**ePortfolio:** <https://alesteka.github.io/essexPublic/>

**REFLECTIVE PIECE OF WORK**

The six-week module began with an introductory session on security and risk management, where we compared qualitative and quantitative approaches to risk assessment. The module also provided an immense amount of information about contemporary threat modelling approaches, including best practices to tackle, prevent, and mitigate risks faced by digitalized businesses.

The first collaborative discussion introduced us to the Internet of Things as a network of interrelated devices underpinning Industry 4.0. The provided readings helped us to understand the importance of proper risk management, as no company is risk-free. We examined real-world examples from the past, which enabled us to address the impacts and consequences of inappropriate measures taken by companies. Similarly, recent Snowflake data breach incident, compromised at least two major firms as stated by cybercriminals themselves. This incident could be one of the largest data breaches, yet the certainty of actual impacts remain questionable (Burgess, 2024). Another recent incident happened to the users of CrowdStrike software, who faced inconvenient computer outages (Lyngaas, 2024). As we can see, the incidents occur across various businesses, including specialized service providers such as cloud and cybersecurity vendors. Hence, the importance of risk awareness, threat identification, and compliance with best security practices should remain paramount priority in the future as well.

The next exercise focused on the use of STRIDE, MITRE ATT&CK, OWASP Cookbook, and other threat modelling frameworks. These frameworks helped us to apply best possible practices related to threat modelling. Together with Data Flow Diagrams (DFD), we were able to address business-related risks, such as those present in bank’s web systems:  
A diagram of a diagram

Description automatically generated

The DFD diagrams offer visual representation of the information flow, and therefore expose possible risks within a process or a system (Kumar, 2024).

The above literature topics were interesting to study because I had never before focused on understanding risks through well-established guidelines provided by professionals in the risk and security management profession. The frameworks offer extensive and structured guidelines to address potential issues at every stage (before, during, and after) of a system implementation. These stages are also accompanied by well-known standards, such as the General Data Protection Regulation (GDPR), ISO standards, and other cybersecurity frameworks, which were the main points of discussion in the fourth week. In that week, the disaster recovery part of the session was my favorite, because it addressed technically focused topics. It helped us to understand the importance of backing up data, utilizing point-in-time snapshots, virtual disaster recovery solutions, and using disaster recovery as a service.

The final two weeks of the module were the most interesting because we were able to explore the most contemporary approaches of risk management. For example, DevSecOps, as a progression from traditional business processes, enables companies to employ methodologies that include collaboration between multiple stakeholders, addressing security, reliability, and code quality, together with an automated development approach. This agile process underpins efficient and secure system development through continuous integration and development (CI/CD) as a practice to build and deliver small changes to the application while addressing security concerns.

The final seminar paper required us to build a threat modelling application that accepts an attack tree specification with a visual representation of the nodes, including the monetary and probability values entered by a user. This was the part of the module I enjoyed working on the most because we had to utilise Python packages I had never encountered before. Building these kinds of graphical representations requires a different approach, as the underlying code involves significant manipulation of nested dictionaries. I had an amazing chance to enhance my understanding of these, along with utilising yaml files, which have gained immense popularity in recent years due to their simplicity, readability, and flexibility compared to XML and even JSON formats (Odoh, 2023).

Overall, the Information Security module was fairly intense, despite lasting only six weeks. During that period, I gained a different perspective and awareness of the importance of proper risk and security management. The initial weeks focused on theoretical principles, including understanding some of the well-known industry-related compliances. This was followed by a more practical final week, where I really enjoyed working on the code and was able to put my skills to use.

**References:**

Burgess, M. (2024) The Snowflake Attack May Be Turning Into One of the Largest Data Breaches Ever. WIRED. Available from: <https://www.wired.com/story/snowflake-breach-advanced-auto-parts-lendingtree/> [Accessed 19 July 2024]

Kumar, S. (2024) Data Flow diagrams and Data Dictionaries. Scaler Topics. Available from: <https://www.scaler.com/topics/software-engineering/data-flow-diagrams/> [Accessed 19 July 2024]

Lyngaas, S. (2024) What is CrowdStrike, the company linked to the global outage? CNN Business. Available from: <https://edition.cnn.com/2024/07/19/tech/crowdstrike-update-global-outage-explainer/index.html> [Accessed 19 July 2024]

Odoh, S. (2023) YAML: A Flexible Data Serialization Language with Advantages Over JSON and XML. Medium. Available from: <https://medium.com/@contactxanta/yaml-a-flexible-data-serialization-language-with-advantages-over-json-and-xml-3786d840b95a> [Accessed 20 July 2024]