A Bayesian Network Model for Predicting Data Breaches

Caused by Insiders of a Health Care Organization

Focus Group B

13-10-2016

Agenda

1. Research introduction
2. Explaining the case
3. Assignments

- Rules
  - Participate actively
  - There are no right or wrong answers
  - Every person's experiences and opinions are important
  - Speak up whether you agree or disagree
  - If you have any question please ask

Research

Introduction

Definitions - 1

- Personal data
  "any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person" (GDPR)

- Data breach
  "A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed" (GDPR)

Definitions - 2

- Insider
  "An employee who is authorized to process physical and/or digital personal data"

- Insider threat
  "an insider who uses his privileged access to intentionally or accidentally perform an act directly or indirectly leading to the unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed"

Definitions - 3

- Prior indicator
  "Information that can be observed before a data breach occurs and provides important information to determine whether a data breach is likely to occur"

- Measure
  "security mechanism, policy, or procedure that can successfully counter insider accidents or malicious insider attacks, reduce risk, resolve vulnerabilities and otherwise improve the protection of personal data within an organization"

Research Goal

Creating a Bayesian Network model to predict the probability of a data breach caused by insiders of a health care organization

1. This model should be based on prior indicators of data breaches caused by insiders and measures taken by an organization to prevent these data breaches
2. The prior indicators will be related to a group of employees
3. With this model one should be able to determine which measures a health care organization should take to minimize the probability of a data breach

Case

Case

What is the probability of a data breach caused by a group of employees in the health care sector who

1. lose employee- or employer-owned mobile devices, or
2. misuse employer-owned mobile devices by not returning them when needed or copying personal data to their own devices

Assignments

Introduction

Explanation

Individual assignment

- Are the 15 statements true or false?
- Write the answers on the form
- Do not discuss the answers with each other

Group assignment

- Divide 10 points over the categories
- The more points the higher the impact
- Discuss the answer and provide an explanation for the division

Assignments

Individual

Individual - Indicators

	True	False
Mobile device misuse results in a data breach more often than mobile device loss		
Employees have a motivation to lose a mobile device		
The capability of the employees depend on their job		
Stress increases the probability of mobile device loss		
Females misuse mobile devices more often than males		
Most of the malicious employees have a strong reason to misuse a mobile device		
Employees who are not committed to their job are less likely to misuse mobile devices		
Care workers are more likely to lose mobile devices than support and technical support staff		

Individual - Measures

	True	False
Protection against mobile device misuse is just as important as protection against mobile device loss		
Training the employees is less important than protecting the mobile devices		
Pre-employment screening is more important than performance management		
Protecting mobile devices is less important than protecting the data on the devices		
Creating policies is more important than training the employees		
Protection against mobile device loss is less important than protection against mobile device misuse		
An awareness program is more important than protection of data on the devices		

Assignments

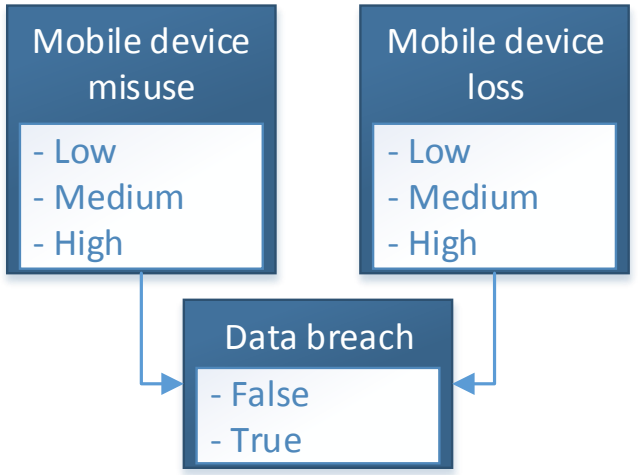
Group

Divide 10 points - 1

Does mobile device misuse result in a data breach more often than mobile device loss?

- Mobile device misuse - .....
- Mobile device loss - .....

Total - 10

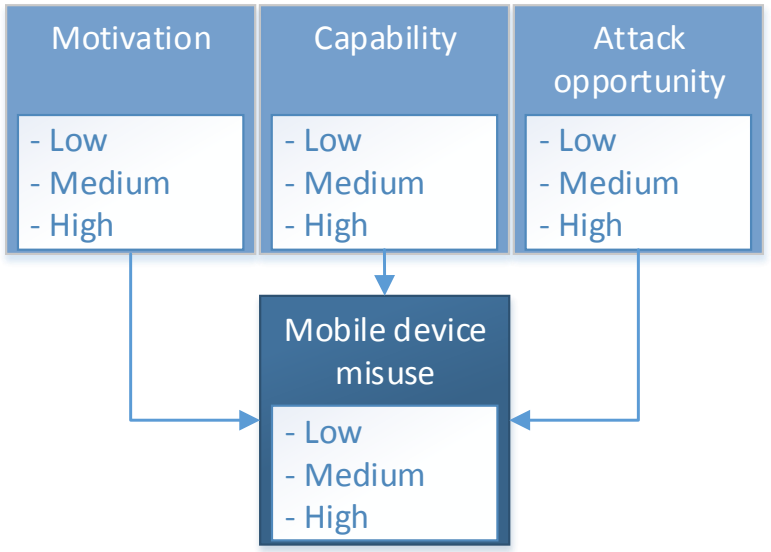


Divide 10 points - 2

Does motivation, capability or attack opportunity have the highest impact on the misuse of mobile devices?

- Motivation - .....
- Capability - .....
- Opportunity - .....

Total - 10

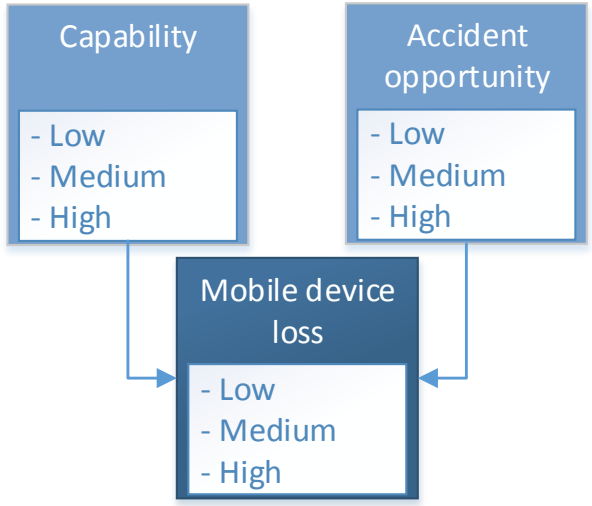


Divide 10 points - 3

Does capability or accident opportunity have the highest impact on mobile device loss?

- Capability - ……
- Opportunity - ……

Total - 10

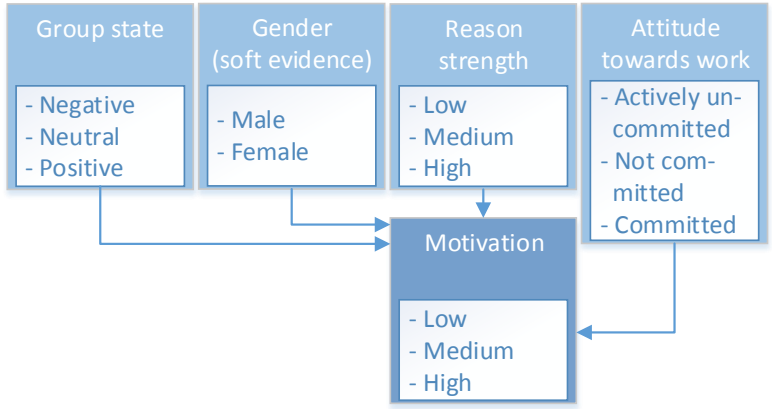


Divide 10 points - 4

What impact have group state, gender, reason strength and attitude towards work on the motivation of the employees?

- Group state - .....
- Gender - .....
- Reason strength - .....
- Attitude towards work - .....

Total - 10

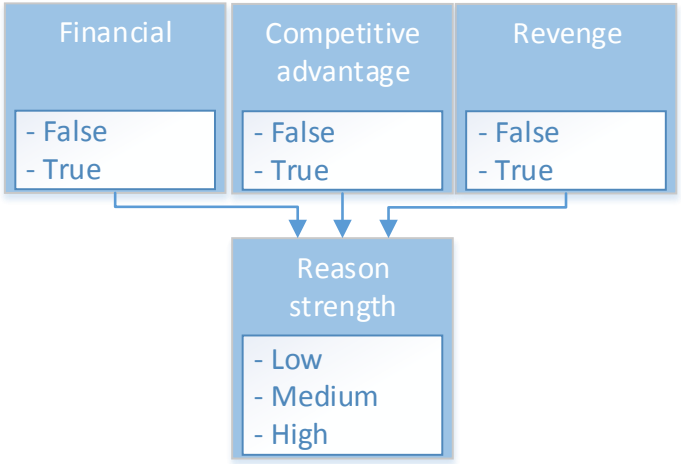


Divide 10 points - 5

Which motivation of the employees to misuse mobile devices is the strongest?

- Financial - .....
- Competitive advantage - .....
- Revenge - .....

Total - 10

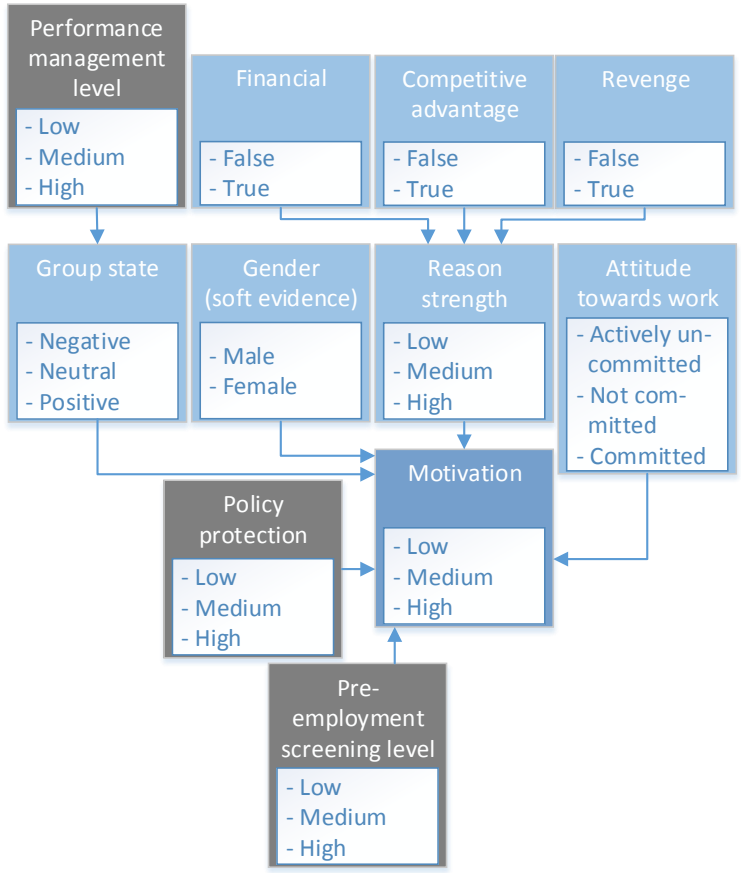


Divide 10 points - 6

Are policies the most important measure to avoid or limit insiders with a motivation to misuse mobile devices?

- Policies - .....
- Performance management - .....
- Pre-employment screening - .....

Total - 10

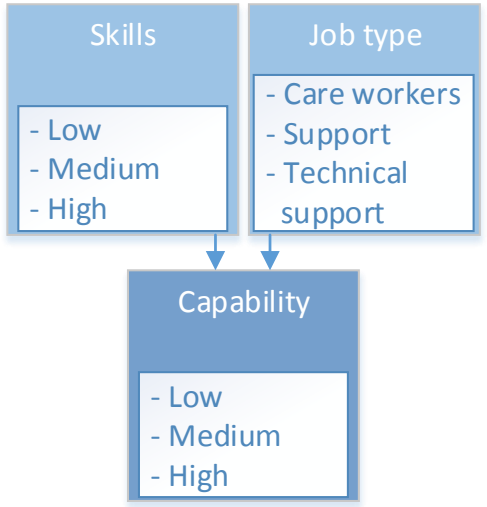


Divide 10 points - 7

What impact have skills and job type on the capability of insiders?

- Skills - ……
- Job type - ……

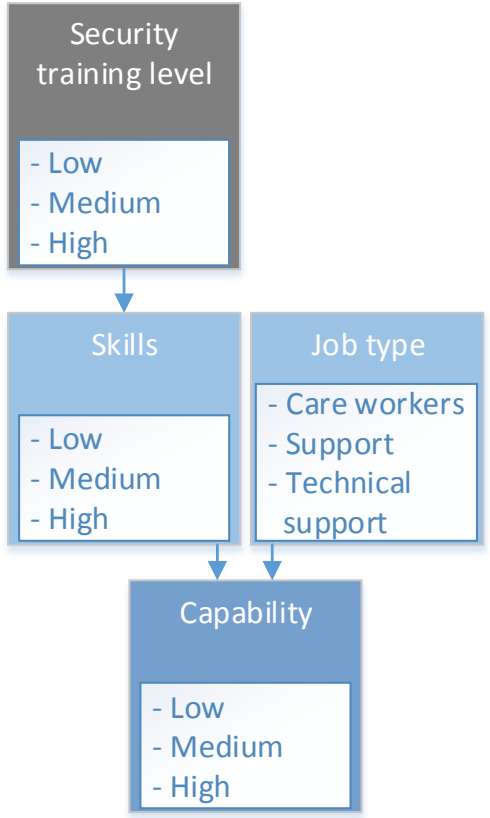
Total - 10



Divide 10 points - 8

What is the skill level of the employees given the training level?

Security training → Skills↓	Low	Medium	High
Low			
Medium			
High			
Total	10	10	10

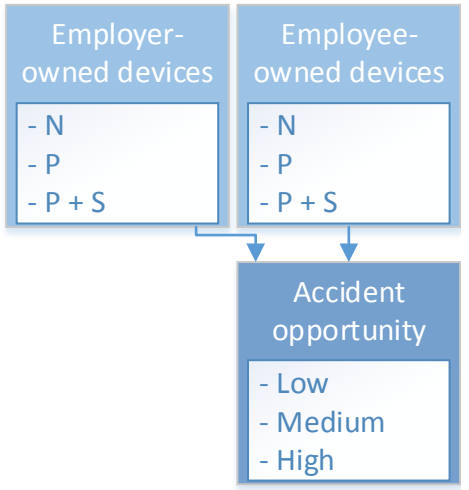


Divide 10 points - 9

Do employees more often lose mobile devices that are owned by the employer or by themselves?

- Employer-owned devices - ……
- Employee-owned devices - ……

Total - 10

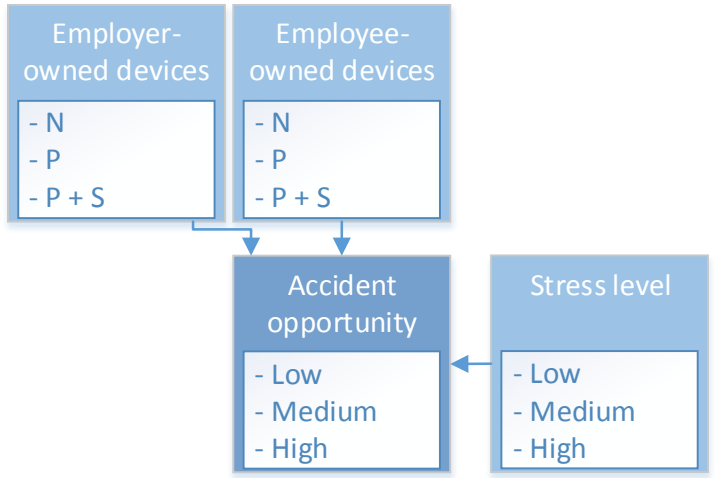


Divide 10 points - 10

Which of the three indicators has the highest impact on an accident opportunity?

- Employer-owned devices - ……
- Employee-owned devices - ……
- Stress level - ……

Total - 10

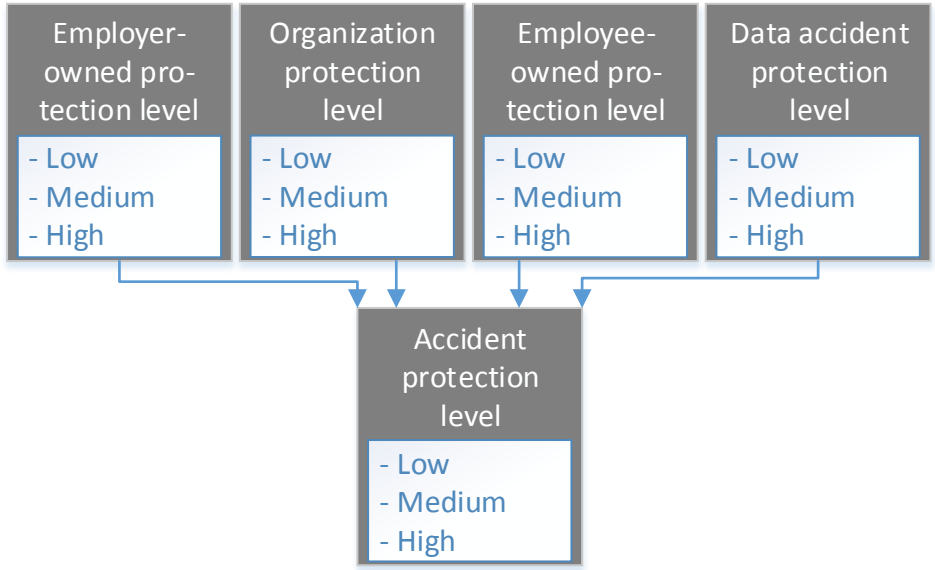


Divide 10 points - 11

Which measures are the most effective to increase the accident protection level?

- Employer-owned protection level - .....
- Employee-owned protection level - .....
- Organization protection level - .....
- Data accident protection level - .....

Total - 10

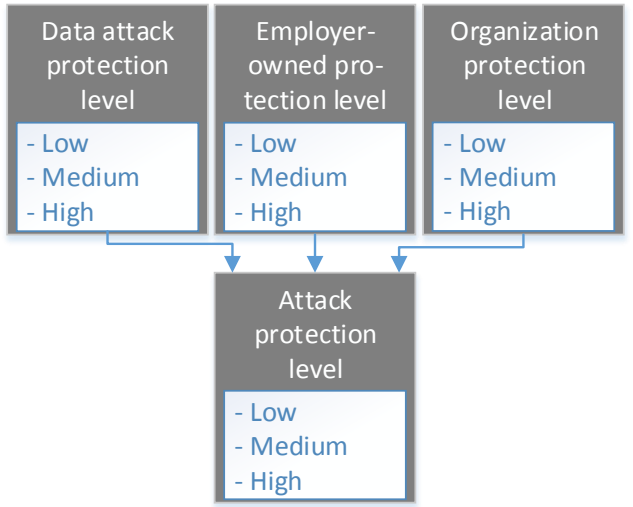


Divide 10 points - 12

Which measures are the most effective to increase the attack protection level?

- Employer-owned protection level - .....
- Organization protection level - .....
- Data attack protection level - .....

Total - 10



Any Other Comments or Questions

Thank you for your participation!

I will send you a summary of this discussion, so you can

- read the outcome of this session, and
- correct wrong statements