Seminar 6 – Data Breach case study

- The course is stated mostly as a group work, so it is all about the group dynamics, how is the group work going, what are the challenges that are encountered and how we resolve them.
- The whole point of the course was about collaborative discussion.
- Recommendations of using an action plan.
- Collaborative discussions were good.

- Exercise – Data Security Breach Cases
- Assessment 2
- Core elements of your e-Portfolio
- Discussion of the key things to think about when preparing and submitting your completed work
- Q&A

Assessment 2:

- Group dynamics is important
- Impossible to put every assumption into the assessment 2. Make own assumptions and decisions.
- Use of threat and risk models like STRIDE & PASTA
- Explanation why the used methodologies is the right one in the specific case
- Example: Nmap is used for sniffing and spoofing methodologies
- Security justifications for accommodations should be mentioned under the business impact of the company we are facing.

Question: Should the report look more as a table format?

- ➔ The second aspect (summarizing the findings) should be in a graphical/table format. Results could be categorized.

Seminar Exercise:

Feedback own group: - Good presentation and excellent analysis.

Group 3:

- Case study MyFittnespal
- Under Armour MyFitnessPla became aware that on 1 February of this 2018 and unauthorized party acquired data associated with MyFitnessPal user accounts.
- Shares dropped 3,8 %

- First no attacker could be determined, in 2019 Dream Market cyber-souk located in the Tor network a source request on HIBP which attributed the data to an e-mail address. But it is still unclear who is the attacker.
- Database sold 2019 for 20.000$ in bitcoin
- The security was able to protect birthdays, location and credit card details from being exposed
- Encryption: Bcrypt → IIP and credit card details were encrypt an so it was much more robust for disclosure
- Bcrypt: More robust but slow with layers of defence to make the progress difficult to reverse.
- SHA-1: Flaws and discredited but fast withfew resources needed and simpler for developers.
- Was the Business Continuity plan instigated: Yes, however UA Kept the data compartmentalised that allowed to keep data seperarted from other types of data such as payment information.
- UA said their plan was effective due to relationships, preparedness and practive (regular cyber incident response test)
- No decision notice on ICO site.
- User Recommendation: change password, don't click links on e-mails
- Ethically, they felt their response was a reflection of the company's values and put the user first thought the process with almost a direct line to their incident response room
- Health mobile apps are not coverd within HIPAA
- Quick acknowledge in 4 days (30 days are regulated)
- Mitigations:
- → Vet and audit the security protections in place.
- → Asses which elements of the app could raise risk. / Provide a security feature list as guideline for implementation.
- → Review the Business Continuity Plan with list of actions to implement in a given scenario. / ISO 22301 compliant business continuity plan.
- → Describe the level of security needed with recommendations. / In recovery: Recognition, Explanation, Apology, Compensation
- → Enhanced detection / Token validation for users / Encryption of all data through local database and cache / Multi layered authentication / Secure code development

Next Session: Each team create a 5 min presentation that argues how the future of the internet could looks like (our group: CCN &/or NDN or COAST)

E-Portfolio Basics:

- Excellent way of recording the learning and development of skills
- Collect, reflect on and present computing artefacts and their online learning experiences.
- Enables to represent the entire educational experience in an organised, integrated and progressive manner.

The e-Portfolio demonstrates:

- Understanding of the module content and its application in a wider social and global context.
- Draw connections between the module material and the coursework, to achieve the module learning objectives.
- Ability to undertake self-assessment, reflecting on personal strengths and weaknesses, identifying personal achievements and providing supporting evidence.
- Creativity, computing aptitude and evidence of acquired skills as an Essex Graduate.

E-Portfolio Assessment Requirements:

- All artefacts
- Output of the scanning and analysing tools
- Evaluation of the design document and the executive summary.
- Analysis of the data gathered and contributions to the discussion forums
- Reflections of the individual contributions and the teamwork process.
- A reflection of the Network and Information Security Management process based on the leanings in this module, as well as the experience as a member of a development team.

E-Portfolio Reflective Piece:

- In video or written text.
- Diary style can be used.

Key points to note:

- Reflection: Not just describe the learnings, make sure to reflect upon it and consider its application in your work, personal, study lives.
- Citation and referencing.
- Total word count for the submission is 2500 word (+10% limit)
- Your e-portfolio content should be presented in a structured, logical way.