

Task 1

Search for 2 example security policies for organisations. Compare these in terms of EISP and ISSP frameworks we have considered. Comment on how comprehensive they are. 4/5 Bullet points will suffice.

★ Example security policies (both taken from the SANS Security Policy Templates web page):

- [Acceptable use policy](#) ("defines acceptable use of equipment and computing services, and the appropriate employee security measures to protect the organization's corporate resources and proprietary information");
- [Remote access policy](#) ("defines standards for connecting to the organization's network from any host or network external to the organization").

★ Comparison with EISP and ISSP framework:

- Both of these policies are examples of a modular ISSP, but could be implemented as part a larger EISP document provided that they complied with the organisational mission statement;
- The presence of both of these documents within an organisation would indicate that the organisation is following the recommended approach of utilising a modular policy implementation;
- Both policy templates appear to conform well to the ISSP framework discussed by Whitman and Mattord, outlining a statement of purpose before detailing acceptable and unacceptable use of the system concerned in a clear and concise manner to ensure reader comprehension. Both templates are headlined with a description of the organisation's expectations for system-specific usage;
- Both templates appear to be highly comprehensive, allowing for a great deal of flexibility for organisation-specific customisation. The guidance is detailed and targeted, whilst stipulating who it applies to. They go one step beyond the frameworks discussed by including a section detailing how compliance with the policy will be monitored and regulated, as well as listing other supporting modular ISSP documentation;
- I believe that the flexibility and level of detail that these templates provide could contribute greatly to the development of a comprehensive EISP document.

Task 2

Draft an example ISSP for an organisation based on Framework in Learning Activities Week 3 Part C. At the beginning of the document describe the organisation for which

you are creating the policy and then complete the policy using the framework. This should be short and not over burdensome.

★ Chosen example ISSP: [Email Policy](#) (has been customised to comply with the outline ISSP framework provided and to align with the organisation)

★ Organisation: a local authority in England, providing statutory services to a constituency of approximately 60000 households (hereafter referred to as "LGA")

★ Policy (definitions have been adapted from Whitman and Mattord):

<<Email Usage Policy Wk3TutQ2.docx>>

Task 3

Considering the planning for security and development of security policies that we have considered, why do you think that there are so many information security breaches? See Cybersecurity Breaches 2023. Provide 4 bullet points.

- According to the Verizon 2023 Data Breach Investigations Report, weak and stolen credentials have, over the last 5 years, become the most common entry point for data breaches. According to the Cybersecurity Breaches report, only 70% of businesses and 55% of charities had a policy to enforce strong password use in their organisation, suggesting that approximately 1 in 3 businesses and almost half of charities are not addressing the threat to their organisation due to weak passwords sufficiently;
- The Verizon Data Breach Investigations Report also finds that the exploitation of vulnerabilities is another very common entry point for data breaches. According to the Cybersecurity Breaches report, only 31% of businesses and 22% of charities had a policy to apply software security updates within 14 days. This would imply that over two thirds of businesses and almost 80% of charities are failing to address software vulnerabilities in a timely manner;
- The Verizon Data Breach Investigations Reports mentions one other very common entry point for data breaches: phishing. According to the Cybersecurity Breaches report, approximately 80% of businesses and charities identified phishing as the cause of an attack or breach. Despite this less than 20% of both businesses and charities had provided training to employees in the 12 months prior to the survey being conducted. Furthermore, less than 50% of businesses had agreed processes for phishing emails. The definition that the latter report provides for phishing revolves around staff receiving fraudulent emails or arriving at fraudulent websites. If organisations were to improve their policies surrounding the training of their staff in this area, it could result in a reduction of successful information security breaches via this vector;

- According to the Cybersecurity Breaches report, approximately 30% of all businesses and charities have formal policy or procedures covering cyber security risks. Of the organisations that have those policies, only 45% of businesses and 34% of charities have reviewed those policies within the 6 months prior to the survey being completed. It is likely that this lack of planning and appropriate review procedures can be attributed to organisations placing a lower priority to cyber security matters, as discussed by the report. Unfortunately this lack of prioritisation is highly likely to be providing higher levels of risk, resulting in easy-to-target vulnerabilities for attackers to exploit.