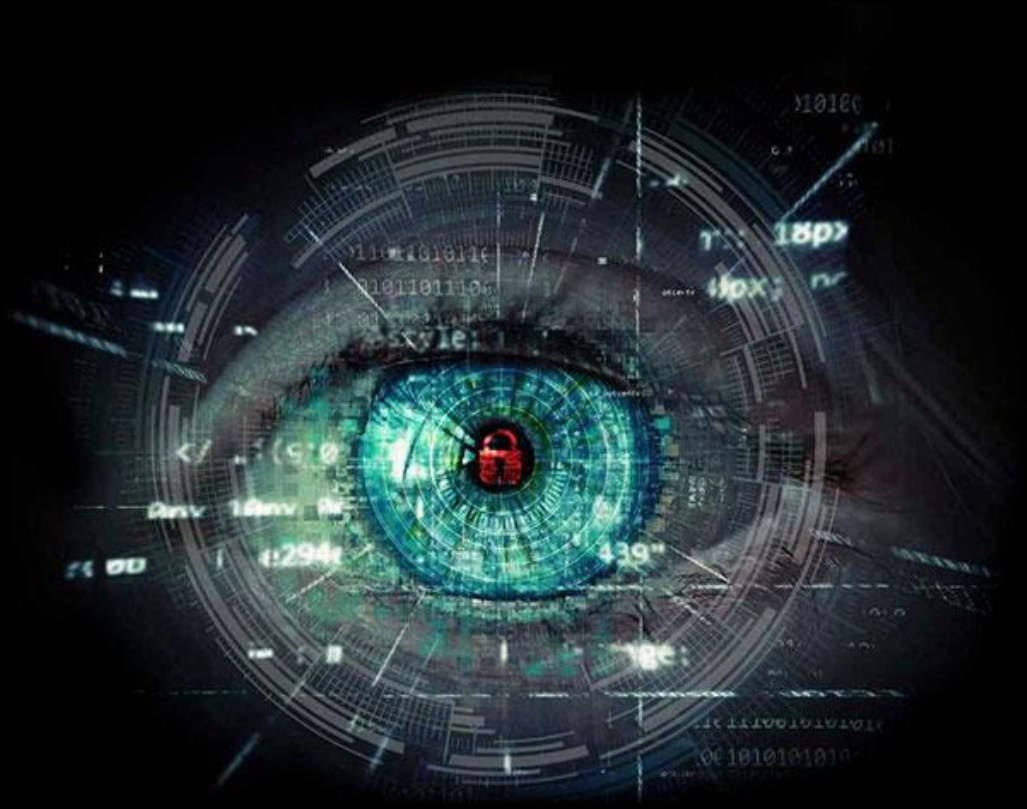
How to manage Human Factor effect on ASMIS?



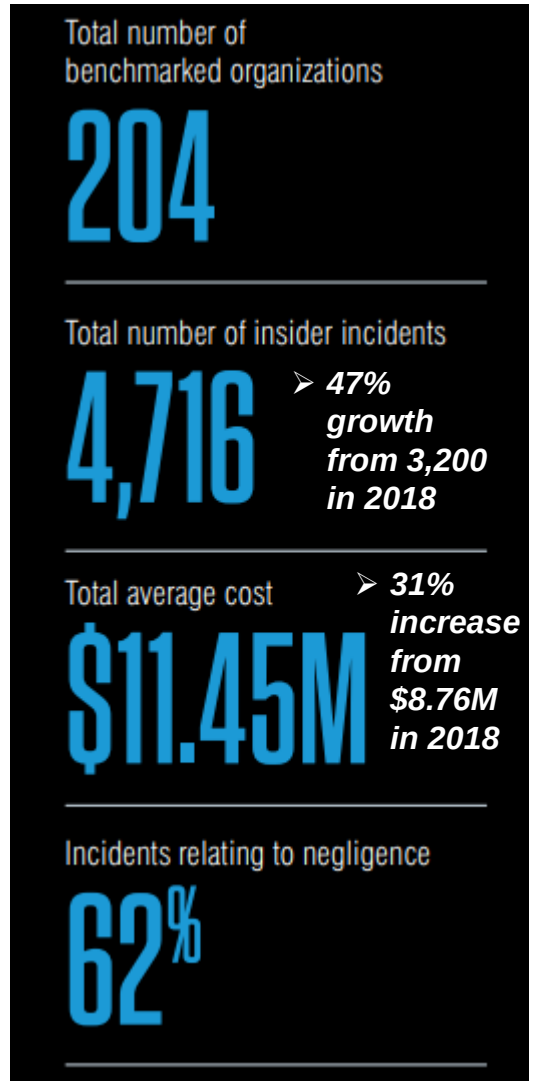
Human Factor

- Ponemon Institute
  2020 global insider threat study

- What is Human Factor ?

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 (CIA) of ASMIS and data

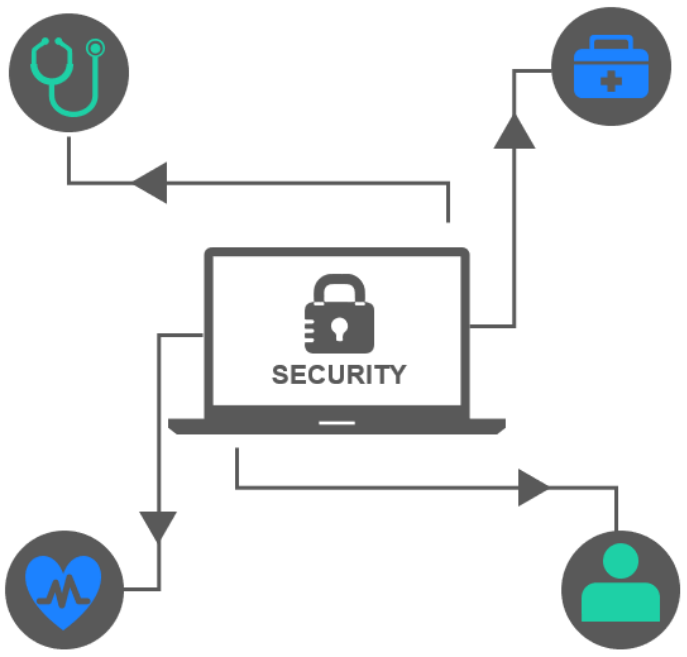
(CERT, 2013)



BUT, is this the fault of our users? No, it is not

(Ponemon Institute, 2020)

Users -> unintentional insider threat without malicious intent ?



01 IMPACT from low user readiness

02 INFLUENTIAL risk tolerance/behaviour

03 FALL BACK on cognitive biases in decision making

So, what solutions can we consider to manage human factors?

01. Impact of low user readiness caused by

work pressures from business process and operational environment settings

Examples?

(Jon, 2017)

How to overcome?

Understanding what cause adverse impacts on employee behaviour. Why users bend or break the rules to get their work done?

This help to clarify any unintended effects on employee morel or employee performance and take actions to mitigate such.

This can be done through;

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

(Vishwanath et al., 2011)

02. Influential risk tolerance and behaviour based on

psychosocial, sociocultural factors

Examples?

(Bank of America. n.d.; Chiu, 2020)

How to overcome?

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

This can be done through;

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

(Shappie et al. 2019)

03. Fall back on cognitive biases in decision making due to
security and compliance fatigue

Examples ?

(Jon, 2017)

How to overcome?

Avoid overloaded information and compliances and security being too complex and/or effortful.

This can be done through;

- ✓ Utilising effective user-system interface designs – single sign-on, multi-factor authentication, password manager
- ✓ Crafting effective security awareness messages
- ✓ Never issue security guidance that is impossible to follow or are not effective

(CERT, 2013; NIST. 2016)

> “Never give an order that cannot be obeyed”
>
> General MacArthur (CERT, 2013)

We need employees who are loyal and engaged to succeed socio-technical security systems !

(NCSC, 2017)

People are not the ‘Weakest Link’

THANK YOU

Mitigating Human Factor effect on ASMIS

Reference

Bank of America (n.d.) *Cyber security during coronavirus: Protect yourself online*. Available from: https://bettermoneyhabits.bankofamerica.com/en/privacy-security/coronavirus-phishing-scams [Accessed 19 September 2021].

Chiu, T. (August 10, 2010) New Study Finds Security Teams Increasingly Stressed. *Security Boulevard*. Available from: https://securityboulevard.com/2020/08/new-study-finds-security-teams-increasingly-stressed/ [Accessed 19 September 2021].

Insider Threat Team, CERT (2013) *Unintentional Insider Threats: A Foundational Study.* Available from: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf [Accessed 25 August 2021].

Jon, L. (March14, 2017) People: the unsung heroes of cyber security. *National Cyber Security Centre*. Available from: https://www.ncsc.gov.uk/blog-post/people-unsung-heroes-cyber-security [Accessed 19 September 2021].

NCSC (2017) *People: The Strongest Link*. Available from: https://www.ncsc.gov.uk/speech/people--the-strongest-link [Accessed 9 September 2021].

NIST (2016) *'Security Fatigue' Can Cause Computer Users to Feel Hopeless and Act Recklessly, New Study Suggests*. Available from: https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly [Accessed 28 August 2021].

Ponemon Institute (2020) *2020 Cost of Insider Threats*. Available from: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-the-cost-of-insider-threats-ponemon-report.pdf [Accessed 25 August 2021].

Shappie, A., Dawson, C. & Debb, S. (2019). Personality as a Predictor of Cybersecurity Behavior. *Psychology of Popular Media Culture*. 9 (4). DOI: 10.1037/ppm0000247.

Sheng, S., Holbrook, M, Kumaraguru, P., Cranor, L. & Downs, J. (2010) Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions, *28th ACM Conference on Human Factors in Computing Systems*, Atlanta, GA, USA, 10-15 April. DOI: DOI:10.1145/1753326.1753383

Vishwanath, A., Herath, T., Chen, R., Wang, J. & Rao, R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*. 51: 576-586. DOI: 10.1016/j.dss.2011.03.002