The Defenders: Proposal Version 1

Back to Project Home

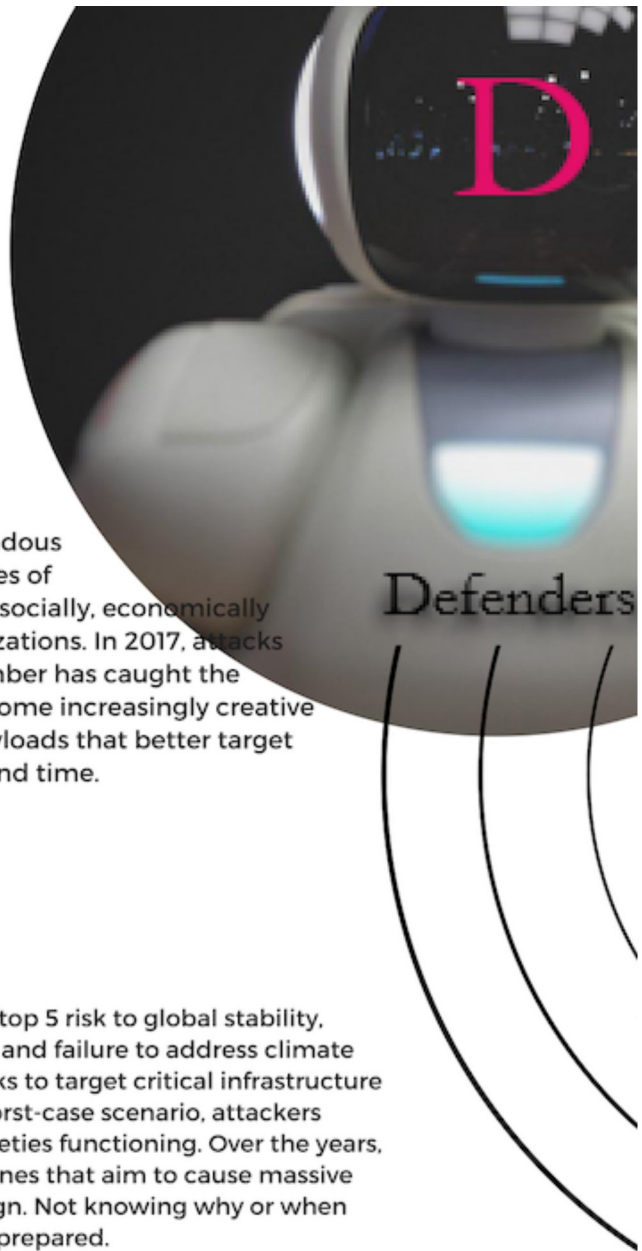| Proposal	Poster	Application	Research Paper

PROJECT
PROPOSAL

INTRODUCTION

The internet has become an indispensable tool in today's business world. While it has fostered a tremendous amount of economic growth, it also introduced a series of profound vulnerabilities with a multitude of impacts: socially, economically and/or invading the privacy of an individual or organizations. In 2017, attacks can total up to $600 billion dollars, this alarming number has caught the world's attention. It is believed that attackers will become increasingly creative with attack methods and increasingly destructive payloads that better target system vulnerabilities, with the luxury of anonymity and time.

MOTIVATION

Cyber-attacks have made its way up to being one of the top 5 risk to global stability, amongst natural disasters, extreme weather, data fraud, and failure to address climate change. "Another growing trend is the use of cyberattacks to target critical infrastructure and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning. Over the years, there has been a shift from profit-motivated attacks to ones that aim to cause massive disruptions, such as the WannaCry ransomware campaign. Not knowing why or when attacks will strike, countries are left unprotected and unprepared.

Hence we would like to use explore various relevant dataset, in hope of uncovering insights that will help us identify trends or correlations towards cyber attacks through the use of appropriate visualization techniques.

GOALS & OBJECTIVES

01 Understand the Type, Source and Impact of Breaches globally

02 Compare the nature and impact of instances of reported breaches between countries

03 Compare breaches between countries over time

04 Evaluate social and economic indicators alongside the number of breaches over time

SELECTED DATASET

1.Breach Level Index
Source : Gemalto, the world leader in digital security.
Purpose : Dataset is designed to provide a simple way to input publicly disclosed information on data breaches and calculate a score indicating breach severity. (https://breachlevelindex.com/)

1. Organization Breached

2. Number of Records Breached

3. Date of Breach:

```
01/01/2013 - 29/06/2018
```

4. Type of Breach

```
-Nuisance (Email, Addresses, Affiliation)
-Account Access (Username, Passwords to websites/ social media)
-Financial Access (Bank Account Credentials)
-Identity Theft ( Information can be used to masquerade someone)
-Existential Data ( Info can be used to threaten business survival)
```

5. Source of Breach:

```
-Lost Device
-Stolen Device
-Malicious Insider
-Malicious Outsider
-State Espionage
```

6. Location: Country

7. Industry:

```
-Technology, Other, Retail, Government, Healthcare, Education
-Financial, Social Media, Hospitality, Entertainment, Insurance
-Non-profit, Industrial, Professional Services
```

8. Risk Score:

```
Log 10 ( Type of Data * Source of Breach * Whether Action was taken)
```

BACKGROUND SURVEY OF RELATED WORKS

01

Go bigThis visualisation effectively use size and toggleable filters to show how severe each data breach is. The interactivity is top notch as each bubble is expanded to show additional information about the singular breach.

https://datafloq.com/read/visualization-worlds-largest-data-breaches-infogra/422

02

Gemalto does yearly reports to study the types, sources and number of reported breaches. However, they have not studied breaches based on the countries where the companies are located at. Hence, our group decided to look into that.

https://breachlevelindex.com

03

The use of proportional symbol map to illustrate the differences in number of breaches is effective. This helps with the visualisation of the distribution of breaches around the world as the distribution of breaches for each country is shown all at one glance.

https://breachlevelindex.com

04

This visualisation is useful for showing the different Human Development Index indicators of various countries shown side by side. It is an aesthetically pleasing form of visualising the distribution in a way that is easy to compare. Moreover, the use of interactive tooltips to show the value of each indicator further enhances its value to this analysis.

http://bl.ocks.org/mthh/7e17b680b35b83b49f1c22a3613bd89f

SKETCHES STORYBOARD
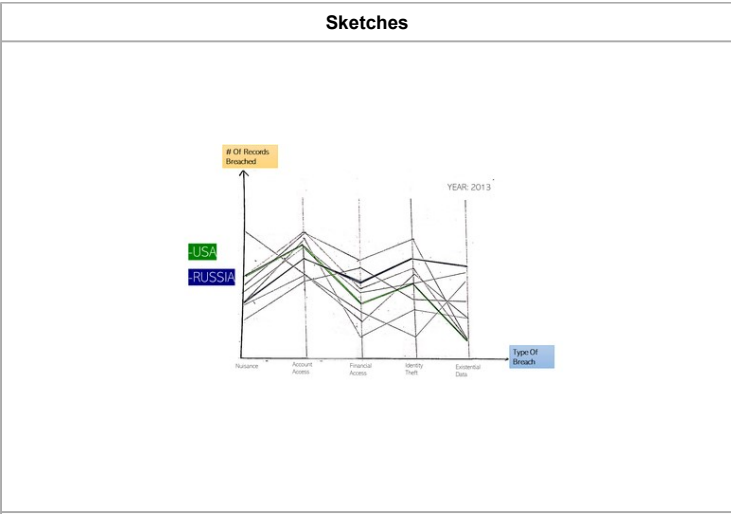
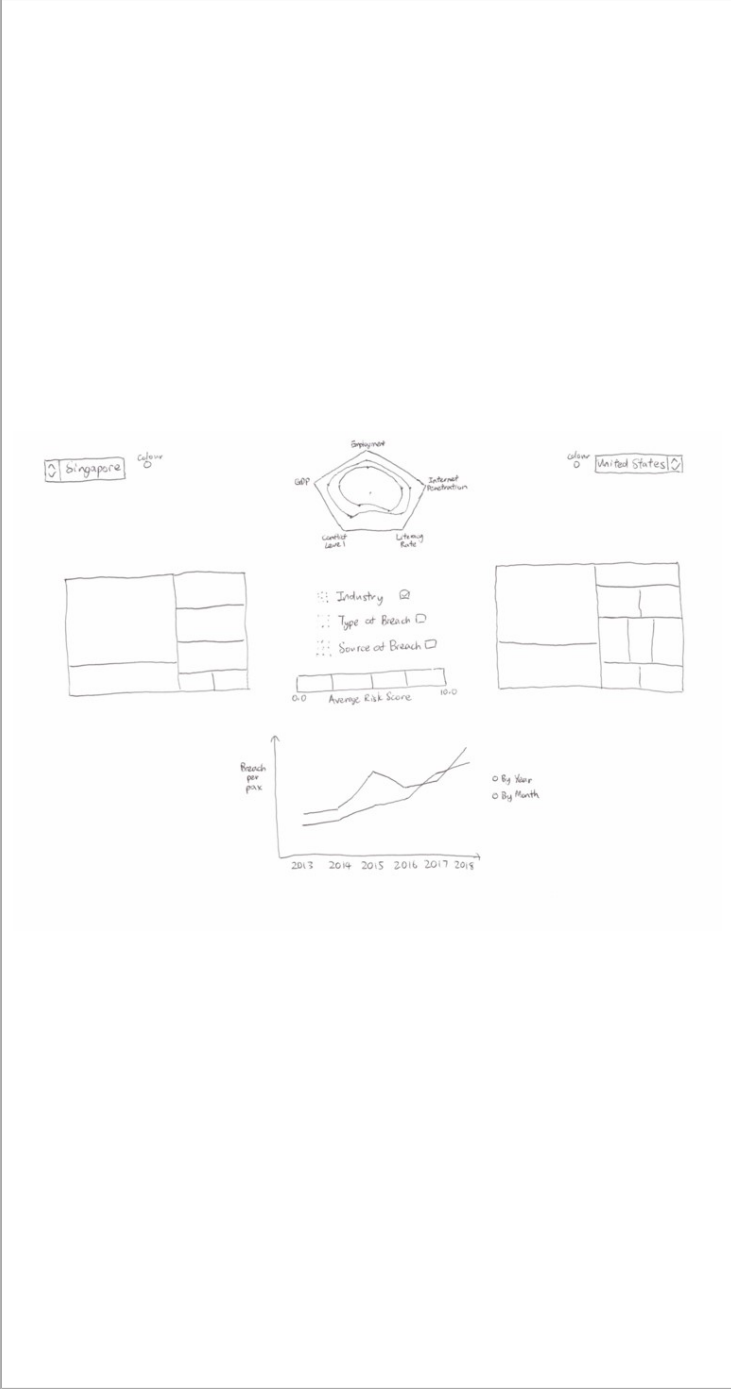| Sketches	How Analyst Can Conduct Analysis
	Breach Overview Consists of an interactive parallel coordinate chart. This visualisation is linked by setting the time period for the data observed through an interactive timeframe. **Parallel Coordinates** The parallel coordinates show the distribution of each feature amongst the different countries. The use of brushing is to highlight the selected country/countries in relation to the rest of the countries. **Dynamic Timeframe** Toggle timeframe according to the period to be visualised.
	Risk Comparison Consists of an interactive line chart, 2 treemaps and a radar chart. These visualisations are linked by checkboxes that detail various features such as type of industry, type of breach and source of breach. Both countries can be toggled and changed to other countries via a dropdown list. **Line Chart** The line chart compares the breaches per pax for 2 countries determined via the dropdown list. The corresponding colors of each country located beside the flag will match the color used for the lines in the line graph Toggle to display trend by year or by month in a cycle plot. Tooltip when hovering the mouse over to show information on: - Breach per pax - Total Breach in Country - Average Risk Score **Treemap** The treemap shows a high level view of our breaches and displaying the breach details at the same time. The different rectangles in the treemap will be colored with different intensities based on risk scores. It allows us to see patterns quickly when our eyes visually aggregate rectangles in the same group. Checkbox to check the different features that we would like to drill down to. Toggle year to display different years' results. Tooltip when hovering the mouse over to show: - Type of Breach - Type of Industry - Source of Breach - Average Risk Score **Radar Chart** The radar chart shows the breakdown of different Human Development Index indicators of various countries shown side by side. This allows us to see the possible different types of countries and see the relation these indicators may have with the breaches the country suffers from Toggle year to display different years' results. Tooltip when hovering the mouse over to show the exact figure of the particular index.

ARCHITECTURE DIAGRAM
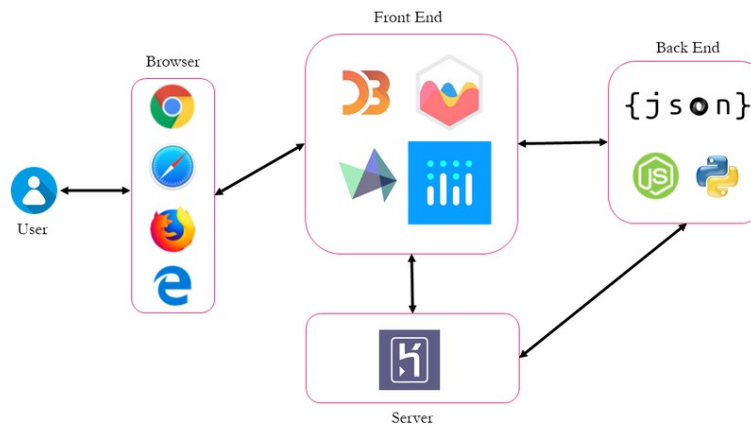
KEY TECHNICAL CHALLENGES

Desired data is incomplete.

Clean data and find more alternatives, till basic requirements are achieved

Steep learning curve of new applications/ language to build project

Diligently attend workshop and do readings

PROJECT TIMELINE

WEEK 10
– Collect + clean data
– Technical exploration
– Data exploration

WEEK 9
– Scoping
– Research
– Story boarding

WEEK 8
– Technical exploration
– Documentations
– Overview of all countries: parallel coordinates

WEEK 7
– Update wiki
– Comparison by country: cycle plot (+ integration)
– Unit testing

WEEK 11
– Research paper
– Comparison by country: tree map
– Unit testing

WEEK 12
– Integration of comparison by country: radar
– Debugging
– Final research paper

WEEK 13
– Design Poster
– Produce content
– Final testing

WEEK 14
– Town-hall preparation
– Finishing touches

REFERENCES

1. https://www.csa.gov.sg/news/press-releases/cyber-threats-in-singapore-grew-in-2017-mirroring-global-trends

2. https://www.todayonline.com/singapore/cyber-threats-singapore-go-phishing-attacks-see-biggest-jump

3. https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

4. http://bl.ocks.org/mthh/7e17b680b35b83b49f1c22a3613bd89f

5. http://www.perceptualedge.com/articles/guests/intro_to_cycle_plots.pdf

Data Sources:

http://hdr.undp.org/en/data#

https://datacatalog.worldbank.org/dataset/harmonized-list-fragility-conflict-and-violence-countries

http://databank.worldbank.org/data/reports.aspx?source=2&series=IT.NET.USER.ZS#

COMMENTS

Feel free to comments, suggestions and feedbacks to help us improve our project!:D

Retrieved from 'https://wiki.smu.edu.sg/18191is428g1/index.php?title=The_Defenders%3A_Proposal_Version_1&oldid=4284'

This page was last modified on 25 November 2018, at 02:02.