UNIVERSITY OF SOUTHAMPTON
Faculty of Physical Sciences and Engineering

A project progress report submitted for the award of
BSc Computer Science

Supervisor: Professor Nawfal Fadhel
Examiner:

Automatically Generated Cyber Security Compliance Engine

by James D'Alton

30 November 2019

Contents

1 Project Description **1**
1.1 The Problem . . . 1
1.2 The Solution . . . 1

2 Background and Literature Review **3**
2.1 Compliance . . . 3
2.1.1 Definition . . . 3
2.1.2 Cyber essentials use case . . . 3
2.1.3 The State of Compliance in the UK (crime stats) . . . 3
2.1.4 Impact . . . 4
2.1.4.1 Use cases (interpol database (supply chain examples (cyber terrorism))) . . . 4

3 Solving the Problem **5**
3.1 Technologies . . . 5

4 Conclusions **7**

Chapter 1

Project Description

1.1 The Problem

There are hundreds of cyber security compliance standards, and many businesses require their partners to comply with numerous standards. "Unlike cybersecurity alone, cyber supply chain risk management focuses on gaining visibility and control not only over the focal organization but also over its extended enterprise partners, such as Tier 1/Tier 2 suppliers and customers. In addition, while cybersecurity emphasizes purely technical means of control, CSCRM seeks to engage both managerial and human factors engineering in preventing risks from disrupting IT systems operations."(Boyson, S. (2014) Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems, Technovation, 34(7), pp. 342–353.) Keeping track of each companys compliance to a particular standard is a lengthy and potentially expensive task since it can be very difficult to maintain without the use of an external service or consultant. ("Says who?")

Most SMEs will not be able to afford this - due to the time and experience level required, it might not be something a system administrator can do on top of their other responsibilities, and a consultant might be too expensive.("Says who?")

1.2 The Solution

An automatically generated cyber security compliance engine, could provide a low cost, time efficient solution for businesses that need a flexible, customisable way of tracking their partners compliance, or their own compliance, with multiple standards.("Says who?")

The goal of this project is to create a client-server system that will generate and store compliance forms for the end user. The forms will be automatically generated via an

interface on the application by an admin, and accessible by users. This will include the ability to update the forms at a later date. This project is a client-server system only, not an application, and it will deal with cyber security compliance only - no other forms of compliance will be within the scope of this project.

Chapter 2

Background and Literature Review

2.1 Compliance

2.1.1 Definition

(TODO: Definition of Compliance)

2.1.2 Cyber essentials use case

"The Government worked with the Information Assurance for Small and Medium Enterprises (IASME) consortium and the Information Security Forum (ISF) to develop Cyber Essentials, a set of basic technical controls to help organisations protect themselves against common online security threats." (Cyber Essentials Scheme: overview (2014) GOV.UK.)

2.1.3 The State of Compliance in the UK (crime stats)

"We have seen a significant growth in cyber criminality in the form of high-profile ransomware campaigns over the last year. Breaches leaked personal data on a massive scale leaving victims vulnerable to fraud, while lives were put at risk and services damaged by the WannaCry ransomware campaign that affected the NHS and many other organisations worldwide. Tactics are currently shifting as businesses are targeted over individuals..." (Cyber Crime (no date) NCA National Crime Agency.)

2.1.4 Impact

Cyber attacks are financially devastating and disrupting and upsetting to people and businesses. We know that there is significant under-reporting, although the new General Data Protection Regulation is likely to prompt a better picture of scale. Currently the level of sentencing at court is not commensurate with the seriousness of attacks, and this is an area which is ripe for consideration.

2.1.4.1 Use cases (interpol database (supply chain examples (cyber terrorism)))

Chapter 3

Solving the Problem

3.1 Technologies

- React - Swagger - Database - Python - Robot Framework

Chapter 4

Conclusions

It works.