Seminar session 4: The Human Factor – Developing a Cyber Security Risk Communication Strategy

Why do we care about risk?

“Understanding the risk of disasters and any other serious events is crucial when we need to design effective infrastructure, emergency response planning and developing policies.” (Wheatley et al., 2016)

What’s that got to do with cyber security?

In the 2010 national security strategy cyber attacks were designated as a tier one threat to the uk and since then the importance of protecting the nation’s cyberspace has grown dramatically in the wake of serious cyber incidents and is reflected in the 2016 National cyber Security strategy.

- HM Government (2010) The National Security Strategy: A strong Britain in an Age of Uncertainty. London.
- HM Government (2016a) National Cyber Security Strategy 2016 to 2021.

What is risk?

Definition:

Noun:

A situation involving exposure to danger

Verb:

Expose (someone or something valued) to danger, harm or loss

Impact of risk:

Risk management ISO 31000 (International Standards Organisation, 2018, p.1), it takes a more balanced viewpoint stating:

- “Risk is the effect of uncertainty on objectives. An effect is a deviation from the expected. It can be positive, negative or both, and can address, crate or result in opportunities and threats.”

NCSC (2016) define risk as:

“Risk is the impact of uncertainty on people or organisations. Risks can emerge from any type of ucertainty, including those related to finance, health and safety, and security.”

Vulnerability, threat and risk:

- Threat – This is similar to a hazard, through hazards are natural events and threats are manufactured.
- Vulnerability – A weakness which can be exploited by a threat to deliver an impact.
- Risk – The effect of uncertainty on the desired outcome (can be positive or negative)

Types of risk:

- Strategic
- Tactical
- Operational

Strategic risk:

- Enterprise or organizational risk issues that should be addressed by higher levels of management.

Tactical risk:

- Tactical risk is the chance of lost due to changes in the business conditions on a real time basis. Difference to strategic is the real time conditions.

Operational risk:

- Day-to-day risks that an organization encounters during its operation

Threat actors:

- People
- Machinery
- Competitors

Cyber Risk:

- Different to other types of risk because it is constant and evolving

Two types:

1. Cyber risks of day life
2. Extreme cyber risks

Security risks to digital services, computers, networks, connected technologies or information (NCSC, 2016).

Why is cyber risk so complex?

- Systemic
- Path dependent
- Context sensitive
- Emergent
- Episodic

Process:

1. Characterise system
2. Identify threats
3. Determine inherent risk and impact
4. Analyze the control environment
5. Determine a likelihood rating
6. Calculate a risk rating

Risk Identification:

Quantitative vs. Qualitative:

Risk = Threat * Vulnerability * impact (Jones & Ashenden, 2005)

Cyber Risk Assessment:

Rankings (e.g. numerical or via matrix)

Managing Risk:

- Avoid the risk
- Accept it
- Mitigate it
- Transfer it

Risk Appetite:

Risk appetite can be defined as ‘the amount and type of risk that an organisation is willing to take in order to meet their strategic objectives. Organisations will have different risk appetites depending on their sector, culture and objectives. A range of appetites exist for different risks and these may change over time (Institute of Risk Managemen).

Social Dimensions:

- Process
- Technology
- Human behaviour