Cyber Threat - What's the Risk

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **1 Gün**

Overview

This is a two hour work shop focused on Cyber threats and the associated risks that we all face within our organisations.

It covers:

- What is a threat?
- Threats cannot be considered in isolation
- Threats
- Risk management
- Risk is evaluated against risk appetite
- How do attacks happen?
- Detection & Management
- Cyber and the law

Prerequisites

There are no prerequisites for this course.

What You Will Learn

- What is a threat?
- Threats cannot be considered in isolation
- Threats
- Risk management
- Risk is evaluated against risk appetite
- How do attacks happen?
- Detection & Management
- Cyber and the law

Outline

What is a threat?

- Defining the threat.
- Are all threats cyber?
- Can non-cyber threats become cyber threats?

Threats cannot be considered in isolation. Consider:

- If there is no impact is something really a threat?
- If there is no vulnerability to exploit, is something a threat?
- If there is no probability of a threat exploiting a vulnerability is it a realistic threat?
- Addressing threats rather than risk means unnecessary cost and security. Principle of PACE – proportionate, appropriate, cost effective with regard to controls to manage the risk. Too much security without understanding the threat level, threats, vulnerabilities and impact can result in poor compliance.

Threats

- Threat sources/actors/influencers.
- Cyber enabled vs cyber dependent (hackers vs malware)

- Are cyber threats the biggest threat to an organisation?

Snowden

- If security is done right staff are the biggest asset and frontline.

Risk management

- Risk is the likelihood that a threat will exploit a vulnerability to create an impact.
- How often do we make risk based decisions? Daily and often subconsciously such as crossing a road. Do we cross where we are or walk 100m down the road to a crossing?
- You have to assess the impact of what information is valuable to you. Losing bank details has high impact so you want to protect that from threats. A shopping list is not likely something you would want to apply high levels of protection to.
- Threat assessment – needs to be realistic. Can be non-malicious when considering threats such as environment. Lack of power, failure of generators can be threats to a system. Lack of backup/DR plan is a vulnerability. Cyber threats tend to be malicious. Assessment should consider motivation, capability, priority e.g Anonymous attacks on HMG.
- Vulnerability assessment – where can threats attack? What is lacking? What is not being done e.g. patching? Monitoring? Auditing? Are policies enforced? Are policies accessible? Cyber tends to be about technical controls in most peoples minds but it also requires appropriate personnel, physical, procedural controls in place too e.g. RBAC policy. Ensuring identification, authentication and authorisation is followed.
- Likelihood – hard to assess but needs to be done. Is often judgemental – two different people will come out with different answers using the same method. Security people tend to be very risk averse – business isn't so risk averse. Principles of information security is that security objectives should line up to the business. Security should be enabling not disabling otherwise why run the system?

Risk is evaluated against risk appetite and a choice made to do 1 of 4 things:

1. Avoid/terminate
2. Share/transfer
3. Reduce/modify/mitigate/treat
4. Accept

- We all do this in some way in our lives – ask for examples such as Mobile phone apps and increasing permissions. Recent example in China where malware writers were bribing app developers to include malware in white listed code. Do we avoid (uninstall), transfer (switch to a different app), reduce (harden the app, use security software) or just accept the risk? Most people accept – convenience overrides security.
- Risk approaches acknowledge you cannot manage threats. You can reduce vulnerabilities (but not zero days) and the impact of a threat.

How do attacks happen?

- Staff can be threats or vulnerabilities e.g. exploited by social engineering, bring in USB sticks or expose our business via a smart phone app

Detection & Management:

- Incident management vs forensics. Managing and stopping an incident vs evidence collection may be conflicting objectives. Depends on the threat and likelihood of securing conviction.
- Vulnerability/pen testing. SQL injection attacks are a well known vector yet they still happen – Panama papers is another example of such an attack How difficult is it to pen test for this? How difficult is it to require data validation on input to avoid this? Good testing and good coding would avoid a lot of these attacks.

Legalities:

- Jurisdictional issues – threats in some countries are virtually immune from prosecution.
- Evidence collection has to be legally admissible.
- Any personal data collected as evidence has to comply with S55 of the DPA.
- Interception of electronic communications is within the LBPRs and ICOs Employment code of practice.