# MSc Cybersecurity

## Research Proposal Presentation

Jane Aldridge – 16th October 2023

# Agenda

- Introduction and Project Title
- Significance of the Project
- Contribution to the Discipline, Aims and Objectives
- Research Problem
- Key Literature Related to the Project
- Artefact Description
- Research Methodology, Development Strategy and Research Design
- Risk Assessment
- Ethical Considerations
- Timeline of Proposed Activities
- Conclusion and Next Steps

# Introduction and Project Title

- The proposed project title is:
  - ‘A control framework for preventing and detecting insider threats, carried out by technologists, within banking’
- Banking was selected because the industry is highly regulated and an insider threat incident can result in significant financial loss and also regulatory fines and reputational damage
- The research will also be focused on just individuals performing a technology role, such as programmers, network engineers, sys admins, technology project managers, technology program managers etc..
- In scope individuals would need to be part of a technology division
- The reason that technologists were chosen was that technology is now seen as being at the core of banking. McKinsey (2023) mentions that banks are seen as being technology companies as much as providers of products and services
- There is also research which shows that there is a correlation between function/job role and peoples behaviour (Legg et al, 2015)
- Behaviour will be an important factor, in determining the risk of an insider threat, as well as certain psychological traits
- Engineering insider threats can be accidental or malicious
- Within engineering the majority of threats should be able to be mitigated by controls, such as a change control process for migrating code into production
- This project is significant because it will provide a framework for detecting technology insider threats within a bank.

# Project Significance

Key
- Accidental insider threat
- Malicious insider threat

## Technology Insider Threat Examples

Goldman Sachs Aug 2013 – fined 7 million USD by the Securities and Exchange Commission (SEC) for sending approx. 16,000 erroneous trading orders to various exchanges. Goldman Sachs also suffered 38 million USD in losses.
'Firms that have market access need to have proper controls in place to prevent technological errors from impacting trading'
Andrew Ceresney, head of SEC's enforcement division
(SEC, 2015)

Goldman Sachs June 2009 – a programmer stole proprietary code used for high frequency trading (FBI, 2011).
'the most substantial theft that the bank can remember ever happening to it'
Joseph Facciponti, Assistant US attorney
(Wired, 2015)

Union Bank of Switzerland March 2002 – a computer systems administrator caused more than 3 million USD of damage by installing a 'logic bomb' (U.S. Department of Justice, 2002)
'Although the damage was contained in this case, the potential for catastrophic damage in other cases is always there.' U.S. Attorney Christopher J. Christie

Citibank Dec 2013 – a technologist erased the configuration files on nine production routers, which meant that 90% of Citibanks networks in North America lost connectivity (United States Attorney Office, 2016).

Compass Bank May 2007 – a programmer stole 1 million customer records, which he used to create counterfeit debit cards (Vijayan, 2008)

Capital One March 2019 – a data breach impacted 106 million customers, and Capital One Shares closed at 5.9% down after the breach was announced (Neto et al, 2020). The incident was due to unauthorized access at cloud provider Amazon Web Services (AWS) by an engineer, who used scanning software to identify cloud servers with misconfigured firewalls (Neto et al, 2020)

Banking is a highly regulated industry, with severe consequences for any breaches. So the impact of a successful insider threat, caused by a technologist, can be significant and as a result cost banks millions. Banking is also a global industry, and highly connected, so the global impact can be huge.

# Contribution to the Discipline, Aims & Objectives

This project will enhance research efforts in the domain of insider threat for banking, by providing:

- A practical conceptual framework that describes the main processes and data attributes required, which can be used to design the technical architecture
- The definition of a unique set of attributes which can be used to prevent insider threat
- Proposes a method to reduce false positives which are a challenge in prevention and detection approaches
- Combines both prevention controls and detection in one framework
- A literature review categorization for insider threat for banking
- A mapping of psychological and behavioural characteristics to the actual data attributes which can be used to detect the risk of an insider threat
- During the initial literature review no research could be found which is aimed at insider threat within banking, from a technology role perspective
- This research could be used by Chief Information Security Officers (CISO) as part of their insider threat strategy

# Why is insider threat a Research Problem?

- The number of insider threat incidents keeps increasing, despite the amount of research in this area. A recent survey showed that 27% of all cybercrime incidents were committed by insiders (Homoliak et al, 2019)
- In addition, there has been an increase in accidental insider threats (Homoliak et al, 2019)
- There are multiple challenges in terms of research, such as the problem of transparency into insider threats for organisations amid concerns around reputational damage or regulatory impact
- There is also the problem of false positives and accuracy when using technology to identify insider threat (Gheyas et al, 2016)

# Initial Literature Review: Key Literature

- Using the date range 2015 to 2023, and searching for the keywords 'insider threat', 'literature review', ten articles were identified. However only four were relevant, the others focused on narrow aspects of insider threat, such as the cloud.
- The search 'insider threat', 'technology', 'banking' returned no relevant articles
- For this initial literature review google scholar was used

| No | Paper Reference | Critical Analysis |
|---|---|---|
| 1 | Homoliak et al, 2019 | • The most comprehensive and up to date literature review was by Homoliak et al, 2019.<br>• Other literature reviews were found to be too narrow in their scope and focused on specific aspects of prevention and detection.<br>• One of the benefits of the Homoliak et al (2019) research is that it provides a very holistic framework to detect and prevent insider threat. |
| 2 | Liu et al, 2019 | • Liu et al, 2019 in their survey focus on data sources, such as system calls, unix shell commands, keyboard and mouse dynamics, although HR data is mentioned, it is a narrow subset of HR data, and just refers to employment data, excluding data from overdue mandatory training and cases which have been raised with employee relations.<br>• The major data sources referred to by Liu et al (2019), would be costly to transport over the network, in terms of network traffic. The cost and effort of capturing and analysing this huge amount of data isn't practical and it can be argued does not warrant the investment. |
| 3 | Wang et al, 2015 | • A paper by Wang et al, 2015 focused on detecting insider threat by analysing application logs looking for unauthorized access attempts, however this is too narrow an approach for detection, and would generate a huge number of false positives. |
| 4 | Sun et al, 2018 | • Sun et al (2018) in their paper also refer to the Liu et al (2019) paper, they do make a very relevant point which is that the false positive rate (FPR) of any detection approach can result in a massive cost, which is why this research proposal is to use a broad range of data to reduce the FPR.<br>• The Sun et al (2018) approach focuses on network datasets, webpage data, social media data and program code analysis. My argument here would be that the volume of false positives would not be manageable, and capturing this data would impact the performance of the network, and is not practical. In addition, important datasets are missing such as email datasets. |

# Initial Literature Review: Key Literature

- Homoliak et al (2019) provide an up to date literature review, and propose a new categorization of existing insider threat research:

  ✓ a) Incidents and Datasets

  This category uses past incidents and datasets to evaluate insider threat detection approaches (Homoliak et al, 2019)

  ✓ b) Analysis of Incidents Category

  Models all aspects of insider threat incidents, including psychological and social aspects, with the aim of understanding what motivates an individual. This category is important for prevention and mitigation of an attack (Homoliak et al, 2019)

  c) Simulations Category

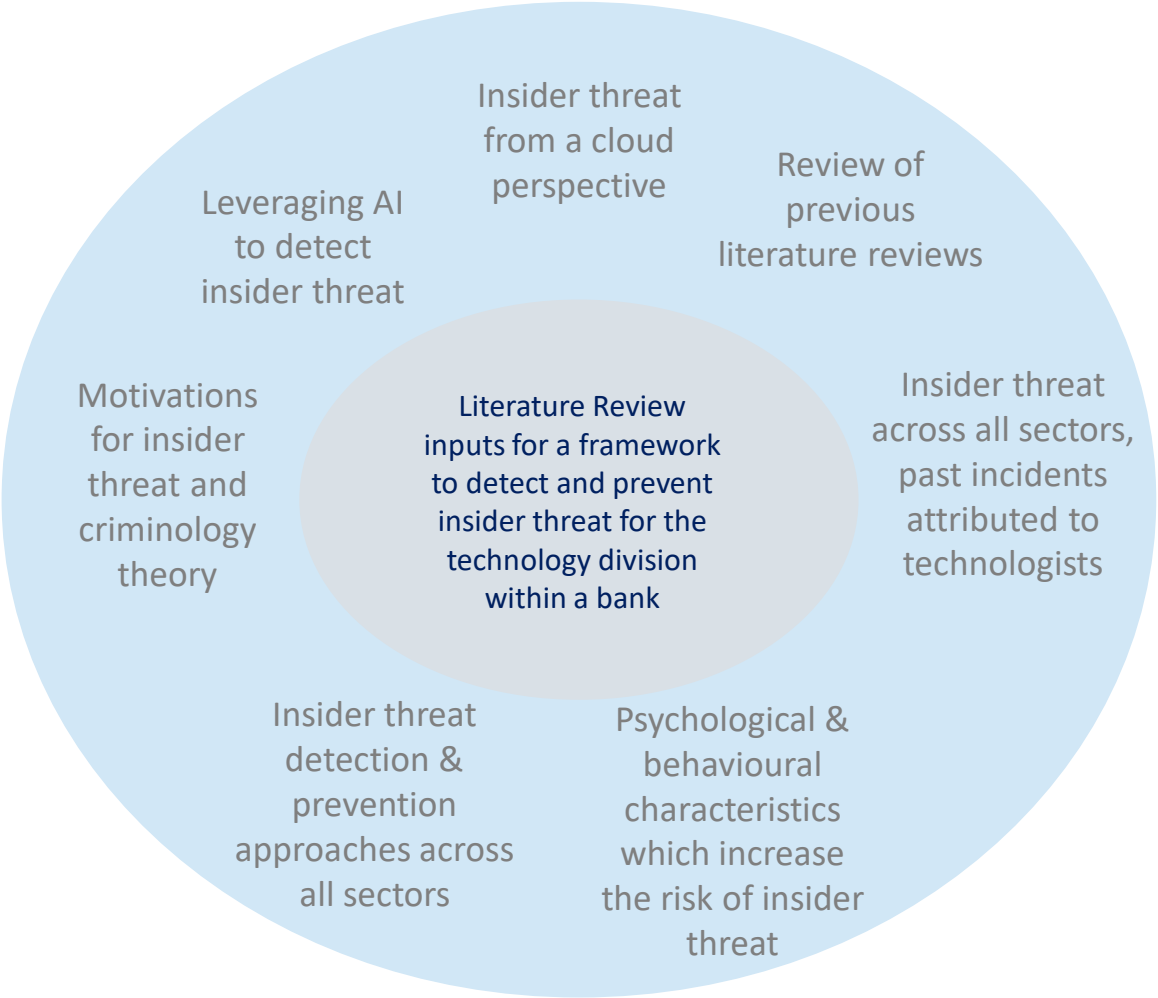
  - This category uses programmed models to simulate insider threat.
  - The simulations category cannot be specific to an individual, and its' objective must be to assess risk at a high level, and so is out of scope for this research, being deemed not practical enough

  ✓ d) Defence Solutions Category

  This involves Insider threat detection, assessment and prevention, and often includes vendor products.

- No paper was found which offers a prevention and detection approach for a bank, for technology employees.

# Literature Review Scope



# Research Project Key Artefacts

A control framework for preventing and detecting insider threats, carried out by technologists, within banking

## Literature Review

- A documented literature review
- The scope will include an analysis of the different literature review topics described on the previous slide

## Dataset & Attribute Description

- A key artefact will be a table of each required dataset, along with the associated attributes and the reason for their inclusion
- This dataset will be required as the data inputs for the framework
- The data analysis will also include an incident analysis of past insider threat cases, which will help to determine the attributes required

## Theoretical Framework

- A conceptual logical framework diagram and description, using inputs from the literature review and also the dataset and attribute analysis
- The scope of the theoretical framework will be based on three main components:
  - Transcription and Indexing
  - Analytics Engine
  - Risk Engine back end

## Risk Engine UX

- A prototype of a UI risk engine, developed using Django, an open source python web framework
- The UX will use dummy test data, based on the theoretical framework
- The aim of the risk engine UX is to demonstrate how the risk of an insider attack will be displayed to the user
- It will also help to visualise the output from the theoretical framework

**Transcription and Indexing**

- Social Media Processing & Indexing
- E-Communications Processing & Indexing

**Analytics Engine**

- Relationship Analysis
- Behaviour Risk Analysis
- Sentiment Analysis

# Research Strategy, Methodology and Design

*Research Methodology*

- When performing an eight month research project on insider threat within banking then the biggest challenge will be accessing data relating to insider threats
- Interviews and surveys are out of scope for this project because banks are reluctant to share information concerning insider threats, due to the reputational and regulatory impacts
- Also, if a bank does agree signing a non disclosure agreement can be time consuming, especially when the project is 8 months
- Taking the above constraints into consideration, the proposed methodology is to use experiments as part of the research methodology
- Experiments would be leveraged to test the theoretical framework by performing a dry run of data obtained through the incident analysis

*Research Design*

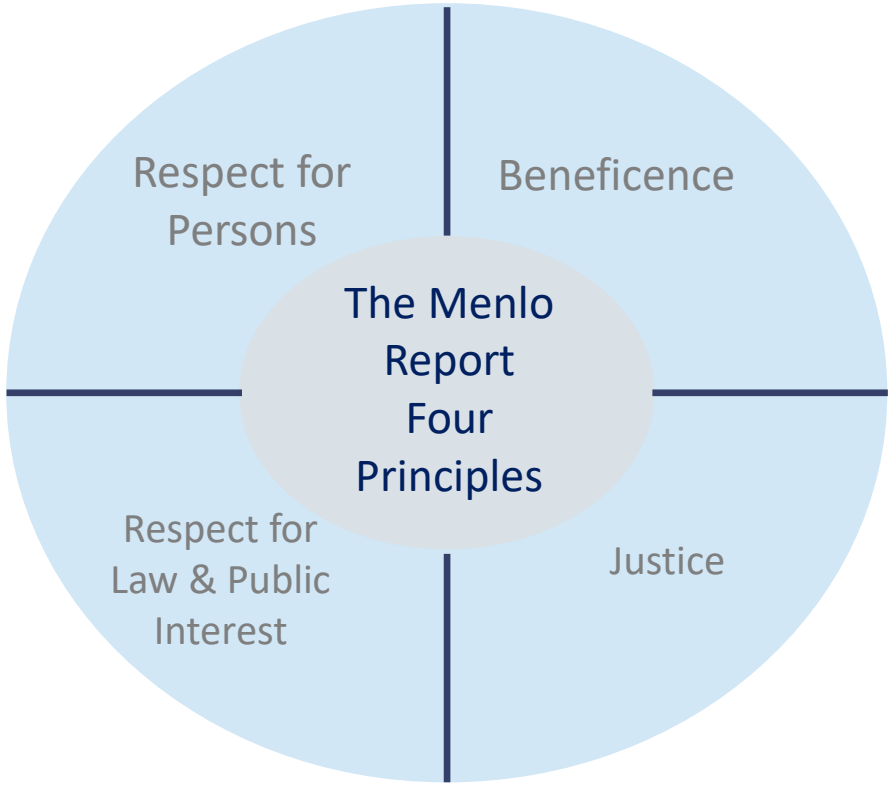
- One of the main exercises as part of this project is to analyse incident data, there are databases of insider threat incident data which can be leveraged
- The three principles of validity, generalizability and reliability need to be applied
- The approach would be to program in python an extraction method which would extract the relevant data, this process would be repeatable because it would be automated
- Then a qualitative approach of analysing the output would aim to determine meaning and conclusions from the data.

# Risk Analysis

| No | Risk Description | Risk Impact Description | Risk Impact | Risk Probability | Risk Mitigation | Overall Risk Rating |
|---|---|---|---|---|---|---|
| 1 | The scope of the project is too large | The project will not be completed in time | High | High | Plan the project timeline at a detailed level and monitor progress closely against the plan. Have a contingency if the project falls behind schedule, which would be to increase the hours spent on the project or to reduce the project scope | High |
| 2 | The development of the UX prototype for the framework requires technical frontend development skills, and a significant learning curve | The UX will not look professional or will take too long to develop and the project will not meet its' deadline | High | Medium | Complete UX training early in the project and find a UX mentor | Medium |
| 3 | One of the challenges of insider threat research is the fact that firms, especially banks, do not wish to share information on past or potential threats, because of the regulatory implications. | The research would not include feedback from banking. | Medium | Medium | Use past incidents for the research as opposed to surveys and interviews. | Medium |
| 4 | Because this framework deals with the human elements of insider threat and also proposes surveillance of individuals, then ethics and also privacy concerns are critical. | Any proposal which impacts an individuals privacy rights and also is not completely ethical, would invalidate the research. | High | Low | The banking industry is regulated, and so any surveillance proposal must fall within the regulatory framework. As an example, there is a regulatory FSA requirement to retain all electronic communications and also to ensure that any query by the regulatory can be supported. Ethical guidelines should be followed. | Medium |
| 5 | The conceptual framework depends on key attributes in order to provide a risk analysis. There needs to be evidence to support the inclusion of these attributes. | If no literature or case studies can be found to support the inclusion of these attributes then this will be a project issue, and the final risk analysis may lose some accuracy | Medium | Low | Include a risk probability, so how likely an insider threat risk for an individual is likely to occur. If datasets or attributes are missing then the risk probability will need to reflect this. | Low |

# Ethical Considerations

- Ethics are an important topic when considering human factors in cybersecurity, such as insider threat, because of the human element and the associated issues such as privacy.
- This project is concerned with the mitigation of insider threats, by using surveillance, which raises many ethical questions.
- The British Computing Society (BCS, 2022) and also the Association for Computing Machinery (ACM, 2023) have documented ethical guidelines which this research project will be adhering to.
- Of particular relevance is the social responsibility to do the right thing, for the wellbeing of others, as stated by the ACM 'computing professionals should consider whether the results of their efforts will be used in socially responsible ways' (ACM, 2023). Section 1a of the BCS guidelines also states that its' members should have a 'due regard for the wellbeing of others'.
- Section 1.3 of the ACM explains that computing professionals should be transparent and provide full disclosure of all system capabilities, limitations and potential problems.
- This means that for this project all findings, risks and limitations of the project should be very transparent and clearly documented.
- The project will also involve legal due-diligence, for any potential privacy or human rights issues or violations.
- To ensure that ethical issues are considered throughout the project, the proposal is to also follow the principles of the Menlo Report (Macnish et al, 2020), as well as the BCS and ACM guidelines.



# Timeline for Research Project (1)

| No | Project Task | Sub-Task | Sub-Task Description | Month 1 | Month 2 | Month 3 | Month 4 | Month 5 | Month 6 | Month 7 | Month 8 (Contingency) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Literature Review (LR) | 1.1 Detection and prevention | LR for insider threat for detection and prevention approaches across all sectors | | | | | | | | |
| | | 1.2 Psychological & Behavioural analysis | LR for psychological and behavioural characteristics which increase the risk of insider threat | | | | | | | | |
| | | 1.3 Criminal Theory Motivations | LR for motivations for insider threat and criminal theory | | | | | | | | |
| | | 1.4 Technology insider threat | LR for insider threat incidents carried out by technologists | | | | | | | | |
| | | 1.5 Technology preventative controls | LR for technology preventative controls | | | | | | | | |
| | | 1.6 Cloud | LR for insider threat from a cloud perspective | | | | | | | | |
| | | 1.7 AI | LR for leveraging AI to detect insider threat | | | | | | | | |
| 2 | Dataset & Attribute Analysis | 2.1 Dataset & Attribute Analysis | Define the datasets and data attributes based on the LR | | | | | | | | |
| 3 | Transcription & Indexing approach | 3.1 Social Media | Define the approach for processing and indexing social media feeds | | | | | | | | |
| | | 3.2 E-communications | Define the approach for processing and indexing e-communications data | | | | | | | | |

# Timeline for Research Project (2)

| No | Project Task | Sub-Task | Sub-Task Description | Month 1 | Month 2 | Month 3 | Month 4 | Month 5 | Month 6 | Month 7 | Month 8 (Contingency) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | Analytics Engine | 4.1 Relationship Analysis | Define the approach for analysing relationship data | | | | | | | | |
| | | 4.2 Behavioural risk analysis | Define the approach for analysis of behavioural data | | | | | | | | |
| | | 4.3 Sentiment analysis | Define the approach for sentiment analysis | | | | | | | | |
| 5 | Risk engine | 5.1 Risk engine back end | Define the back end processing | | | | | | | | |
| | | 5.2 Design the prototype UI | Design the prototype | | | | | | | | |
| | | 5.3 Develop the prototype | Development | | | | | | | | |
| | | 5.4 Test the prototype | Testing, including creation of dummy data | | | | | | | | |
| 6 | Training | 6.1 Django training | Structured training for Django | | | | | | | | |
| 7 | Project final-write-up | 7.1 Write-up | Complete all documentation and also proof reading | | | | | | | | |

# Conclusion and Next Steps

- Insider threat is an important research topic because statistics show that insider threats are still increasing (Homoliak et al, 2019)
- There are also many research challenges, such as the number of false positives generated when trying to detect insider threat
- This research will add to the knowledge in this area by defining a broader set of attributes and also by proposing a solution to the false positive challenge, as well as presenting a front to back holistic framework
- The research is focused on banking because of the regulatory and financial impact of an incident
- Ethics are an important consideration because of the human aspects involved

# References


Legg, P,. Buckley, O,. Goldsmith, M,. Creese, S,. (2015) *Automated Insider Threat Detection System Using User and Role-based Profile Assessment.* IEEE Systems Journal.

McKinsey (2023) Unlocking the Banking Technology Workforce. Available from:
https://www.mckinsey.com/industries/financial-services/our-insights/unlocking-the-banking-technology-workforce
[Accessed 11th October 2023]

Association for Computing Machinery (N.D.). ACM Code of Ethics and Professional Conduct. Available from: **https://www.acm.org/code-of-ethics**
[Accessed 1st October 2023]

British Computer Society (2022). BCS Code of Conduct. Available from: **https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/**
[Accessed 1st October 2023]

Vanclay, F., Baines, J., Taylor C. (2013) Principles for ethical research involving humans: ethical professional practice in impact assessment Part I. Impact Assessment and Project Appraisal 31(4): 243-253.

SEC,. (2015) SEC Charges Goldman Sachs with Violating Market Access Rule. Available from:
https://www.sec.gov/news/press-release/2015-133
[Accessed 11th October 2023]

FBI,. (2011) Former Goldman Sachs Computer Programmer Sentenced in Manhattan Federal Court to 97 months in prison for stealing firm's trade secrets. Available from:
https://archives.fbi.gov/archives/newyork/press-releases/2011/former-goldman-sachs-computer-programmer-sentenced-in-manhattan-federal-court-to-97-months-in-prison-for-stealing-firm2019s-trade-secrets
[Accessed 11th October 2023]

Wired,. (2015) Programmer convicted bizarre goldman sachs case again
https://www.wired.com/2015/05/programmer-convicted-bizarre-goldman-sachs-caseagain/
[Accessed 11th October 2023]

US department of Justice,. (2002) Disgruntled UBS Painewebber Employee Charged. Available from:
https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/duronioIndict.htm, https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/duronioIndict.htm, US department of justice, 2002, https://www.justice.gov/usao-ndtx/pr/former-citibank-employee-sentenced-21-months-federal-prison-causing-intentional-damage, July 2016,
[Accessed 11th October 2023]

# References (2)


Sun, N,. Zhang,. Rimba, P,. Gao, S,. Zhang, K,. Xiang, Y. (2018) *Data Driven Cybersecurity Incident Prediction: A Survey*. Communications Surveys and Tutorials Vol 21, No 2.

Liu, L,. De Vel, O,. Han, Q,. Gao, S,. Zhang, J,. Xiang, Y. (2018) *Detecting and Preventing Cyber Insider Threats: A Survey.* Communications Surveys and Tutorials. Vol 20, No 2.

Homoliak, I,. Toffalini, F,. Guarnizo, J,. Elovici, Y,. Ochoa, M. (2019) Insight into insiders and IT: A Survey of insider Threat Taxonomies, Analysis, Modelling, and Countermeasures. ACM Computing Surveys, Vol.52, No 2, Article 30.

Gheyas, I,. Abdullah, A,. (2016) *Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis.* Big Data Analytics (2016) 1:6.

Wang, J,. Gupta, M,. Rao, R,. (2015) Insider Threats in Financial Institution. *MIS Quarterly, Vol. 39, No, 1, pp91-112.*

Neto, N,. Madnick, S,. (2020) A case study of the capital one data breach. SSRN electronic journal.