Slide 01

Hi all, today I am focusing my presentation on how can we mitigate cyber security risk caused by the human factor effect of our own ASMIS's users on the system itself.

Slide 02

Let's recap what Human Factor is and why it is an essential determinator in Cyber Security. **This is just for making a solid base for understanding the solutions I am proposing here later in the presentation.**

Referring back to my earlier report on "Addressing Human Factors for Secure & Usable ASMIS", I referred to the study from

Ponemon Institute in the USA – it is an independent research and education organisation, focused on advancing the responsible use of information and privacy management practices.

In their 2020 global insider threat study covering 204 organisations – 4716 recorded insider incidents -> of which 62% of security breaches are from human error and negligence of employees (non-malicious).

-> Number of incidents recorded in 2020 was 4716, and in 2018 only 3200 were recorded - the number of incidents increased by 47%

-> Average cost increased to 31% from $8.76 million in 2018 to $11.45 million

So what is Human Factor ? According to the definition guidance of Insider Threat Team, CERT (2013),

Our users - an employee, a contractor, or a patient who have or had authorised access to ASMIS/data could ***become an unintentional insider threat through action or inaction without malicious intent ->*** causing harm to the confidentiality, integrity, or availability of ASMIS and data.

BUT, is this the fault of our users? No, it is not. In my following few slides, I will explain why and ***how we can address these through understanding, collaboration, and practical solutions***.

Slide 03

So lets see; **How can our current/past users become** an unintentional insider threat through action or inaction?

In my previous report, I identified 3 conditions that could contribute to non-malicious insider threats or even could make unavoidable adverse outcomes harming CIA (confidentiality, integrity, or availability)

1. IMPACT of low ASMIS user readiness

Caused by business processes and environment settings leading to ***work stress-based cognitive impacts (attention deficits, poor situational awareness, and reduced working memory capacity)***

Example - responding to a phishing message when attending to too many emails

2. INFLUENTIAL risk tolerance/behaviour

Caused by psychosocial, sociocultural factors leading to ***variable risk perceptions***

(Examples of psychosocial factors include social support, loneliness, marriage status, social disruption, bereavement, work environment, social status, and social integration.)

Example - Shappie et al. (2019) provides evidence that ***Individuals high in conscientiousness and openness are more likely to engage in cybersecurity-related behaviours.***

3. FALL BACK on cognitive biases in decision making

Caused by security and compliance fatigue due to bombarded demands for compliance that users cannot take anymore, leading to ***becoming less likely to comply as users tend to fall back on cognitive biases when making decisions***

Example - ***Ignoring continuous messages from Antivirus software***

Slide 04

So,

what solutions can we consider to manage human factors?

Slide 05

Let's go through Human factors one by one and find out how we can control damage from unintentional insider threats? **as they can never be eliminated entirely**.

The 1st identified HUMAN FACTOR

Impact of low user readiness caused by work pressures from business process and operational environment settings

As increase work pressures from business processes and environment settings leads to….. work stress-based cognitive impacts the likelihood of employees lowering the acceptable performance thresholds and shedding some or even critical security-related responsibilities.

Real life Example:

1. If employee **X** gets five minutes between meetings, if there isn't enough to log on and print the documents that the employee needs, and might tend to go to a colleague **Y** and ask to use the computer to print the required documents. That colleague **Y** quickly lets employee **X** use the personal account while getting a cup of tea. Since employee **X** has only 5 minutes, leave the computer unattended to the next meeting as colleague **Y** gets delayed at the coffee machine area chatting with another.
2. Having 7/8 passwords to remember to work on a busy working day?

How to overcome?

First of all, we have to understand what cause adverse impacts on employee behaviour

Why users bend or break the rules to get their work done?

This can be done through a;

- ✓ A periodic short worker survey or
- ✓ Investigation of the business processes and the operational environment

We can gather the information that helps to clarify any unintended effects on employee morel or employee performance and take actions to mitigate such operational work settings.

Slide 06

The 2nd identified HUMAN FACTOR

Psychosocial, Sociocultural factors may influence risk tolerance/behaviour.

Real life Example:

Would you really spot a phishing email on a busy working day among another 50/60 emails if you have to keep on answering the phone while attending to emails - when you have to process them all in seconds and think about 10 other things at the same time?

A study by Shappie et al. (2019) provides evidence that ***Individuals high in conscientiousness and openness are more likely to engage in cybersecurity-related behaviours.***

The ***study also concluded that education could bridge this gap*** by providing anti-phishing education, reducing the inclination to provide information to phishing web pages by 40%.

How to overcome?

Improving employees' sense of cyber security self-efficacy by evaluating socio/cultural work environment

This can be done through; definitely through proper trainings

- ✓ Investing in and enhancing cyber security practices by employing emotion- and logic-based influencers
- ✓ Conducting training, and awareness on individuals' biases and tendencies

Slide 07

The 3rd identified HUMAN FACTOR

Security and compliance fatigue ruling cognitive biases in cyber security related decision making

What is cognitive biases ? Mental processes affecting our capability to act on a specific situation based what we have met in the past are addressed as cognitive biases.

Why **cognitive biases is important?** They can play an important role in shaping our decision-making process in reasoning, evaluating, or remembering a situation.

Due to overloaded information and compliances, one can become less likely to compliant and can relay on cognitive biases when making decisions

Real life Example:

1. Complex password policy?

How to overcome?

Security needs to fit into work processes rather than disrupt them - avoid overloaded information and compliances / security being too complex and/or effortful.

This can be done through;

- ✓ Utilising effective user-system interface designs – password manager /single sign-on, multi-factor authentication, Biometrics.
- ✓ More is not the answer - crafting effective security awareness messages is vital to avoid any security and compliance fatigue
- ✓ Referring to General MacArthur's famous quote 'never give an order that cannot be obeyed' - never issue security guidance that is impossible to follow or are not effective

Slide 08

People are not the 'Weakest Link -> organisations need staff who are loyal and engaged

Security is a complex, socio-technical system.

We really need to know how best to support users in doing their jobs so that they can do those jobs without security getting in the way.

Understanding how people function as elements of socio-technical security systems through a people-centred perspective adds to our knowledge of organisational security.

People are not the weakest link, they are the primary attack vector.

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

Bruce Schneier

I have now come to the end of my presentation.