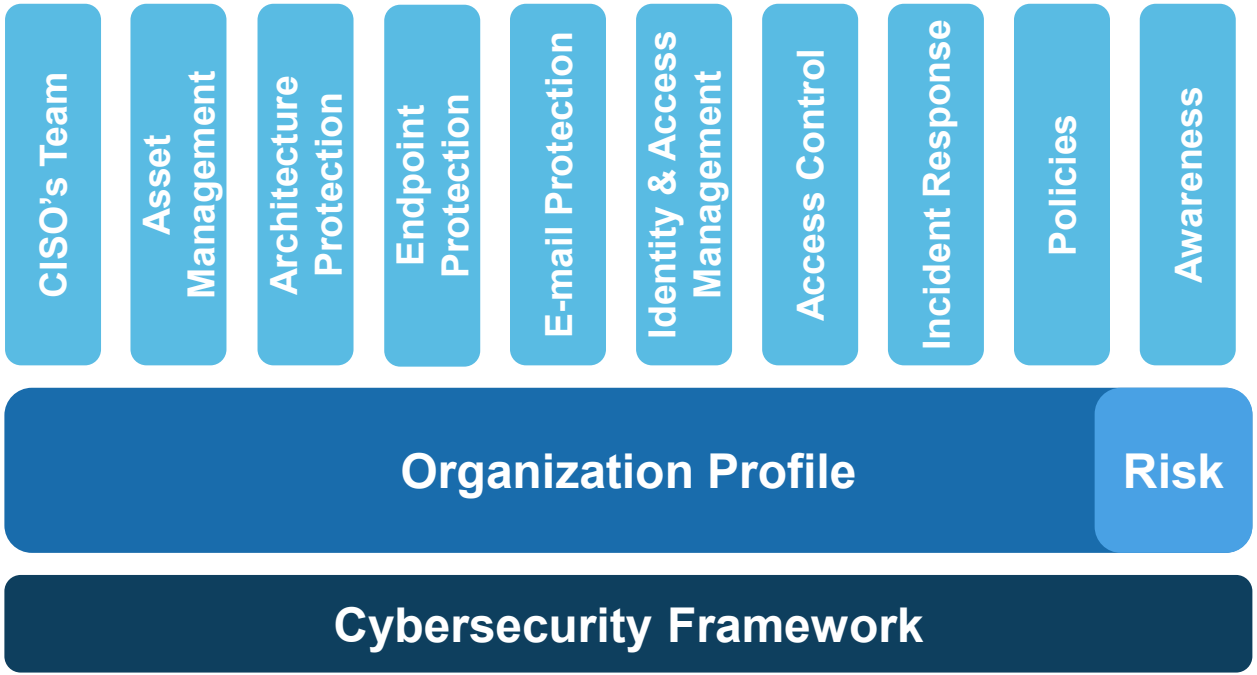
Function	Category	People	Process	Technology
Identify	Asset Management	Applies	Applies	Applies
	Business Environment	Applies	Applies	
	Governance	Applies	Applies	
	Risk Assessment	Applies	Applies	Applies
	Risk Management Strategy	Applies	Applies	
	Supply Chain Risk Management	Applies	Applies	
Protect	Identity Management and Access Control	Applies	Applies	Applies
	Awareness and Training	Applies	Applies	
	Data Security	Applies	Applies	Applies
	Information Protection Processes and Procedures	Applies	Applies	Applies
	Maintenance	Applies	Applies	Applies
	Protective Technology	Applies	Applies	Applies
Detect	Anomalies and Events	Applies	Applies	Applies
	Security Continuous Monitoring	Applies	Applies	Applies
	Detection Processes	Applies	Applies	
Respond	Response Planning	Applies	Applies	
	Communications	Applies	Applies	
	Analysis	Applies	Applies	Applies
	Mitigation	Applies	Applies	Applies
	Improvements	Applies	Applies	
Recover	Recovery Planning	Applies	Applies	
	Improvements	Applies	Applies	
	Communications	Applies	Applies	

Building a Cybersecurity Strategy

Risk Assessment

- Conduct a Risk Assessment based on your organization's profile can show:
  - Inside threats
  - Outside threats
  - Risks aligned with the strategy of the organization like:
    - Patient Safety
    - Electronic Health Record availability, privacy and integrity
- The HITRUST Threat Catalogue could be a good source of risks to be considered during the assessment
- The result should be a GAP Analysis that is going to be one of the inputs in the strategy construction

Building a Cybersecurity Strategy



CISO's Team

Protect, Defend, Prevent

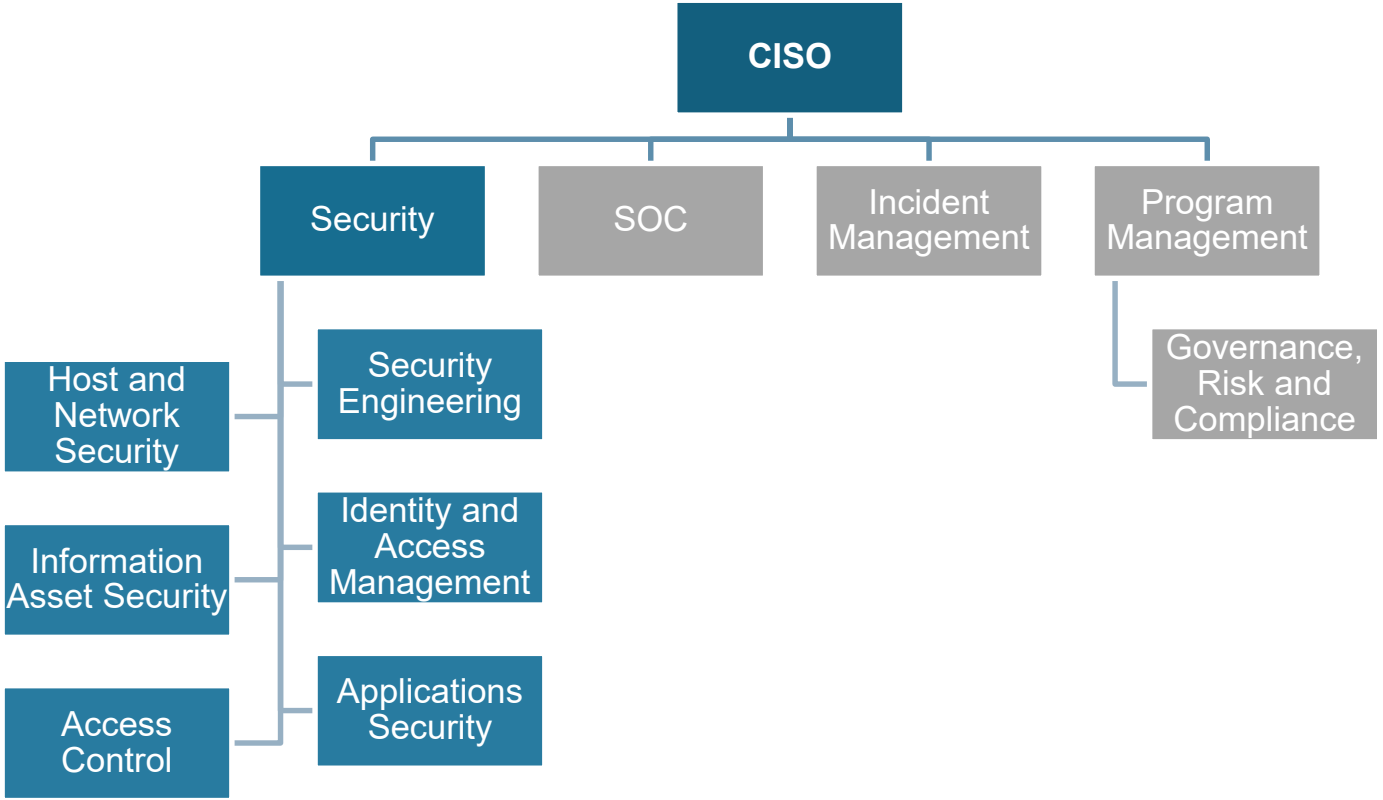
Monitor, Hunt, Detect

Govern, Manage, Educate

Respond, Recover, Sustain

Carnegie Mellon University "Structuring the Chief Information Security Officer Organization"

CISO's Team



Carnegie Mellon University "Structuring the Chief Information Security Officer Organization"

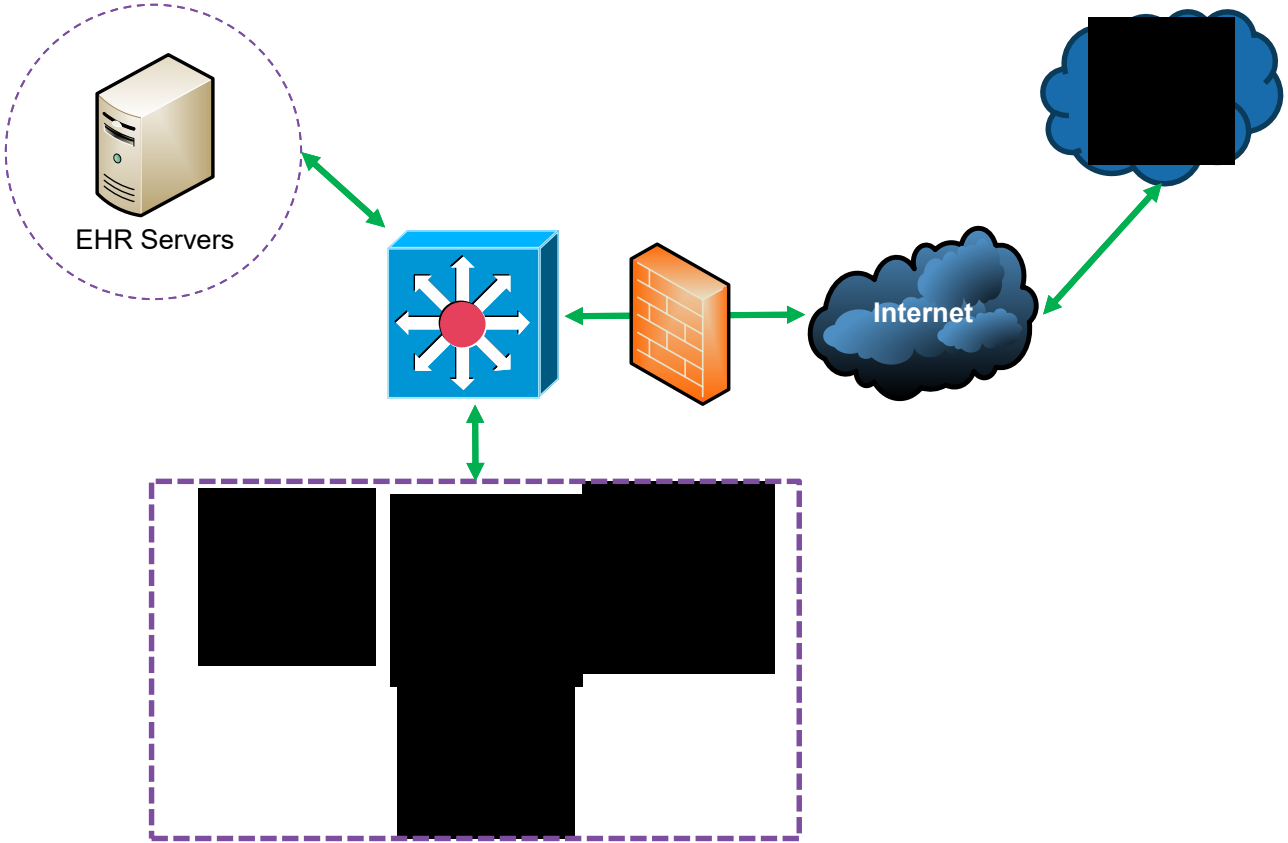
Asset Management

- Build an updated inventory including medical devices
- Use tools with agents to keep an updated remote inventory of the asset
- Make sure to create or to participate in a committee to evaluate new incoming technology
- ISO 55001:2014 – Asset management
- AdHopHTA – European Project on Hospital Based Health Technology Assessment

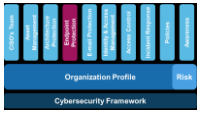
"AdHopHTA – European Project on Hospital Based Health Technology Assessment"
http://www.adhophta.eu/sites/files/adhophta/media/adhophta_handbook_website.pdf

Asset Management

"Architecture" Protection



Endpoint Protection



- First line of defense between the end user and your devices
- An Antivirus based on signatures is not enough for todays threats
- It will help you to keep your inventory updated
- Time retrospective and a sandbox are useful to find the patient zero

E-mail Protection

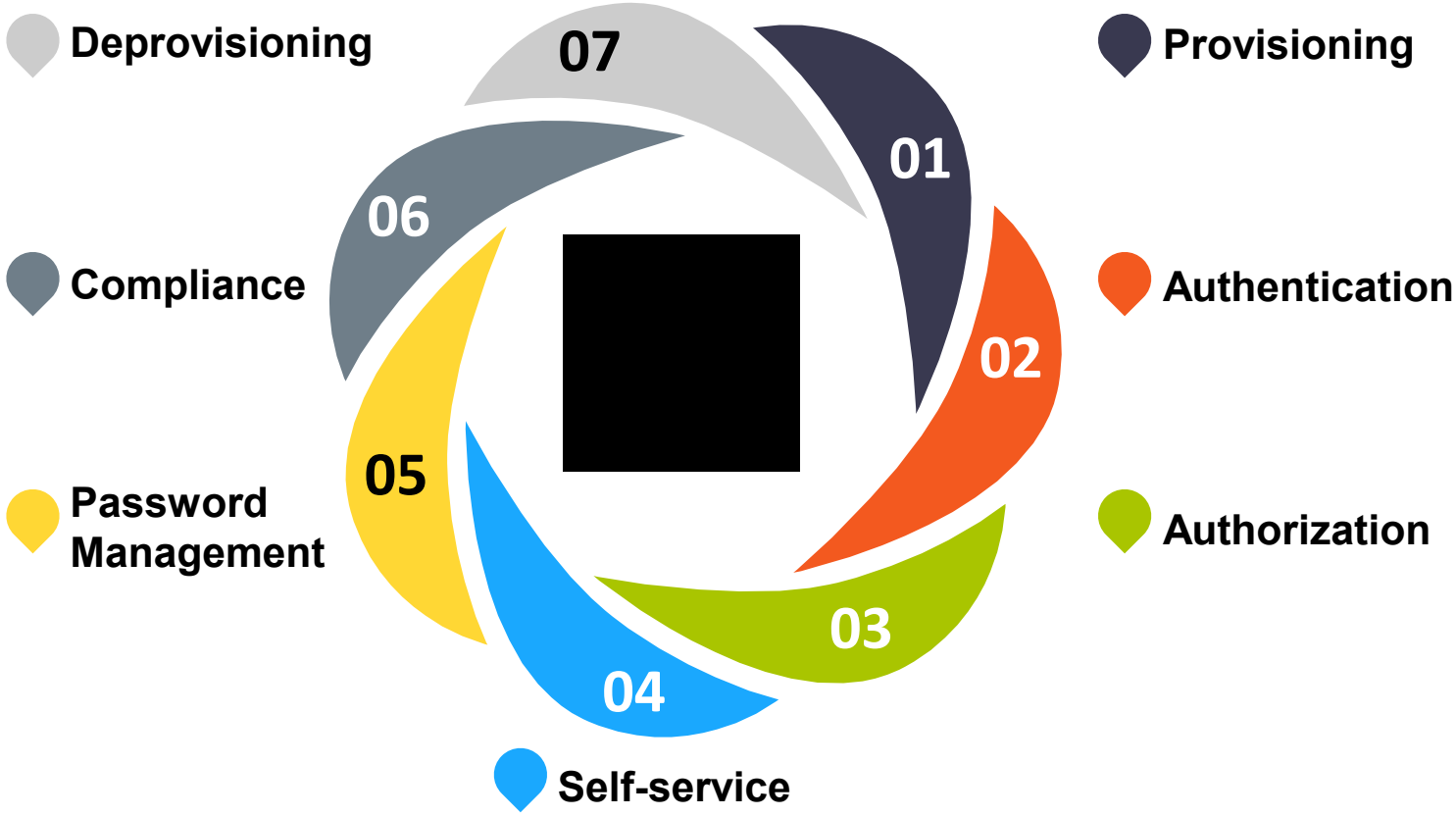
Table 6: Recent Significant Security Incident: Initial Point of Compromise

Initial Point of Compromise	N	percent
E-mail (e.g., phishing e-mail)	**117**	**61.9%**
Compromised organizational website	6	3.2%
Hardware or software infected with malware "off the shelf" (e.g., pre-loaded malicious software)	6	3.2%
Infected or compromised mobile device	4	2.1%
Infected or compromised medical device	4	2.1%
Third party website (e.g., watering hole attack or otherwise)	3	1.6%
Compromised cloud provider/service	3	1.6%
Other	24	12.7%
Don't know	22	11.6%

Q. Thinking about your organization's most recent significant incident, which of the following best describes the initial point of compromise?

"2018 HIMSS Cybersecurity Survey" https://www.himss.org/2018-himss-cybersecurity-survey

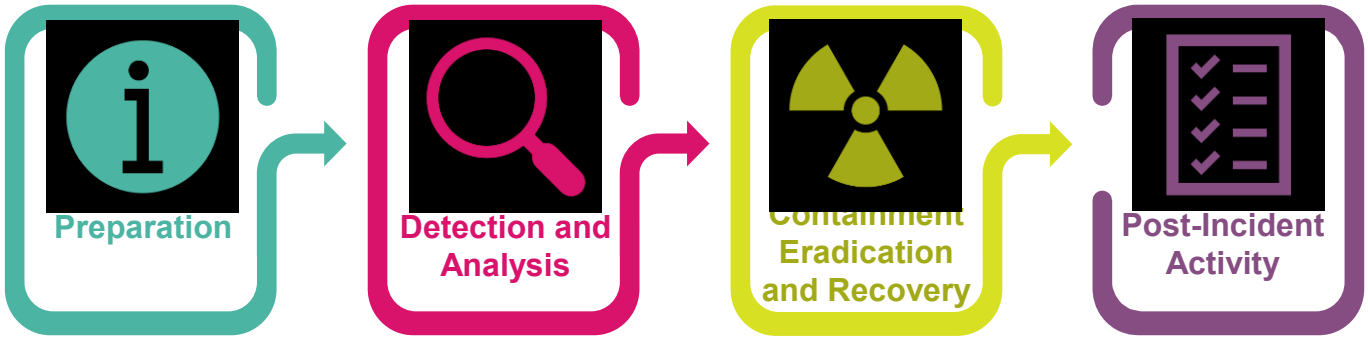
Identity and Access Management



Access Control

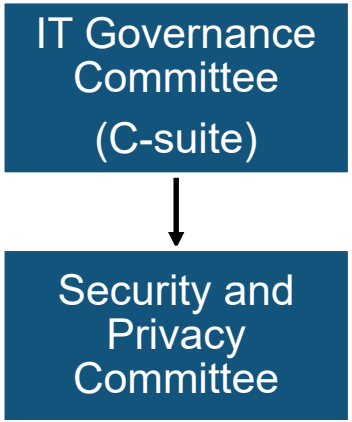
Incident Response

- The incident response team is conformed at the time of the event and the roles, responsibilities and tools are well defined in a procedure
- The end user should also be trained in order to know what he/she needs to do in case of a cybersecurity incident



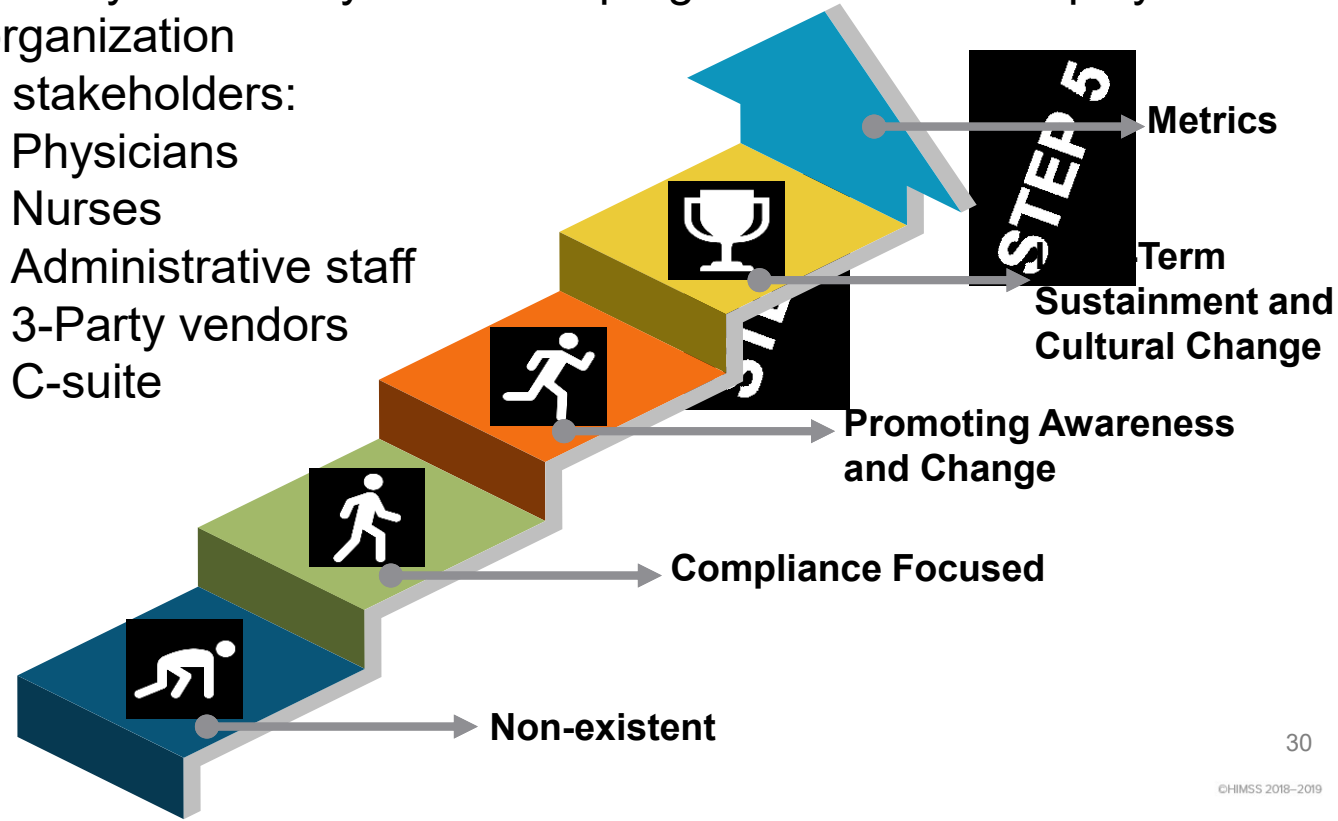
Policies

- Development and maintenance of policies and procedures are a main component
- Policies are defined in the Security and Privacy Committee that is a part of the IT Governance Strategy

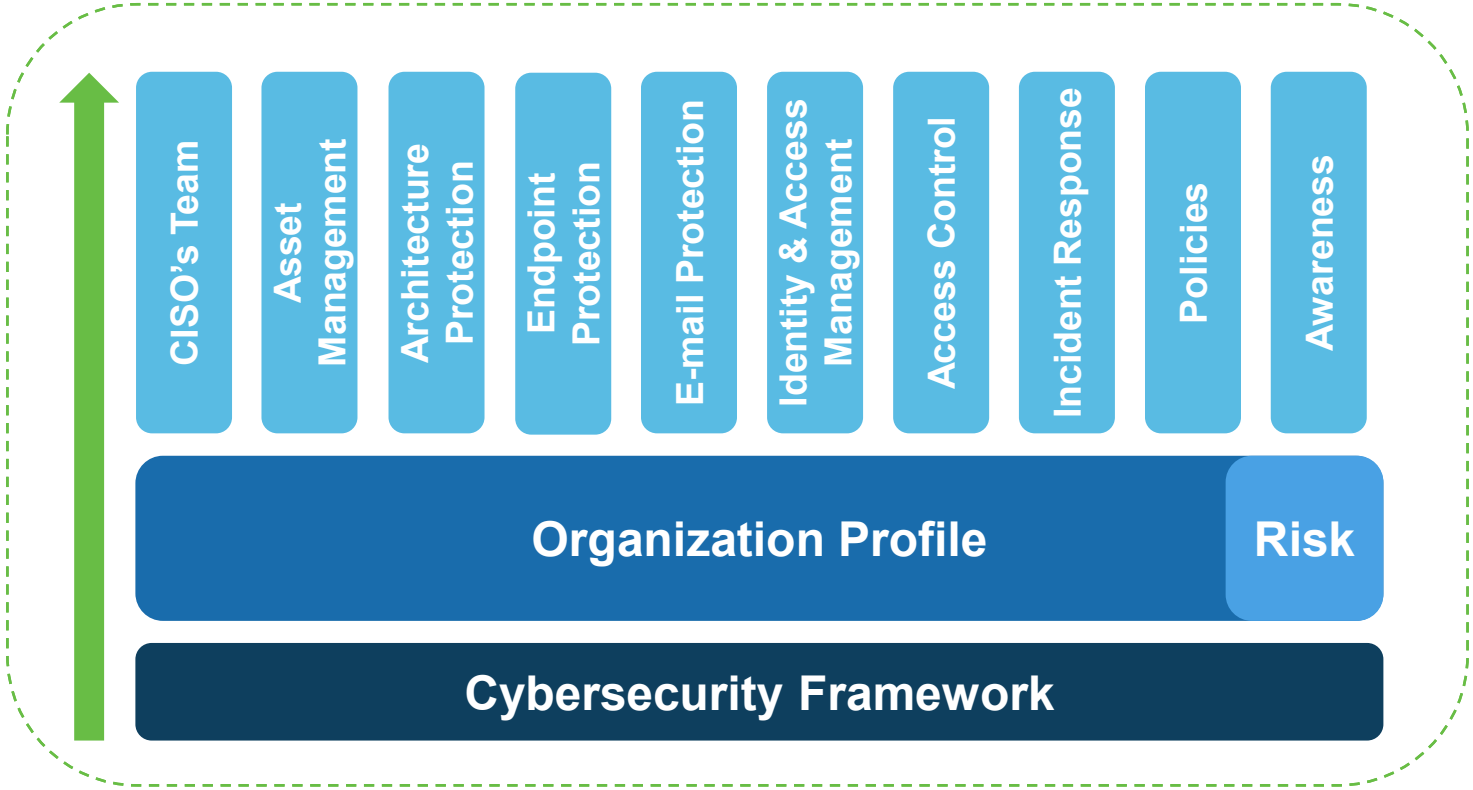


Awareness: Cultural Change

- Build an cybersecurity education program for all the employees of the organization
- Main stakeholders:
  - Physicians
  - Nurses
  - Administrative staff
  - 3-Party vendors
  - C-suite

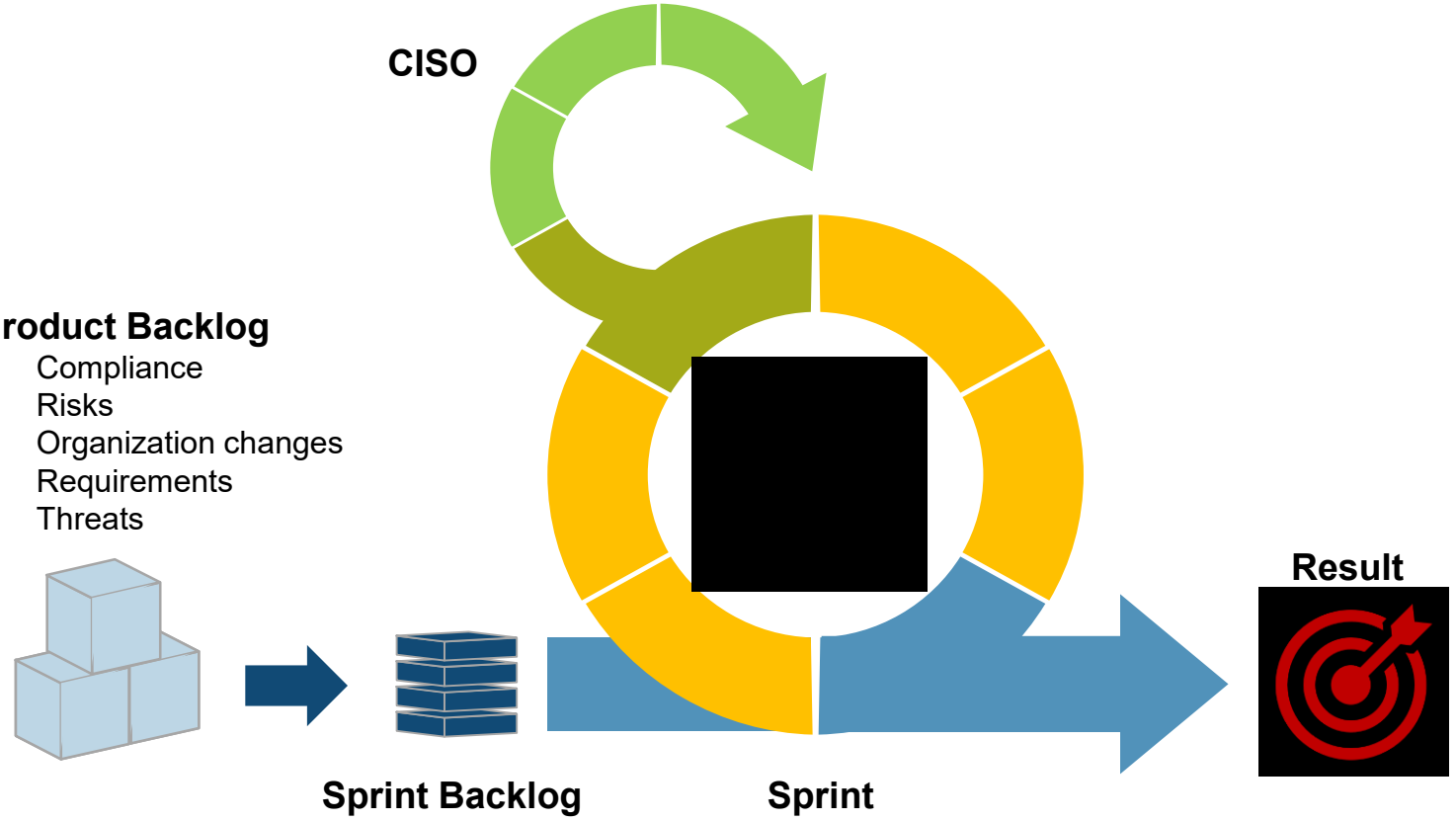


Building a Cybersecurity Strategy



Cybersecurity Strategy

Which should be the goal?



Questions

FUNDACIÓN VALLE DEL LILI
Excelencia en Salud al servicio de la comunidad

- Susan Villaquiral
- E-mail: Susan.Villaquiral@fvl.org.co
- Twitter: @sdv_87

- Remember to complete the online session evaluation

¡Gracias!