NTNU

Kunnskap for en bedre verden

HSPAMI-FRAMEWORK:

Towards Modelling and Analyzing Healthcare Staffs' Information Security Practices

Prosper K. Yeng
PhD Candidate
Center for Cyber and Info. Sec./eHealth Welfare Sec. Group
prosper.yeng@ntnu.no

Outline

Motivation

Current trend study approaches

Regulatory, Legal and standard requirements

Framework

Discussion/Conclusion

NTNU

About 3 million records breached (half the total population of Norway)

Insider aid(whether deliberate or not)

Citizens humble inquiry: "Are hospitals providing adequate protection to our sensitive data "

THE ATTACKS

NEWS

3 phishing hacks breach 20,000 Catawba Valley patient records

by **Jessica Davis** | October 25, 2018

While investigating one phishing attack in August, medical center officials discovered a hacker had access to three accounts for more

NEWS

CMS responds to data breach affecting 75,000 in federal ACA portal

by **Susan Morse** | October 22, 2018

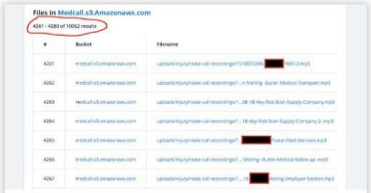
Open enrollment, which begins November 1, will not be negatively impacted, CMS says.

NEWS

Two phishing attacks on Minnesota DHS breach 21,000 patient records

by **Jessica Davis** | October 12, 2018

For more than a month, two separate employee accounts were compromised by the cyberattacks before the IT department



NEWS

Update: Misconfigured database breaches MedCall Advisors

by **Jessica Davis** | October 10, 2018

A researcher discovered the North Carolina-based tech vendor is leaking protected patient data through its Amazon S3 bucket

NEWS

3 Massachusetts hospitals fined nearly $1 million by OCR for HIPAA violations

by **Jessica Davis** | September 21, 2018

Boston Medical Center, Brigham and Women's Hospital and Massachusetts General Hospital let ABC film a documentary on site without

NEWS

Employee error exposed Blue Cross patient data for 3 months

by **Jessica Davis** | September 21, 2018

An employee uploaded a file containing member information to a public-facing website in April, but officials did not discover

NTNU

Why is healthcare data the target?

According to ISO 27799:2016

Healthcare organizations usually collect detailed personal information due to the ultimate importance to perfectly identify patients and correctly match them to their health records.

The detailed personal information is of great value to cybercriminals for committing identity theft.

Healthcare records Richer and More Sensitive

(Caroline Humer and J. Finkle, 2014, ISO 27799:2016)

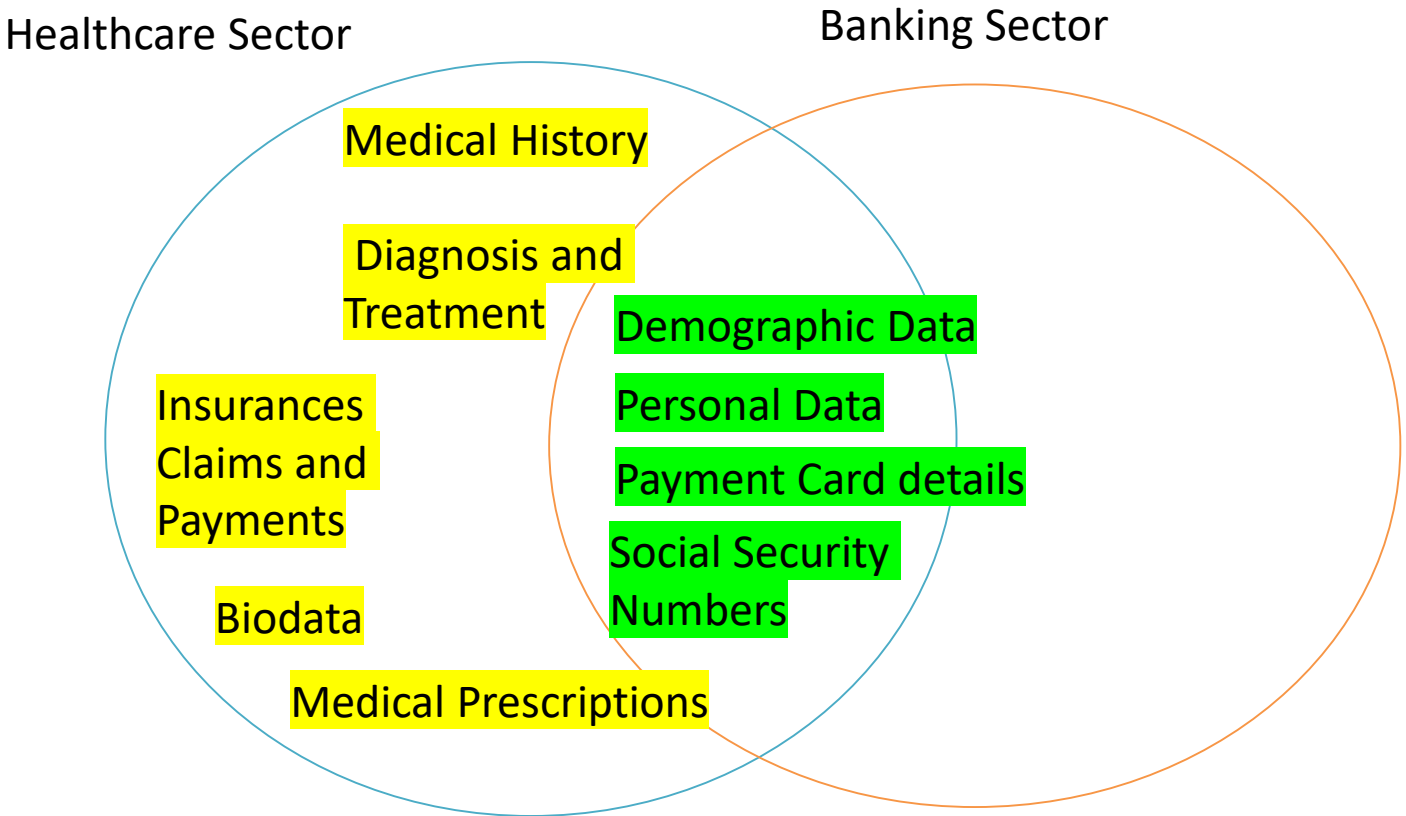



DIAGRAM 1
DARK WEB SERVICES
PORNOGRAPHY
PHARMACEUTICALS
WEAPONS
BLOGS
FINANCIAL FRAUD SITES
DRUGS
FAKE DOCUMENTATION SERVICES
CARDING SITES
wp.com/securityaffairs.co

Mutual Trust

Threat on

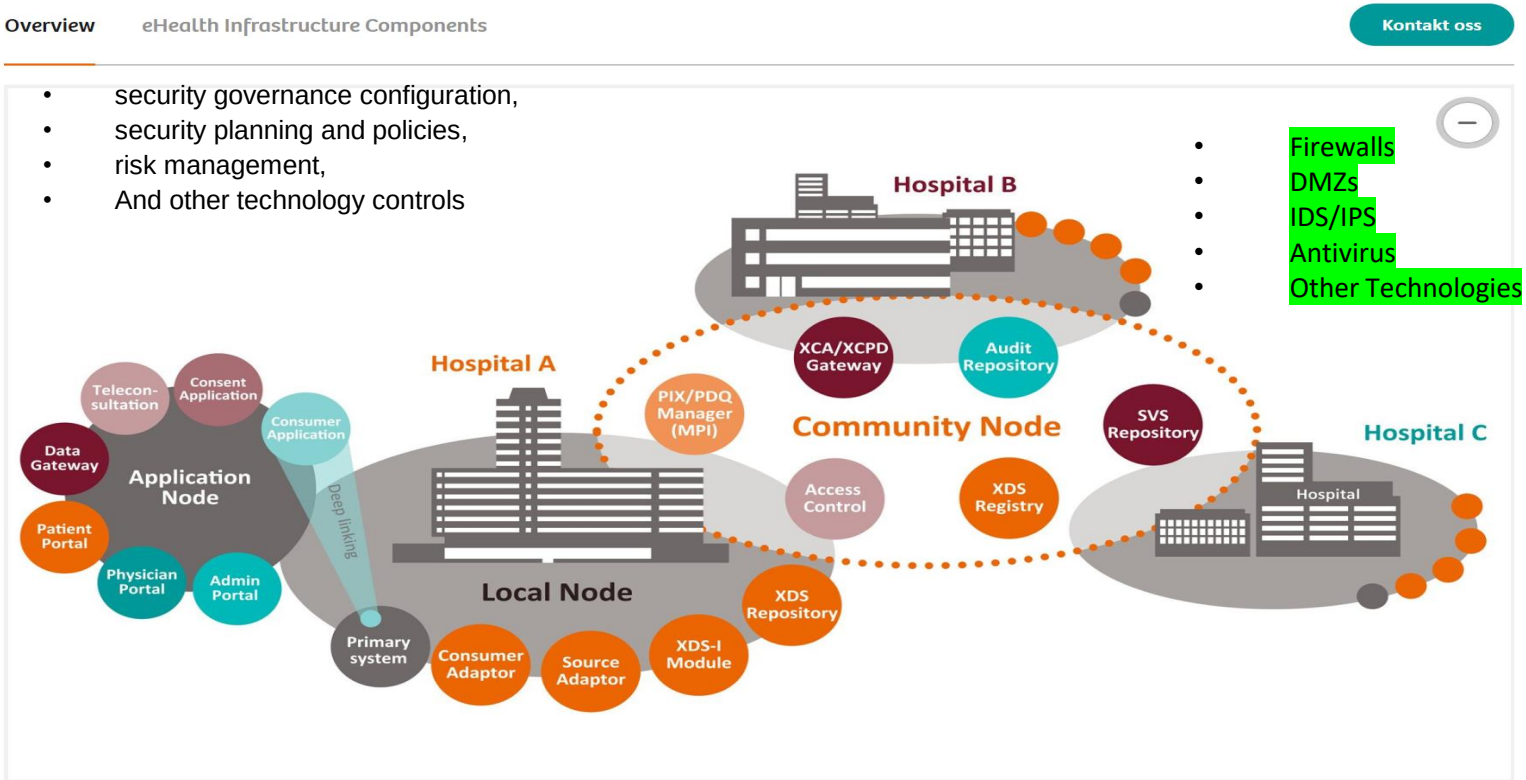
- mutual trust and confidentiality
- between healthcare and patients

(Pedersen, S. and G. Hartvigsen,2015)

"If patients do not feel that their personal medical information will be kept confidential, they may withhold important medical information from health care providers making it difficult to provide quality and effective health care"Drye et al.,2010

More attention on tech. measures than the human firewall!

Norwegian eHealth infrastructure(Siemens-healthineers, 2018)



Default Priority of healthcare staff- not information security

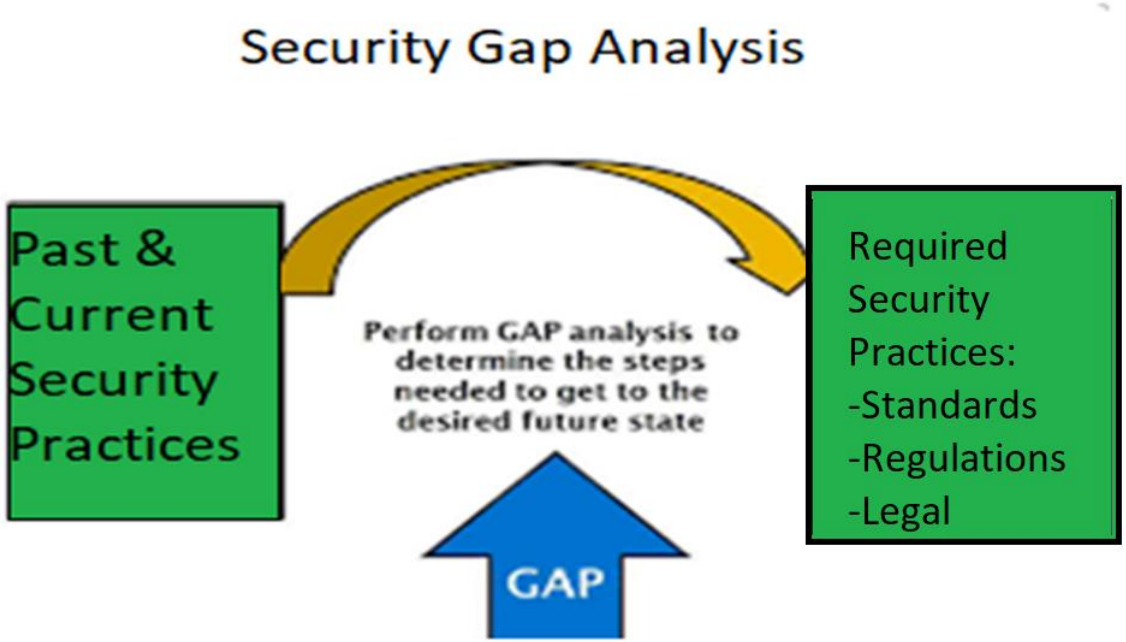
- Default setting of healthcare staffs is on healthcare delivery
- Funding in healthcare being chronically reduced leading to reduction in personnel with increased workload
- Humans- the Weakest link in the sucurity chain

In summary


Healthcare staffs' Concious care practice
Technological
Measures

END OF ROAD???

Goal


Security Gap Analysis
Past & Current Security Practices
Perform GAP analysis to determine the steps needed to get to the desired future state
GAP
Required Security Practices:
-Standards
-Regulations
-Legal

Research Questions

- How can the security practice of a healthcare staffs be determined?
- What characteristics and security practices of healthcare staffs should be observed?
- How should that be observed?
- Where should that be observation?

Staffs' Charateristics Cont…

Safa, N.S., et al 2015, Yuryna et al., 2017

- Socio-demographic characteristics
  - age,
  - gender,
  - education,
  - workload level,
  - emergency situation
  - the security experience

- psycho-socio-cultural traits referred to personal behaviors that are influenced by psychological, social and cultural factors:
  - ✓ perception,
  - ✓ attitude,
  - ✓ norms
  - ✓ beliefs
  - ✓ Social Bonding
  - ✓ Peer Pressure

Security Practices

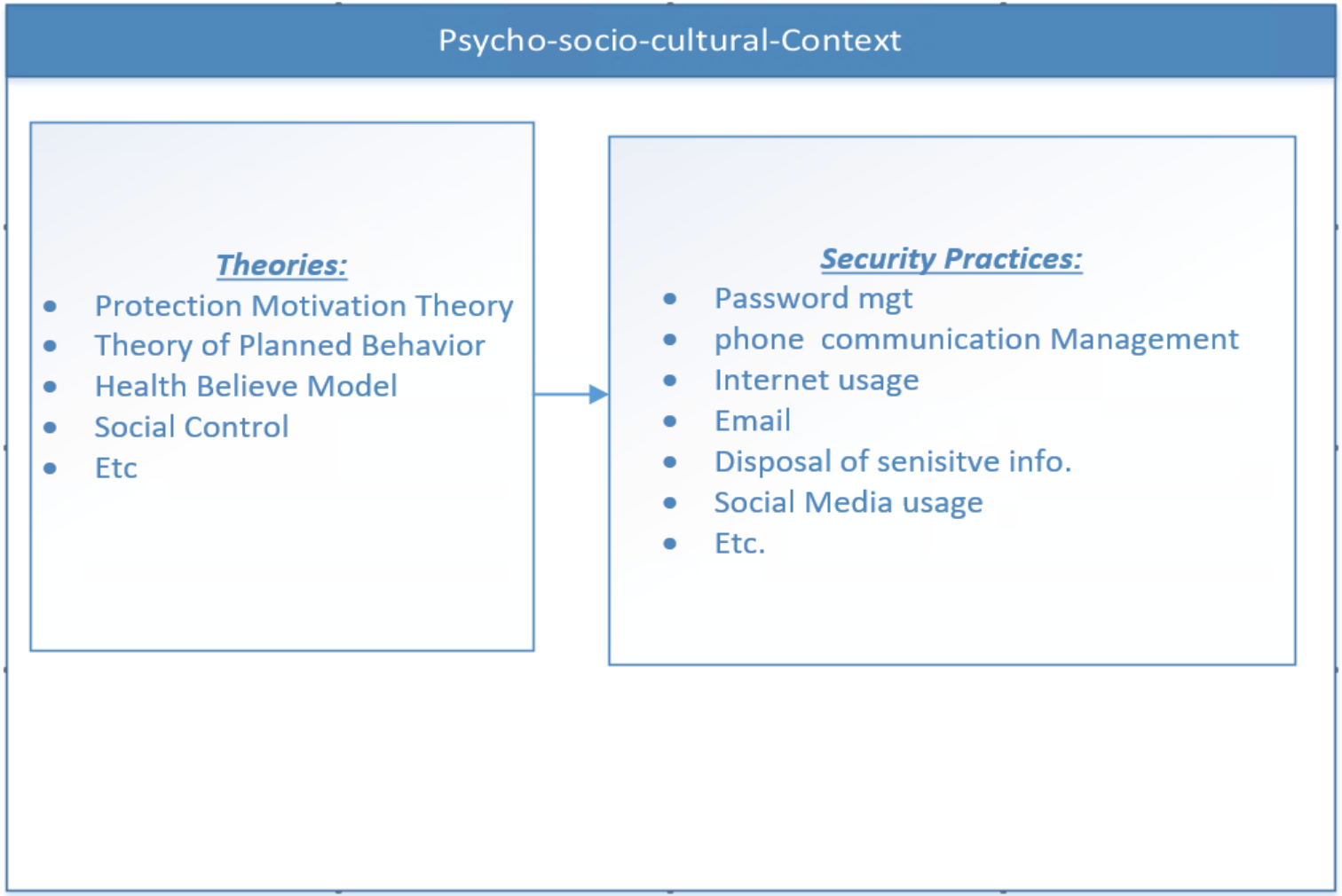
- Security Practices includes security measures being adopted by healthcare staff in their IS usage in order to prevent compromising the CIA of resources

- **Security practices**:
- internet use,
- email use,
- social media use,
- password management,
- incident reporting,
- information handling
- mobile computing
- Etc.

McCormac, A., et al. 2017

Literature Survey

Framework/Study	HSPAMI Study areas addressed	Approach
A conceptual framework [11]	Users perception	Qualitative, Quantitative
Framework for healthcare information assurance policy and compliance[12]	Users perception	Qualitativy
Security practices of healthcare staffs in real clinical setting.[15]	Users perception, Social Control	Survey with questionnaires
Protection Motivation Theory (PMT) and Theory of Planned Behavior (TPB)[16]	Users perception	Survey with questionnaires
Conceptual Framework [19]	Big data analysis	Comparison of input data with known attack signatures
Network anomaly detection sensor (SNAD)[20]	Big data analysis	Comparison of input data with established pattern
Local Outlier Factor (LOF) in Electronic Patients Records [21]	Big data analysis	KNN
Cyberattacks Against U.S. Healthcare Systems[22]	Social Engineering	Reviews of phishing attacks
Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system[24].	Social Engineering	Phishing Attack-Defense simulation
Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions[25]	Social Engineering	Phishing Attack-Defense simulation


Psycho-socio-cultural-Context
Theories:
Protection Motivation Theory
Theory of Planned Behavior
Health Believe Model
Social Control
Etc
Security Practices:
Password mgt
phone communication Management
Internet usage
Email
Disposal of senisitve info.
Social Media usage
Etc.

Protection Motivation Theory(PMT)

- Ability to protect oneself base on;
  - perceived severity of a threatened event,
  - perceived probability of the occurrence, or vulnerability,
  - the impact of the recommended, preventive Measure
  - perceived self-efficacy.

Social Engineering

- Observe security practice
- Develop security metric

Big data analysis
(Boddy, et al., 2016;Chen et al., 2012; Yeng et al., 2019)

Model and analyze access-related data

Determine Anomaly

Assess Anomaly to determine malice behavior

Determine and adminster intevention measures

Summary of Survey

- All the studies:
  - Recognized the issues of human factors in healthcare information security
  - Contributed towards enhancing the ‘human-firewall’ to augment the technological measures
  - What is in short fall was:
    - the lack of holistic approach
    - Lack of anchorage to the desires of national and international Regulations, Laws and standards in healthcare

NTNU

Need for holistic measure?

Attack-Defense without Psycho-socio-cultural metrics and vise versa

Observational Measures (Review)

- Observational measures include observing how users respond to the security controls towards meeting security requirements of the policies ISO:27000:2018.

Observational Measures (Review)

What characteristics and security practices of healthcare staffs should be observed?

How should that be observed?

Where should that be observation?

Existing observational measuers

- The sources of measures include (Yeng et al. 2019)
  - system setting;
  - installed programs;
  - running processes;
  - online activities;
  - browser history;
  - network connections;
  - warnings;
  - file system;
  - running processes of backup task.

NTNU

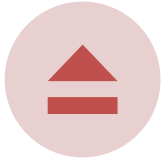
ISSUES WITH EXISTING OBSERTIONAL MEASURES

None of the above studies indicated their observational measures to meet the key security lookups as provisioned in various standards and code of conducts for healthcare security and data privacy protection in Norway

Develop Observational measures from Required Security practices in Healthcare

Regulations (GDPR, NIS Directives, HIPPAA)

Laws



Standards(ISO 27002,27799:2016)

Ethics, Best Practices and Code of conducts

Security tools in healthcare(Anomaly Detection systems)

Reports on data breaches in healthcare

Relevant laws in healthcare

The Health Records Act,

The Health Personnel Act,

The Personal Health Data Filing System Act,

The Health Research Act,

The Patients' and Users' Rights Act

(Pedersen, S. and G. Hartvigsen,2015)

Other Regulations, Standards and Directives

Health Insurance Portability and Accountability Act

The HIPAA privacy rule;

the HIPAA security rule

ISO 27799:2016

The Hippocratic oath required to upheld confidentiality of PHI.

Code of Conduct for information security and data protection in the healthcare and care services (e.g., Norway).

Network and Information Systems (NIS) EU Directives

Spectrum of observational measures

- Access Control
- Employees, competence and attitude-forming campaigns
- Communications Security
- Physical security and the handling of equipment
- Security IT operations
- Digital Communication with healthcare users
- ICT Readiness
- Handling of information security breaches
- Suppliers and Agreements

How was the observational measures developed?

The code of conduct and ISO 27799 provided various technical implementations

Forming H0 AND H1

For instance,

under access control, technical measures are to be kept in place to prevent unauthorized accesses to PHI.

How was the observational measures developed? Cont…

- So, the observational measures were developed by forming an alternative hypothesis from the technical security measures.

- In this instance, the alternative hypothesis was formed as, “There are unauthorized accesses to PHI”.

How was the observational measures developed? Cont…

- The alternative hypothesis presented
  - a responsibility
  - and a challenge
- for us to explore and synthesize the observational measures for the specified security practices.

How was the observational measures developed? Cont…

- Tailed observational measures found include
  - self-authorization,
  - interorganizational accesses of PHI

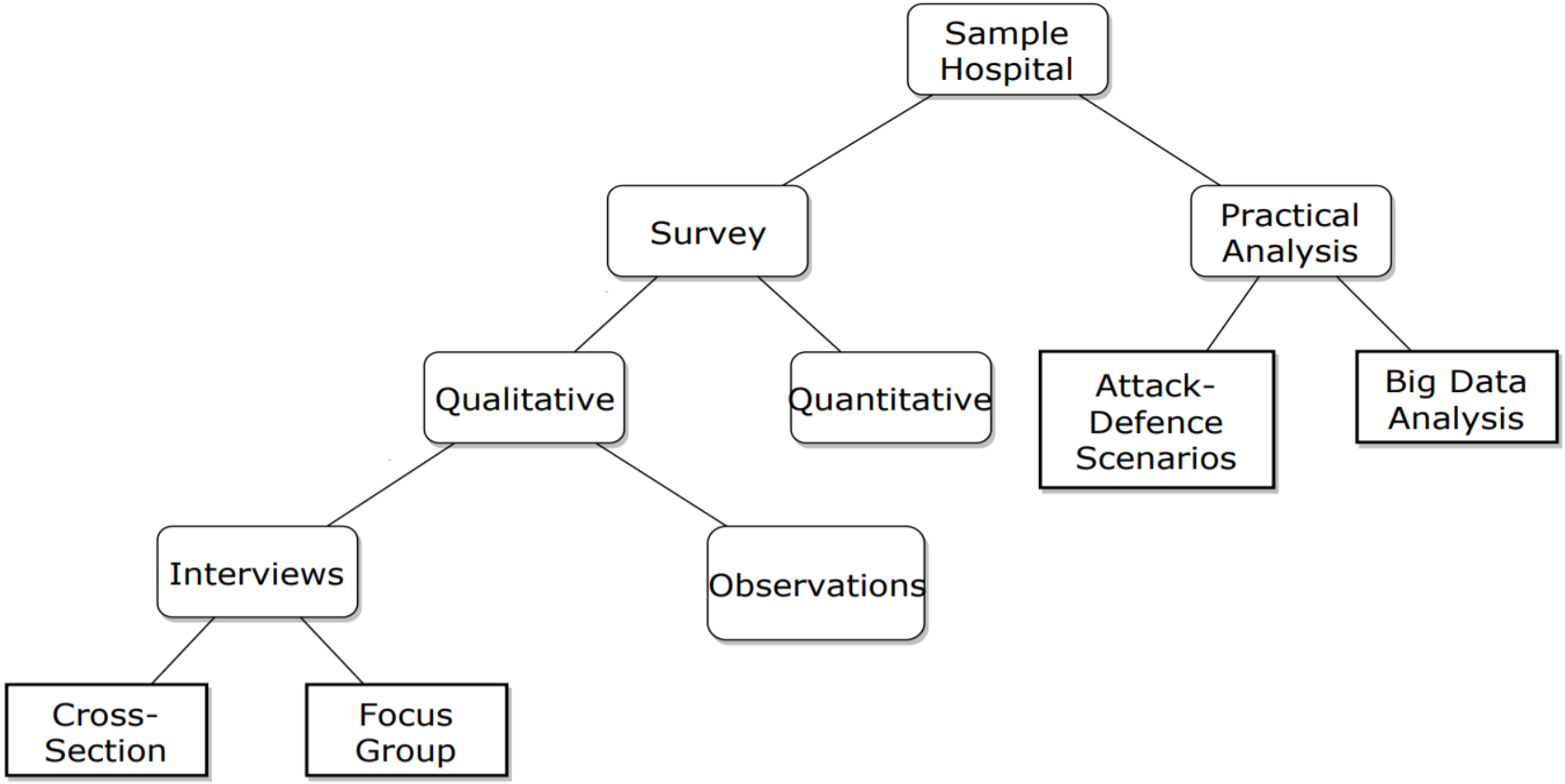
How was the observational measures developed? Cont…

In addition, the following methods could be used in the assessment

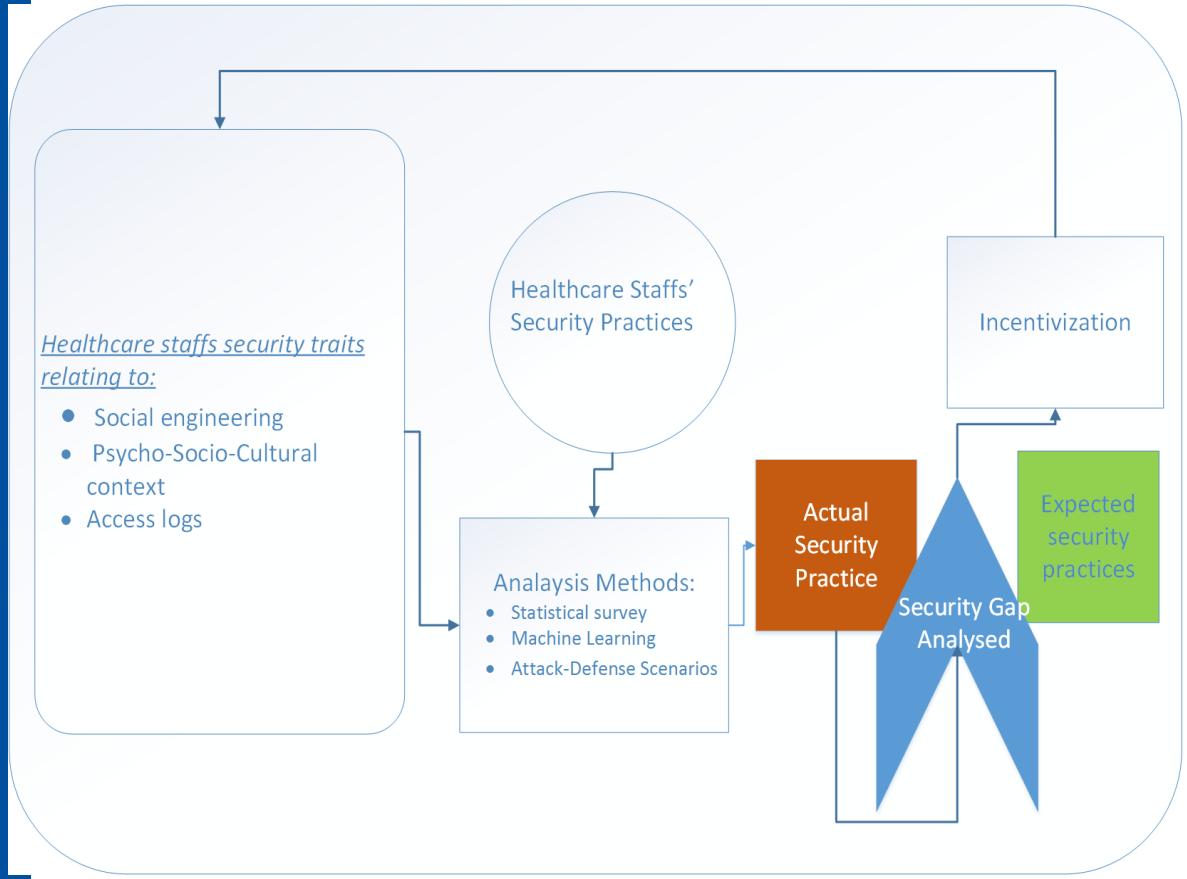
- Artificial Inteligence/Machine Learning
- Test scenarios (eg if the necessary and relevant PHI would be available in situations where the EHR is deemed not available)
- Statistical analysis(qualitative, quantitative)

H1	Possible causes and Related Threats	Detection/Observational Measure	Source/Logs
1. Access Control			
There are unauthorized accesses to PHI	user access misconfiguration, impersonations resulting in direct violation of patient' confidentiality, security and privacy issue on necessary and relevant accesses	Compare user access profile with current accesses. Check accesses with authorization register eg purpose, time, location, authorizer, access rights, planned therapeutic patient and schedule, quantum of authorize access, Check misuse of self-authorization and interorganizational accesses	EHR, Network log
Personnel do not have unique authentications	This can cause unauthorized accesses. Eg password sharing	Check for sharing authentication criteria, logins after shift time, and location of logins, login with default password and unique user computer behavior such as keystrokes and mouse clicks dynamics. Psycho-socio-cultural measures	HER
2. Employees, competence and attitude-forming campaigns			
PHI is disclosed through the usage of e-mail, text or other unencrypted channels	It compromises the right of patients to confidentiality	Use content filtering to scan email text, images and attachments, for potential threats. Test to get PHI and user credentials via social engineering and phasing attacks	HER/ Attack-Defense scenario
4. Physical security and the handling of equipment			
Not all personnel obtain keys/access/cards/password through known procedures	Unauthorized persons can have Keys/Access cards to computing resources	Check for abnormal physical access profile of users. Eg. Abnormal physical accesses will deviate from their established profile or pattern	Physical access log
7. ICT Readiness			
Shutdown of EHR will cause non-availability of essential PHI	Non-available essential PHI will result in a range of incorrect patient treatment to loss of lives	Test for the availability of essential PHI in electronic information system shutdown scenarios/Qualitative Study	

Study Structure



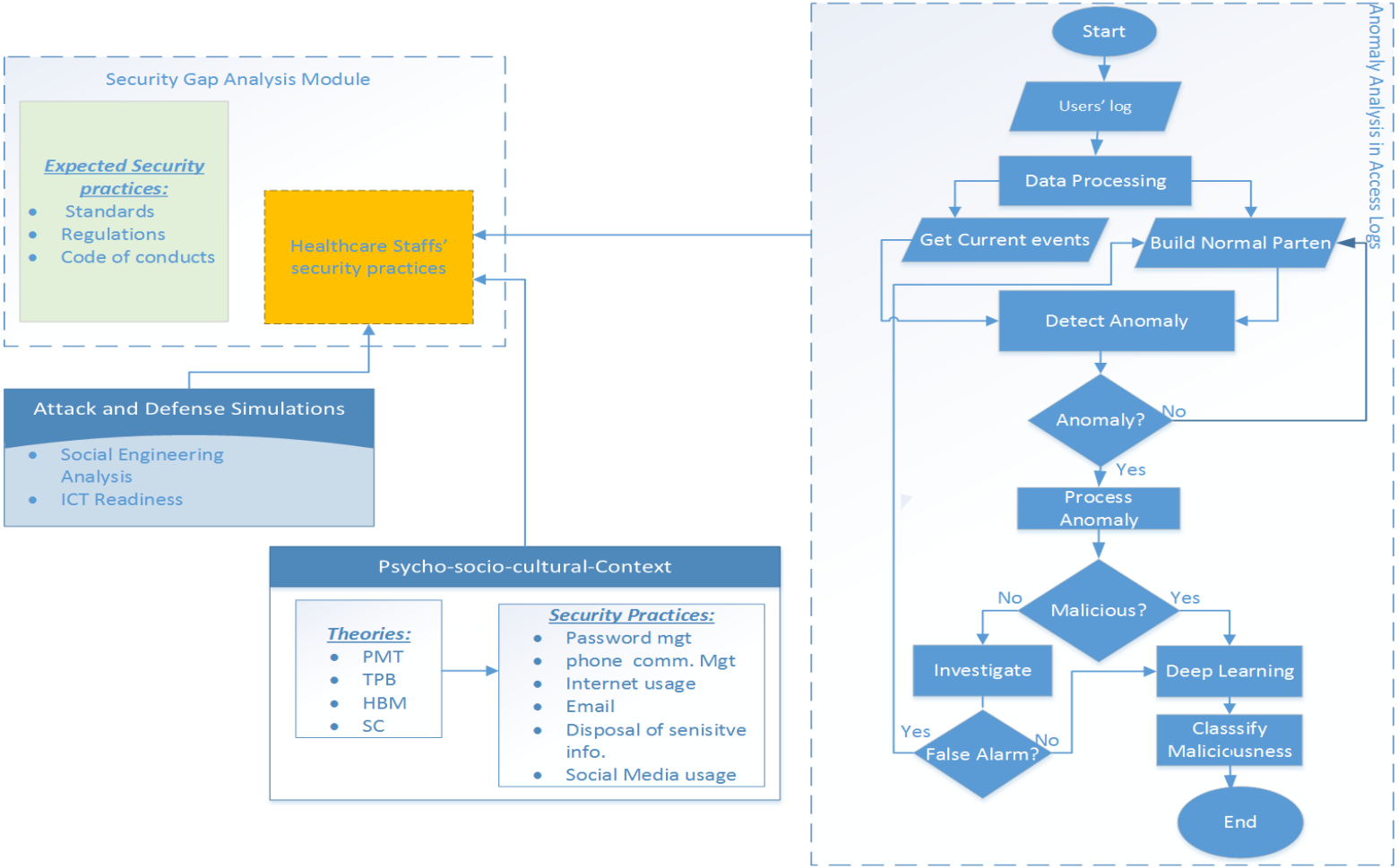
Overview of HSPAMI Study Cycle



Security Practices:

- Password mgt
- phone communication Management
- Internet usage
- Email
- Disposal of senisitve info.
- Social Media usage
- Etc.

Proposed framework



Conclusion

Comprehensive framework was proposed towards modeling and analyzing healthcare staffs' security practices

The framework was based on mandated security conducts combined with standards which are most specific to healthcare information security.

Conclusion cont…

- These standards and code of conducts, are measured up to global standards, legal and regulatory requirement which are being revived to improve upon their vitality for healthcare security counter measures

NTNU

Conclusion Cont…

Concious care security practices could be inculcated onto our busy, weakest link in the security chain(healthcare staffs) with HSPAMI framework

Reference

1. Foroughi, F. and P. Luksch. Observation Measures to Profile User Security Behaviour. in 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). 2018.
2. ISO, ISO 27799:2016(en), Health informatics Information security management in health using ISO/IEC 27002. 2016.
3. Nurse, J.R.C., et al. Understanding Insider Threat: A Framework for Characterising Attacks.IEEE Security and Privacy Workshops. 2014.
4. Boddy, A., et al. A Study into Detecting Anomalous Behaviours within HealthCare Infrastructures. in 2016 9th International Conference on Developments in eSystems Engineering. 2016.
5. Walker-Roberts, S., M. Hammoudeh, and A. Dehghantanha, A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. IEEE Access, 2018. 6: p. 25167-25177.
6. e-helse, D.f. Implementation of GDPR in health care sector in Norway. 2019; Available from: https://ehelse.no/personvern-og-informasjonssikkerhet/eus-personvernforordning/implementation-of-gdpr-in-health-care-sector-in-norway.
7. LOVDATA, Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven) - Kapittel 3. Taushetsplikt, innsynsrett og rett til å motsette seg behandling av helseopplysninger. 2019.
8. omsorgsdepartementet, H.-o., Act of 18 May 2001 No. 24 on Personal Health Data Filing Systems and the Processing of Personal Health Data (Personal Health Data Filing System Act), in 042041-990016. 2006, regjeringen.no.
9. Supervision, N.B.o.H., The Act of 2 July 1999 No. 63 relating to Patients' Rights (the Patients' Rights Act) in 63. 1999.
10. Neuhaus, C., A. Polze, and M. M R Chowdhuryy, Survey on Healthcare IT Systems: Standards, Regulations and Security. 2011.
11. GDPR.Report, Businesses at risk due to unidentified network traffic according to global survey - GDPR.Report. 2018.
12. Hipaa Journal, Healthcare Data Breach Statistics. 2019.
13. Norwegian Centre for E-health Research. Diabetesdagboka.no. 2018; Available from: http://www.diabetesdagboka.no/en/.
14. EUR-Lex, The European Parliament and the Council of the European Union, Regulation (EU) 2016/679, EU, Editor. 2016.
15. Pedersen, S. and G. Hartvigsen, Lessons learned from 25 years with telemedicine in Northern Norway. 2015


Thank You For Your Attention!
Questions?
PROSPER K. YENG
PhD. Candidate
Norwegian University of Science and Technology
E-mail: Prosper.Yeng@ntnu.no