Protecting Personal Investors on UK Investment Platforms from Cyber Threats

Gerard Phillips

Technical Report

RHUL–ISG–2021–2

10 March 2021

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Student Number: 100937313

Gerard Phillips

Protecting Personal Investors on UK Investment Platforms from Cyber Threats

Supervisor: Geraint Price

Submitted as part of the requirements for the award of the
MSc in Information Security
at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature: 

Date: 23 August 2020

Table of Contents

List of Figures

List of Tables

Glossary

Term	Description
API	Application Program Interface
APT	Advanced Persistent Threat
Assets	Financial assets are quite different to infosec assets. Personal assets include cash and cash equivalents, property or land, personal property and Investments, such as annuities, bonds, the cash value of life insurance policies, mutual funds, pensions, retirement plans, stocks. https://www.investopedia.com/terms/a/assetclasses.asp
AUA	Assets Under Administration. Sometimes called Assets Under Management. A measure of the total assets for which a financial institution provides administrative services and charges a fee for doing so [13].
BoE	Bank of England
Brokerage	Typically a company that acts as a "middleman" connecting buyers and sellers of shares in stock markets to make trades.
Carding sites	A carding forum or carding website is an illegal site used to share stolen credit card data, and discuss techniques for obtaining credit card data, validating it and using it for criminal activity [Imperva.com].
CiSP	Cyber Security Information Sharing Partnership
CNI	Critical National Infrastructure
Defined benefits pension scheme	A traditional form of pension where the benefits are typically based on salary and length of service.
Defined contributions pension scheme	A scheme where an individual's pension is based upon how much they can save (as opposed to how long they have worked, for example). Employers may contribute to the pension.
ENISA	European Union Agency for Cybersecurity
FCA	Financial Conduct Authority
Fintech	Financial technology. Used to describe new technology that seeks to improve and automate the delivery and use of financial services [6].
FSS	Financial Services Sector
GDPR	General Data Protection Regulation
IC4TD	Information and Communications Technology for Development Initiative [18].
Investment	There are two main types of platform: "*Direct to Consumer*

Term	Description
Platforms	(D2C) platforms are used by consumers without the help of a financial adviser, while *adviser platforms* are chosen by advisers but are paid for by consumers" [13].
IoT	Internet of Things
ISAs	Individual Savings Accounts. These are government savings schemes which attract tax advantages to encourage saving. There are four types of ISAs. The most common are stocks and shares ISAs and cash ISAs. The remaining two are innovative finance ISA and the lifetime ISA. [https://www.gov.uk/individual-savings-accounts/how-isas-work]
ISMS	Information Security Management System
NCSC	National Cyber Security Centre
NIDs	Network Intrusion Detection systems
NIST	National Institute of Standards and Technology
ONS	Office for National Statistics
Open Banking and Finance	Open banking and finance allows third-party financial service providers "open access to consumer banking, transaction, and other financial data from banks and non-bank financial institutions through the use of application programming interfaces. " https://www.investopedia.com/terms/o/open-banking.asp
Order-Execution	The steps involved from placing a trade to the order being fulfilled.
PIDs	Prevention Intrusion Detection Systems
PII	Personal Identifiable Information
PRA	Prudential Regulation Authority
'Pump and Dump'	A form of securities fraud that involves artificially inflating the price of an owned stockthrough false and misleading positive statements, in order to sell the cheaply purchased stock at a higher price. [Wikipedia]
Robo-Advisor	Digital platforms that provide automated, algorithm-driven financial planning services with little to no human supervision [13].
SAD	Synthesised Attacks Dataset
SIPP	A Self Invested Personal Pension (SIPP) is a means of saving for a pension by investing in stocks and shares. To encourage people to provide for their own pensions It attracts various tax advantages from government.

Term	Description
Stocks and shares	Stocks and shares are forms of ownership in a public company. If you buy a share you own a part of that company. Sometimes called “equity”.
SWIFT	The Society for Worldwide Interbank Financial Telecommunication (SWIFT). It provides a secure network between financial institutions. It is often used for transferring payments between banks for example.
The “UK Regulatory Forum	The five principal organisations that regulates the financial sector in the UK.
TTP	Tactics, techniques and procedures. A method used in the MITRE ATT&CK taxonomy to describe the technical detail of a cyber-attack. (Attack vectors and threat events.)

Executive Summary

Investors in the UK are an important part of the country's economy. Collectively they contribute billions of pounds sterling to the financial services sector, which is part of the country's critical national infrastructure.

Increasing numbers of investors use digital platforms and are at increasing risk of cyber-crime. Yet they are largely overlooked and under-represented in cyber security research which focusses principally on threats to financial institutions. This paper goes some way to redress this imbalance.

It examines existing research then develops a new threat model to identify threats to investors. It populates the model with a synthesised dataset of major cyber-attacks on Financial Service Sector (FSS) institutions. Using the new threat model the data is then analysed, threats are identified and new scenarios to defend against those risks are proposed.

Both existing and possible future threats to investors are identified. Around 12% of all existing incidents in the synthesised dataset target investor settings. The motivation for almost all attacks is theft and they are carried out by organised criminal gangs, mostly working from Eastern Europe. They target personal customer accounts and the principal attack vectors are malware, forms of card fraud and "multiple" vector attacks. However, significant gaps in the data suggest this may be only part of a larger picture.

Several scenarios for future attacks on investors are presented. These include high volume and automated attacks on individual investors on their home networks or devices; targeting innovative hybrid card-based applications, such as the Revolut card; and targeting open banking and finance technologies which share personal finance data across different provider platforms.

The research found there were four significant barriers to understanding the threats to investors. First, existing threat models were designed to examine threats to FSS institutions, not investors. Second, UK-specific data was not available. Third, existing models simply do not conceptualise the idea of an "investor threat landscape"; this significantly limits their relevance in understanding threats to investors. Finally, there are almost no threat-centric scenarios for investors and none (yet found) that detail how to prevent and mitigate identified threats.

This paper meets these challenges by innovating a new threat model; creating a synthesised proxy database; proposing new threat landscapes; and developing new strategic and intermediate threat scenarios designed to protect against threats to investors.

In conclusion, recent fraud cyber-crime statistics suggests that investors may already be victims of cyber criminals. An initial survey of investors is conducted which demonstrates investors have only a partial understanding of cyber security. Investment platforms specifically could do more to support investors to learn to be safer online. Finally it is suggested that the national regulator, the Financial Conduct Authority, might share more data on cyber-attacks with the cyber community to protect both investors and companies in the financial services sector.

Chapter 1: Introduction

This thesis takes as its subject millions of ordinary people in the UK who use investment platforms, or similar financial mechanisms, to invest for their future. This may be as savings, or pensions, or just something to leave to loved ones.

The motivation for the research question came from a perception that much has been published on how financial institutions, such as banks, are to be protected. But there was little in the literature or in cyber security practice that examined the threats to personal investors from cyber-crime.

The research question this paper asks is "What are the principal cyber threats to investors' assets on UK investment platforms and what can be done to prevent or mitigate these threats?"

1.1 Research Objectives

The Preliminary Literature Review set out the objectives of the research. Objectives 1-3 below are background objectives and are addressed in chapters 2 and 3 of this paper. Objectives 4-7 are analytical objectives and are covered here in chapters 4-7. The objectives are:

1) To understand the structure and topography of the financial services sector (FSS) in the UK and of the role of investors and investment platforms within it (Chapter 2);
2) To review the state of cyber-crime in the financial services sector globally and to consider specifically UK data on FSS cyber incidents (Chapter 3);
3) To examine how the criminal ecosystem is evolving and maturing to support cyber-crime and to infer what this might mean for future attacks on investors in the UK (Chapter 3);
4) To develop a framework (a model) to understand the threats arising to investor from FSS cyber-crime (Chapter 4);
5) To assemble available data and to populate a new threat model (Chapter 5);
6) To use the new threat model as a structure to analyse the real-world attacks on investors, financial institutions and on supporting infrastructure services (Chapter 6); and
7) To examine how threats to investors using investment platforms can be prevented and mitigated using threat scenarios (Chapter 7).

1.2 Methodology

The research objectives have been operationalised as follows. A literature review of relevant materials provides the content for Objectives 1, 2 and 3 (covered in chapters 2 and 3).

To understand and evaluate FSS threats this paper uses the information security technique of threat modelling. As original contributions to the research literature it builds on existing research and constructs a specific threat model relevant to

personal investors in the financial services sector (Objective 4, chapter 4). It then surveys and synthesises existing available data to produce a bespoke synthesised attacks dataset (SAD). This is then used to populate the new threat model (Objective 5, chapter 5).

The next steps are to analyse the new dataset using the new threat model; create a new "investor threat landscape"; and then incorporate three distinct threat landscapes into the one model: the investor landscape, the FSS institution landscape and the FSS infrastructure landscape (Objective 6, chapter 6).

New threat scenarios are then proposed specifically for the investor threat landscape. A strategic set of scenarios are developed followed by a case study of an intermediate level scenario. This demonstrates how threats can be prevented or mitigated (Objective 7, chapter 7). Finally, an original survey of UK investors is presented and some implications are discussed. (Objective 7, chapter 7).

Table 1 illustrates how the research objectives align with the methodology and structure of the paper.

Table 1: Mapping Research Objectives to Methodology and Chapter Structure

Research Objective	Methodology	Chapter Structure
1: Structure & topography of FSS	• Literature review	• Chapter 2
2: Cyber-crime across the FSS	• Literature review	• Chapter 3
3: The maturing criminal ecosystem	• Literature review	• Chapter 3
4: Build a framework to understand malicious threats to the Financial Services Sector	• Review literature then construct own threat model	• Chapter 4
5: Assemble available data	• Synthesise data to produce own bespoke attacks dataset	• Chapter 5
6: Analyse threats to investors and investment platforms	• Apply new threat model to synthesised attacks dataset and analyse by threat landscape	• Chapter 6
7: Prevention and mitigation of threats to investors and on platforms	• Develop strategic threat scenarios • Case study of intermediate level threat scenario • Undertake original investor survey	• Chapter 7

Source: [Compiled by Author]

Chapter 2: The UK Financial Services Sector

This chapter briefly explains why the UK Financial Services Sector (UK FSS) is important to the cyber-security of the nation, what it is and how it is regulated by government. This provides a starting point for next understanding who investors are, how they invest using investment platforms and why both are likely to be an increasingly attractive target for cyber criminals.

2.1 The Financial Services Sector as Part of UK Critical National Infrastructure

The EU Council Directive 2008/114/EC defines critical infrastructure as an "Asset, system, or part thereof located in a nation which is essential for the maintenance of vital societal functions, health, safety, security, economic, or social well-being of people, and the disruption of which would have a significant impact in that nation as a result of the failure to maintain those functions [1]."

Financial services, contributing to the economic well-being of the country, are clearly part of the critical national infrastructure of the UK. This is confirmed by its inclusion in the UK National Cyber Security Strategy 2016-2021 [2] and as evidenced by its inclusion in the work of the UK Government's Centre for the Protection of National Infrastructure [3].

The importance of the financial sector to the UK economy is well documented. In summary it generates wealth for the UK, provides jobs and helps the UK compete internationally with other countries. For example, as at July 2019, the financial services sector contributed 6.9% of total UK economic output, which amounted to £132 billion. Internationally, the UK has a trade surplus of £44.4 billion in the financial and insurance activities sector, thus also bringing wealth into the country [4].

The sector also brings the UK influence because of its position as an international financial centre. A 2018 report by "TheCityUK" [5] makes the case: the UK banking sector assets were the largest in Europe; it was the leading global net exporter of financial assets; nearly twice the number of dollars are traded in the UK as the US; more than half as many euros are traded in the UK as in the Eurozone; it has leading specialist competencies in green finance, Islamic finance, maritime business services and infrastructure investment. The UK is also increasingly positioning itself as a leading sector in financial technologies (FinTech) [5].

2.2 How the Financial Services Sector is Structured and Regulated

A useful overview of the structure of the UK FSS is provided by the UK's regulator, the Financial Conduct Authority (the FCA) [6]. They divide the UK financial services industry into seven sectors:

1) Retail banking and payments;
2) Retail lending;

3) General insurance and protection;
4) Pensions savings and retirement income;
5) Retail investments;
6) Investment management; and
7) Wholesale financial markets.

A comprehensive review of each sector can be found in the 2020 FCA annual sector review [6].

Financial regulation in the UK in 2020 involves a number of different organisations each with specific responsibilities and objectives. It is complex [7] and not always transparent where roles start or end. The principal bodies are referred to collectively as the "UK Regulatory Forum" [8] and comprise five organisations: the Financial Conduct Authority (FCA); the Prudential Regulation Authority (PRA); the Bank of England; the Payment Systems Regulator; and the Competition and Markets Authority.

The most important regulator for our purposes is the FCA. This is the principal body that sets controls for financial institutions and polices the regulations. The strategic objective of the FCA is to ensure "that financial markets work well by:

1) Providing an appropriate degree of protection for consumers;
2) Protecting and enhancing the integrity of the UK financial system; and
3) Promoting effective competition [9]."

The interest in this paper in the FCA is principally in how it operates in delivering the second of these responsibilities, protecting and enhancing the integrity of the UK financial system. Within this, the key operational area of interest is how it supports financial institutions' resilience to cyber-attacks.

2.3 Investors Make Attractive Targets

"Investors", broadly, are persons who use investment platforms, banks or other developing hybrid services (e.g. the Revolut card [10]) to accumulate and grow investments, savings or pensions. For example, they might trade in stocks or shares[1], save using financial products such as Individual Savings Accounts (ISAs)[2], or build a personal pension through defined contributions pension schemes[3] or SIPPs[4].

[1] Stocks and shares are forms of ownership in a public company. If you buy a share you own a part of that company.

[2] ISAs are individual savings accounts. These are government savings schemes which attract tax advantages to encourage saving.

[3] A defined benefit pension scheme is one where an individual's pension is based upon how much they can save (as opposed to how long they have worked, for example).

[4] A Self Invested Personal Pension (SIPP) is a means of saving for a pension by investing in stocks and shares. To encourage people to provide for their own pensions It attracts various tax advantages from government.

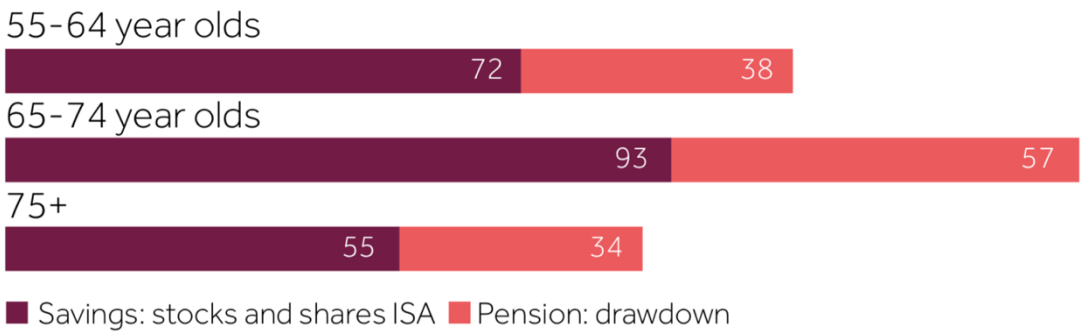
Within the financial sector overall personal investors generally are more active in the *pensions savings and retirement income* and *investment management* sectors. There are several million people such investors, each of whom could be a target for cyber criminals.

The following figures give an indication of the numbers of people and sums of money involved: to take first pensions, then stocks and shares.

For pensions, 35 million consumers hold around £2.8 trillion assets under management [11]. Major changes in the pensions sector over the past few decades have pushed the onus for saving for retirement generally from employer to employee [6] and this trend is continuing. For example, within the pensions sector over 800,000 people held Self Invested Personal Pensions (SIPPs) in 2020 and the value of these in 2018 was £2.4 bn [11].

For stocks and shares, 13.5% of UK shares are owned by UK individuals [12] while within share ownership, 2.2 million people in the UK were subscribed to a stocks & shares ISA account in 2019 [11]. Figure 1 illustrates, as at 2017, estimates of assets held by persons aged over 55; the values given are in billions sterling.

Figure 1: Estimate of Assets (£bn) Held by Over 55s



Source: [6]

Demographic, regulatory and technical changes in the UK [6] suggests that the numbers of investors are growing and will continue to grow, as will the sums they invest.

2.4 Investment Platforms Make Attractive Targets

Investment Platforms are typically the mechanisms many people use to manage their investments in the stock markets. The FCA defines investment platforms thus: "Investment platforms arrange, safeguard and administer investments on behalf of consumers and offer them access to retail investment products from a number of different providers. Consumers can use platforms to access information and tools to inform and help them with investment choices and can use them to make transactions, such as buying and selling shares and funds [13]."

Generally a user accesses the platform (e.g. a web page) using a browser (from a desktop / laptop computer) or an app (on a mobile phone or tablet). After authentication and authorisation the user is offered a dashboard with summaries of their investments (e.g., stocks and shares, ISAs, SIPP, cash held etc.), usually along with a suite of research tools. They can then use options on the screen to manage or

trade their assets. Via the platform's interface, they can trade directly on exchanges around the world across a whole suite of assets. (The exact options vary depending on platform.)

Investment platforms are growing in popularity as a consumer mechanism of choice for making investments [13]. More people are using investment platforms ("an increase of around 2.2 million customer accounts between 2013 and 2017") [13] and more money is being invested through them ("the investment platform market had doubled since 2013, from £250bn to £500bn assets under administration (AUA)[5]" [13].

Examples of popular investment platforms are given in Table 2 below. They are a mix of old established UK banks (Barclays, Lloyds), UK merchant banks (Close Brothers), European banks (Saxo, IG), traditional insurers (Aviva, Fidelity), traditional investors (Hargreaves Lansdown, TD), new "heavyweight" investors (AJ Bell) and newer "niche" investment platforms (such as e-Toro and Nutmeg, our "digital challengers"). Most are regulated either by the FCA or are European Economic Community authorised, which means that it is a firm that is regulated in another European Economic Area (EEA) country.

Table 2: Popular Investment Platforms Available in the UK

Investment Platform
AJ Bell / YouInvest Dealing Account
Alliance Trust Savings investment platform
Aviva
Barclays SIPP
Barclays Smart Investor investment platform
Bestinvest investment platform
Charles Stanley Direct investment platform review
Close Brothers investment platform
Degiro Share Dealing
e-Toro Free stocks
Fidelity investment platform
Fineco Bank Multi-Currency Trading Account
Halifax Share Dealing Account (subsidiary of Lloyds)
Halifax Share Dealing investment platform (subsidiary of Lloyds)
Hargreaves Lansdown Fund and Share Account
Hargreaves Lansdown investment platform

[5] Assets Under Administration (AUA) is a measure of the total assets for which a financial institution provides administrative services and charges a fee for doing so [14].

Investment Platform
HSBC InvestDirect investment platform
i-web (subsidiary of Lloyds)
IG Share Dealing Account
Interactive Investor investment platform
Interactive Investor Share Dealing Account
Nutmeg
Online Shore
Saxo Markets Share Dealing Account
Selftrade (Now Equiniti) investment platform
TD Direct Investing fund supermarket review
The Share Centre investment platform
Vanguard investment platform
Willis Owen

Source: [15] [16] [17]

There are many investment platforms in the UK holding billions of pounds sterling (and other currencies) [15] [16] [17]. These monies are managed using digital platforms and offer a lucrative target to cyber criminals.

2.5 Chapter Summary

This chapter identifies three important points. First, investors contribute significantly to the "economic well-being" of the financial services sector and as such are part of the UK critical national infrastructure. Defending their interests is a responsibility of both the FCA and the NCSC.

Second, as a class of people there are millions of investors who invest, collectively, billions of pounds in the UK economy. The numbers of both investors and the sums they invest should be expected to increase due to demographic and government regulatory changes (e.g., pensions reform).

Third, improvements in technology are also driving change. Although a recent innovation, digital investment platforms are increasingly becoming established as a principal method of investing. Trading platforms hold billions of pounds of peoples' money. This can be expected to continue to increase.

It can reasonably be concluded from this that both investors and investment platforms, as each grows in both number and value, will increasingly present attractive targets for cyber criminals.

Chapter 3: Cyber Attacks and the Maturing Criminal Market Economy

This chapter does two things; in section 3.1 it reviews available literature and examines cyber-attacks on FSS institutions globally and in the UK. In section 3.2 it explores how criminal groups are supported by a mature criminal ecosystem, it looks at the different types of criminal groups and their capabilities, and it investigates how these are changing.

Bringing both sets of findings together it suggests that an increase in attacks on investors and investment platforms is to be expected. In response to this some mitigations are proposed.

3.1 Cyber attacks on financial sector services

3.1.1 The Expanding Attack Surface

The finance industry, like many others, is part of a global economy and a number of technical factors are driving a growth in the attack surface [18] [19] [20]. There are four continuing global trends. First, there has been an increase in connectivity between financial institutions, the Society for Worldwide Interbank Financial Telecommunication (SWIFT)[6] payments system being one example. Second, new technologies enable an increase in the numbers of clients who were previously excluded from financial services. For example, there are now millions of new customers in emerging markets using global banking services (such as the Information and Communications Technology for Development initiative (ICT4D), in Africa) [18]. Third, there is a continuing increase in the number of online and mobile banking applications and of devices connecting these new clients to banking and other finance networks. Mobile devices in particular are "transforming the landscape" across the world" [18]. Last, a separate but related point, the introduction of millions of new (often vulnerable) Internet of Things (IoT) products [18] and devices in people's homes provides an attack vector for attackers looking to gain initial access to a victim's network.

Evidence that criminals have adapted both their targets and their techniques as the attack surface has changed comes from a study [20] of attacks on banking institutions globally over the past twenty years shows. It shows:

- From the late 1990s the trend was to target credit cards (selling stolen data on carding sites);
- From the mid-2000s attacks were against online banking users (trojans such as ZeuS, SpyEye, Shylock);
- From 2014 onwards attacks were against bank payment and core banking systems (e.g., the 2016 Bangladesh Bank heist, the 2018 CosmosBank in

[6] "The Society for Worldwide Interbank Financial Telecommunication (SWIFT), legally S.W.I.F.T. SCRL, provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardized and reliable environment [21]."

India), and from around 2018, attacks against the interbank networks (Mexico April 2018, Chile, the Redbanc network, January 2019).

- Recently, mobile banking trojans and other forms of mobile malware are now becoming a leading means of consumer bank fraud [18].

A significant further development affecting the UK and Europe is the introduction of open banking and open finance, a Europe-wide initiative that allows sharing of personal financial data (and Personal Identifiable Information (PII)) between different financial institutions. This is important as the more complex any system becomes, the greater a possibility an exploit may be found in its design, configuration or in implementation.

Specific to the UK the FCA [6] have also identified emerging technologies, the maturing use of "big data" and artificial intelligence, and investment in Fintech (financial technologies) as emerging FSS trends. These could further extend the attack surface for criminals.

It needs also be noted that regardless of the introduction of new technologies, the retention and use of legacy technology remains a security vulnerability for some FSS institutions. Lists of known vulnerabilities are typically posted on hacker / white hat websites (such as Exploit Database [22]), as often is the source code for exploiting them.

3.1.2 Attacks on Financial Services in the UK

Reliable and consistent data on attacks on UK FSS institutions has proved difficult to find. There is a requirement on FCA regulated institutions to report incidents to the FCA and they have proved the best source of information. There are three pieces of evidence: i) time series data from 2015-2018, ii) a response to a Freedom of Information request in 2019, and iii) a report from the FCA Cyber Coordination Groups in 2020.

Time series data from the FCA (see Table 3 below) shows that cyber incidents have been increasing across all sectors of the UK financial services between 2015-2018.

Table 3: Cyber Incidents by Financial Services Sector 2015-18.

Sector	2018	2017	2016	2015
General Insurance & Protection	33	7	1	3
Pension Savings & Retirement Income	9			
Retail Banking & Payments	25	1	1	1
Retail Investments	11		1	
Retail Lending	21	4	1	
Wholesale Financial Markets	34	3		
Investment Management	12	10	3	

Source: [23]

Data produced following a Freedom of Information (FoI) request in 2019 covers the period from 2018 to January / May 2019 and is summarised in Table 4.

Table 4: Cyber Incidents Data (FCA 2019 FoI Request)

Root cause	Occurrences Jan-Dec 2018[7]	Occurrences in Jan-May 2019
Hardware and software issues	157	64
Change management	146	53
Third-party failure	174	79
Cyber-attack - Distributed denial of service (DDoS)	10	2
Cyber-attack - Malware	16	5
Cyber-attack - Ransomware	19	0
Cyber-attack - Phishing or other compromise of credentials	48	29
To be confirmed	93	82
Human error	47	24
Process/control failure	45	17
Failure to manage adequate IT capacity	25	4
External factors	17	3
Theft	11	3
Cause unknown	11	5
Total	**819**	**370**

Source: [24]

To accompany publication of this data an Executive Director for the FCA, Megan Butler, gave a speech [25] in London in November 2018 offering further insights. Taking both sources together three themes emerge.

First, the immediate feature to note is that 11% of incidents were cyber-attacks and the attack vectors over both years were principally phishing, malware, ransomware and DDoS. Consumer banks (many of which have digital investment platforms) were a significant target and accounted for nearly 60% of all incidents [25].

Second, the data may hide further attacks. 89% of incidents do not appear to be cyber-attacks; however, 13% of incidents (104 out of 819) were either "cause unknown" or "to be confirmed".

[7] The greater incidents recorded in 2018 was considered due to the introduction of the GDPR that year [24].

Third, the capability of FSS institutions to protect themselves from attack is highly variable. Only 56% of firms had effective asset information controls while around a third of firms did not perform regular cyber assessments. Further "only the largest firms have automated their detection systems to spot potential cyber-attacks" [25] and there was a tendency for firms not to upgrade their IT systems in good time.

Table 5: FCA Cyber Coordination Group (FSS Industry Concerns)

Theme	Topics discussed
Theme 1: Cyber Risk	*The current threat landscape* • The Supply Chain • Social engineering • Ransomware • Malicious insider • Credential stuffing *Emerging & future trends* • DevSecOps (development and security in operations) • Cloud security (in particular, that provided by externally managed services) • Payment systems security
Theme 2: Identity and Access Management (IDaM)	• IDaM governance • Identify and prioritise accounts • Record Keeping • Importance of Privileges • Importance of Passwords • Security Monitoring and Testing
Theme 3: Third Parties and Supply Chain	• Understanding third party suppliers • Establish and maintain control • People, process, technology • Work together to improve
Theme 4: Malicious E-Mails	• Identify, monitor and adapt • Maintain a secure culture • Treat emails addresses as assets

Source: [Compiled by Author from 26]

The third piece of evidence was published in March 2020 [26]. This was a report of FCA "Cyber Coordination Groups" which comprise around 175 UK FSS firms that

meet to share ideas arising from their cyber experiences. This is good quality and more granular intelligence.

Table 5 summarises the key items covered in the report. The principle - and significant - point to pick out is that it supports the evidence from Butler above that FSS institutions are not as robust in their defence against attacks as one might expect.

For example, discussing identity and access management conversation turned to the importance of passwords; when discussing third party and supply chain risks conversation turned to the need to maintain control; the importance of a secure culture was discussed when considering the threat from malicious emails. These and other matters covered by the Cyber Coordination Groups seem to cover fairly basic and standard controls that one would expect to see in any ISO27001 accredited or ISO27000 "family-aware" organisation. The implication is that industry standard practices are not particularly robust in some FSS institutions.

3.2 The Development of a Criminal Economic Infrastructure

There are many forms of attacks on FSS institutions. This paper is concerned principally with criminals who would intentionally attack individual investors, FSS institutions or supporting infrastructure services[8]. It is not concerned with "script kiddies" or "hacktivists" as they are not principally motivated by theft [27].

This section describes how the criminal ecosystem supports cyber-attacks and how the composition and capabilities of criminal groups has changed.

3.2.1 The Enabling Criminal Ecosystem

Simple criminality is straightforward to understand, the motivations are to make money and not get caught. Stringhini [28] describes how a criminal ecosystem has developed to enable this and a scenario illustrates how this works.

Assume a criminal wants to steal money from personal accounts. They need to know what method (attack vector) they might use. Perhaps a drive by download that installs malware on a website, or a phishing email containing malware as an attachment or a link to it. If the malware is to do its job it needs to find an exploit in the victim's system. This can be complex, but an exploit kit can be commissioned from other criminals, this is a highly technical piece of software that will do this job for you. Next, they need a host for their infrastructure that is delivering the attack; a bulletproof hosting service provider should suffice. Or perhaps they prefer that someone else does the malware spreading and infection for them. They can commission a "pay per install" service (PPI) to do this. PPI operators can offer a choice of options, including how many infections to install and even what countries to attack. If on the other hand they choose to run a botnet themselves they can commission support to run a command and control infrastructure.

[8] These kinds of attacks are termed in the research literature as "cyber dependent crimes", i.e., those which have become possible only with the development and adoption of computers and new technologies [28].

Assume the criminal now has stolen user credentials and have accessed a victim's account. Where to send the money? If the criminal doesn't know how to set up a fake account that service can be bought on the dark market too. Such services, with options, can be safely procured [28]. For those unclear about their choices advice can be found on dark web forums (using a service similar to DeepDotWeb, for instance[9]) using an anonymous browser such as Tor.

Another refinement, assuming one is not in a criminal gang with all the needed skills, is the option to join an "affiliate programme", a team of like-minded criminals using "branded" services provided by yet other criminals. Collectively the team carries out the crime and each takes a proportion of the proceeds for their contribution [28].

This scenario illustrates an important point: the existence of a cyber-crime economy providing a range of criminal services lowers the technical bar to entry for conducting cyber-attacks. This has two implications; first it means that no one person needs to have all the technical knowledge or skills needed to conduct an attack. Lower-skilled criminals can effectively commission high-skilled attacks with the right support. Second, it could result in *more* criminals turning to this type of crime. Resulting in yet more attacks.

One recent example from the synthesised attacks database in Appendix A of this paper illustrates the scale of this criminal market. In February 2020 thirty-six people from seven countries were indicted in the United States for their alleged involvement in the Infraud Organization, whose business was to sell stolen personal and financial information. The entry in the Database [#64][10] explains: "The organization was said to have more than 10,000 registered members who bought and sold illicit products including malware, data from credit card dumps, and information needed for identity fraud." Other examples of criminal marketplaces detailed in Appendix A are CardPlanet [#11] and BriansClub [#12].

3.2.2 Criminal Groups and their Increasing Capabilities

The above example also illustrates three further points, supported elsewhere in the research [18] [19] [20], and reinforced in the figures 2 and 3 following.

First, criminal (also called "threat actors") are highly differentiated, in ambition, capability and methods and different groups favour different targets. For example, nation state actors or their proxies will be patient, even over years, and wait for a possible bounty of millions of dollars.

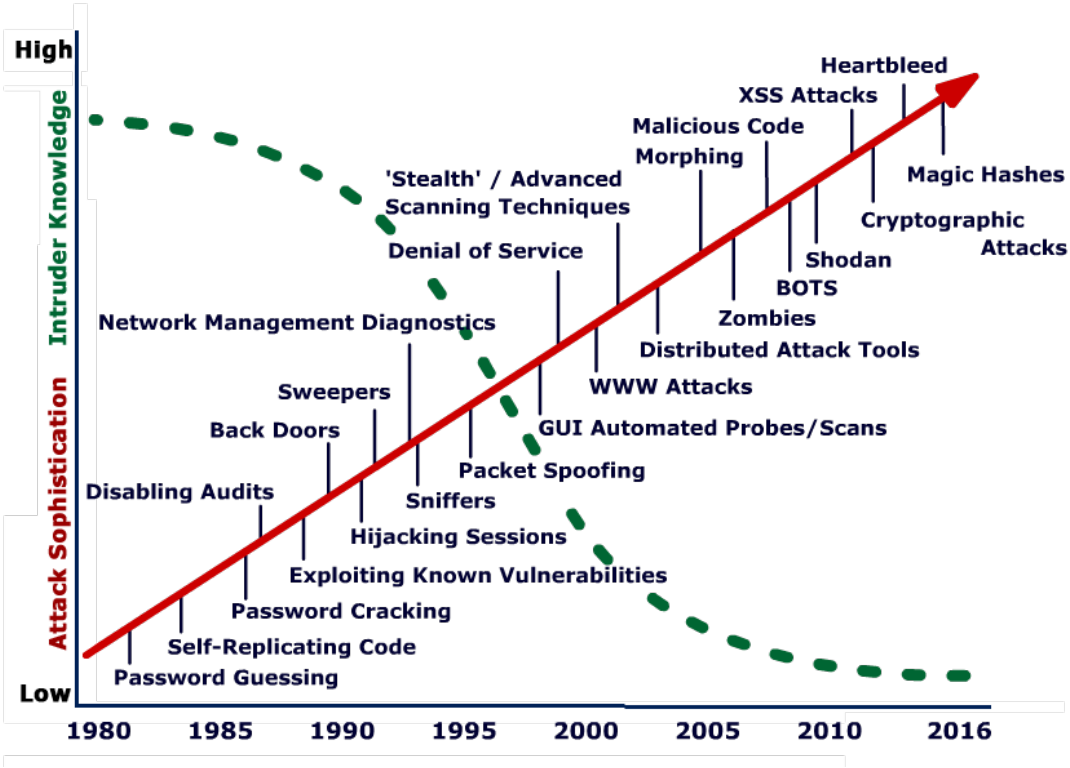
At the other end of this scale might be single skilled individuals looking for a far smaller payload, but one that is easier to execute and, critically, takes far less time to conduct (thus reducing the chances of being caught). High volume automated attacks [18] would be one way to proceed; this makes attacks economically viable as it means that even if only a small proportion of people fall victim to any attack, its scale is such that it still brings significant reward to the attacker to motivate them to launch the attack.

---

[9] DeepDotWeb was closed down by the FBI in 2019, but other sites can be expected to replace it [29].

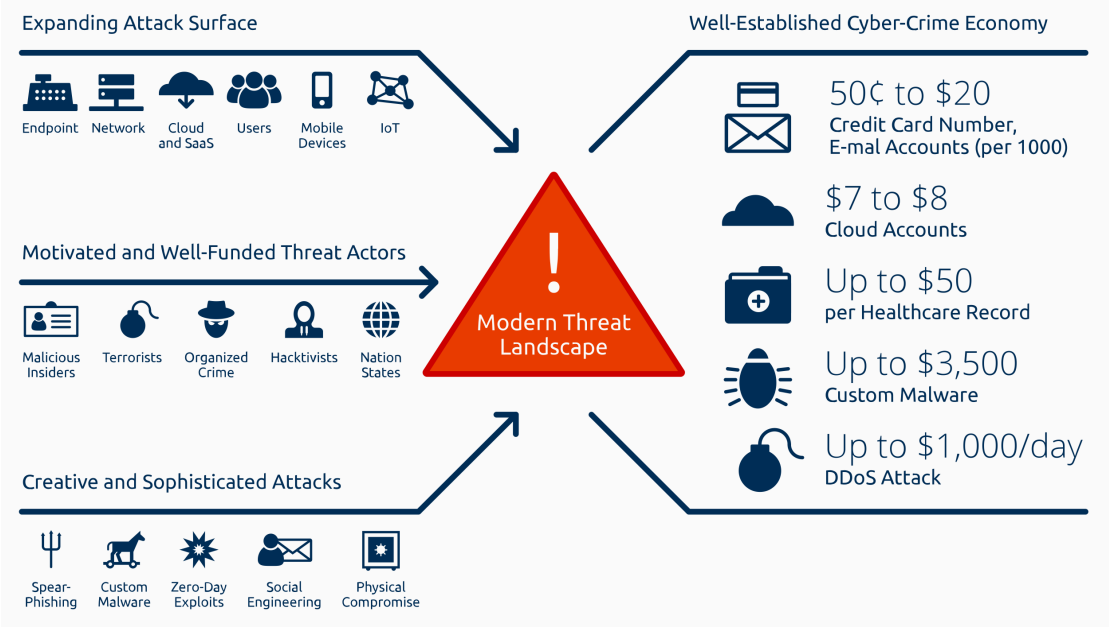
[10] Annotations in this paper such as #1, #2 etc. refer to the ID row in the database at Appendix 1.

Figure 2: A Typical Threat Landscape circa 2016



Source [30]

Figure 3: A Modern Threat Landscape circa 2020



Source [31]

Organised criminal gangs and affiliates would sit between these two positions. A good example of this approach is given by Fin7 Advanced Persistent Threat (APT) group attacks, the group responsible for the 2013 Carbanak attack. The group stole more than €1 billion from banks in more than thirty countries over three years, according to Europol [#102]. APTs can also be nation state proxies.

Second, independent of any access a criminal may have to other people's skills, as the attack techniques have become more sophisticated they have also, paradoxically, become easier to use and thus more accessible to lower skilled criminals [20]. This is illustrated above in Figure 3.

Third, at the same time, the technical degree of sophistication for exploit malware is also increasing meaning attacks are more difficult to prevent or mitigate against. The general narrative is that nation states and their APT proxies develop more sophisticated tools, and these somehow become available ("trickle down") to other threat actors. This increases the effectiveness of criminal exploits. A clear example of this is the 2017 WannaCry ransomware crypto-worm attack. While it seems [32] the attack may have been initiated from North Korea (who allegedly need the hard currency) the worm propagated through an exploit (EternalBlue) developed by America's National Security Agency. This trend is thought to become more likely as more nation states develop their offensive cyber capability [20].

3.2.3 Making Crime Pay: How Criminals Monetise Cyber-crime

A review of the criminal ecosystem would be incomplete without some understanding of how criminals monetise the proceeds of their crime. Appendix B sets out a detailed table, assembled by the author from various sources [33] [34], setting out how assets can be exploited and monetised. The table identifies for each asset the typical technique used for the exploit and how it can be monetised. A "comment" column provides further detail.

From this summary it seems criminals have three options when it comes to monetising their attacks, they can take direct cash payouts, cash equivalents, or use the data to launch further attacks.

Direct cash payouts are the option of choice [28] as it is after all typically the "end goal" of theft. Examples here would be direct transfers out of a personal account (e.g. bank); attack on a payments transfer system (e.g. via inter-bank transfer or through a "whaling" fraud); setting up a new account (fraud), then withdrawing cash; a payment through ransomware extortion e.g. from a DDoS, typically using cryptocurrency; using credit card processors; or ATM cash withdrawals.

The preferred method of payment will be that which cannot be traced. Crypto currencies are popular for this reason, especially Monero [33]. The risk to the criminal comes at the point at which the currency needs to be converted and withdrawn as cash. Also popular [28] are money transfer services such as Western Union (untraceable), which is preferred to PayPal (managed centrally).

"Cash equivalents" can be transferred into hard cash. For example, selling information on the dark web is popular, such as PII, credit card or account details. Credit cards can also be cloned and used. With this kind of asset time is crucial, as the older the data the less money it will sell for, as the data breach or theft may have

been noticed and remedied. Particularly lucrative [33] is renting out other peoples' computing capacity (without their knowledge) for example, for crypto jacking and botnet infection.

Data can be used to enable further attacks on other assets, for example by using a person's passwords and credentials, card and account information or other PII data to enable identity fraud [34].

Evidence of how criminals collaborate to monetise their assets, for example through some form of cryptocurrency money-laundering clearing house is difficult to find. It is not unreasonable however to imagine such a service being available on the dark web for a price. Access to such forums to test this assumption is not within the scope of this paper.

3.3 Chapter Summary

Threats to investors are likely to increase and the institutions that protect their investments might not be as secure as expected. There are three elements to this argument: changes in technology, changes within the criminal ecosystem, and from what we do know about UK FSS institutions.

Technologically the attack surface is increasing and this can be expected to continue. In addition, an added layer of complexity arising from the trend for different systems working together presents further attack vectors. A good example in both cases in the UK is the implementation of Open Banking. An increase in attack vectors is one probable outcome.

Second, a criminal ecosystem is in place to support a high level of differentiation in cyber-attacks. Less sophisticated criminals have access to better tools and a network of services to enable more complex attacks. No one person needs to have all the technical knowledge or skills needed to conduct an attack. Such criminals might be drawn to attack individuals (such as investors) which present an easier challenge than, say, banks. More sophisticated criminals, with APT capabilities, are increasingly likely to have access to variants of nation-state level tools. Such attacks could prove difficult to defend against. They might target banks, exchanges or other "higher value" systems.

Overall, this extends the capabilities of criminals at both the lower and higher ends of the skills continuum. The lowering of a technical "bar to entry" could also result in an increase in the numbers of criminals undertaking attacks.

Third, available evidence from the FCA suggests that the capability of UK FSS institutions to protect themselves from attacks appears highly variable and in some cases below industry standards (e.g. the ISO27000 family). At the same time available UK data, while partial, shows a general increase in attacks across all UK finance sectors. These include the Pension Savings & Retirement Income and Retail Investments sectors where investors are typically most active.

Some small mitigations to these developments can be suggested. Individual investors could be supported to learn how better to protect their identity and credentials. The Barclays Bank "Digital Eagles" scheme [35] [36] is an excellent example of what can be done to educate people to use the internet safely. FSS

institutions (if they don't already) could explore ways to make it more difficult for criminals to monetise the proceeds of crimes and thus degrade criminal motivation. More generally, the FCA could be more open in sharing the detail of cyber-attacks on UK FSS companies. This could enable the FSS cyber security community collectively to collaborate to better defend itself.

Chapter 4: Threat Models

This chapter introduces the information security technique of threat modelling as a means of understanding and responding to threats, specifically to attacks on investors, FSS institutions and FSS infrastructure services. It reviews existing models, including some developed particularly for FSS institutions (the APEX program).

From this it is concluded that none of the existing models are suitable to the purpose of protecting investors as well as FSS institutions. In an original contribution to the literature a new high-level model is therefore proposed constructed from core threat modelling concepts.

One further shortcoming of most reviewed models is an inability to integrate detailed prevention and mitigation measures into real-world threat scenarios. An intermediate-level threat model is therefore constructed for this purpose.

4.1 Understanding threat models

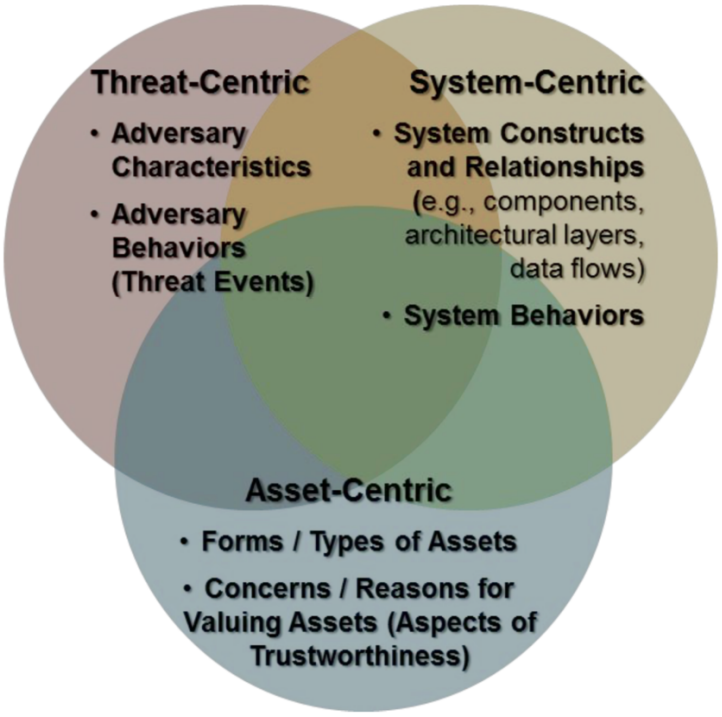
Threat modelling commonly is used to understand how cyber-attacks are conducted and thus what can be done to prevent or mitigate such attacks [19]. A typical threat modelling process [37] has three broad steps, to select a threat model; to populate that model with data; and to devise and run scenarios relevant to the threats. One then can draw conclusions and take actions.

There are many threat models and they can be used to different ends. Broadly they have five uses [37]:

1) as an input into an organisations risk management framework;
2) in cyber wargaming (develop and "play through" attack scenarios, test defences);
3) in "technology profiling and foraging" (identify gaps in defence and adapt or propose new technologies to fill those gaps);
4) for operational systems development (testing how live systems can respond to attacks, as part of the system development lifecycle, reviewing the design, analysis and testing of software); and
5) as part of wider systems for security operations and analysis (focussing on specific threats, sharing threat information with concerned parties, etc.).

There are three broad approaches to undertaking threat modelling. Shostack [27] proposes three strategies, one focussed on assets, one focussed on attackers and one focussed on software development. Figure 4 [37] shows how these different threat modelling approaches can relate to each other, though slightly different terminology is used. In the figure, "threat centric" refers to an attacker focused approach, "asset centric" to assets, and "system centric" encompasses a software development approach.

Figure 4: Threat Modelling Approaches



[Source: 37]

Of the three approaches this study will follow the threat-centric approach principally because this approach best fits with answering the research question of this paper, which is investigate the principal threats to investors assets, i.e., the focus is on specific adversaries and their attacks (or "threat events", as described in the figure).

This is also a pragmatic approach as both asset and system-centric approaches would require an in-depth knowledge of each financial institution's assets, policies, processes and technologies, specific to every attack. It could be possible to go some way to approximate this information from other sources, e.g., open source intelligence (OSINT) gathering, but this could require more time for research than is available.

By contrast there is sufficient data on cyber-attacks on FSS institutions to allow a threat-centric model to be developed. Another advantage of a threat-centric model is that it lends itself well to integration into a conventional ISMS risk management framework [38] [39] [40].

4.2 Review of Existing Threat Models

This sub-section first reviews the most common threat models then focusses on threat models developed specifically for FSS institutions as part of the US APEX program.

4.2.1 Common Threat Models

A recent (2018) and very comprehensive review of existing threat models was produced by Bodeau et al. [37]. It examined 19 threat modelling frameworks and

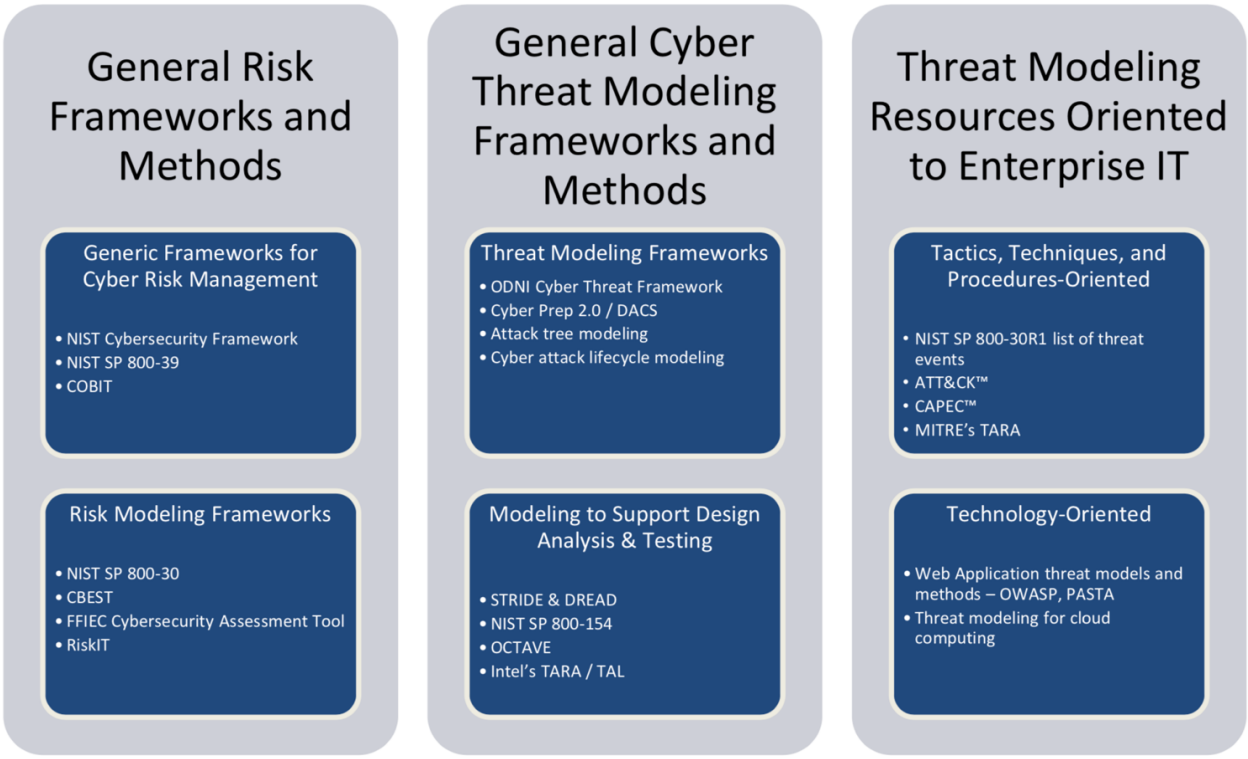
these are listed in Table 6. One reason there are so many models is that different models are designed for different intended uses in different business environments. Figure 5 that follows shows graphically how models can be further grouped by purpose.

Table 6: Summary of Threat Models and Frameworks

Model	Intended Use	Business Environment
DSB Six-Tier Threat Hierarchy	Risk Framing	Military
Cyber Prep and DACS	Risk Framing	Neutral
TAL	Risk Framing	Neutral
NIST SP 800-154 (DRAFT)	Design Analysis	Neutral
STRIDE	Design Analysis	Created for software development
DREAD	Design Analysis	Created for software development
OWASP	Design Analysis	Neutral
Invincea	Design Analysis	Neutral
CBEST	Penetration Testing	Bank of England UK finance sector
NIST SP 800-30R1	Risk Assessment	US Federal model
COBIT and Risk IT	Risk Assessment	Neutral
OCTAVE / Allegro	Risk Assessment	Neutral
Intel's TARA & TAL	Risk Assessment	Neutral
IDDIL / ATC	Risk Assessment	Neutral
STIX	Threat information sharing	Neutral
OMG Threat / Risk Model	Threat information sharing	Neutral
ATT&CK	Threat information sharing	Neutral
CAPEC	Threat information sharing	Neutral
ODNI, NSA/CSS	Threat information sharing	Neutral

Source [37]

Figure 5: Cyber Threat Modelling Frameworks and Methods



Source: [41]

The review allows one readily to compare key features of each model and thus to assess its suitability for whatever purpose the user may have. For each model a "threat domain coverage" is proposed, which broadly describes the types of threats the model is intended to address. Some models are more high-level or strategic in nature (e.g. CBEST), others more granular and specific (e.g., they employ Tactics, Techniques and Procedures (TTP) oriented approaches such as MITRE ATT&CK). Some models are populated with representative values (e.g. "types of attackers") others not. Some focus on the attack lifecycle in its entirety (from reconnaissance to maintaining access once a system has been compromised), others only from the point of exploit to maintaining access. The review also includes a "degree of adoption" criteria that shows whether a model is designed to fill a niche or is more widely used within the cyber community. Worth noting also, different models use different terms to describe similar concepts; care is needed when making comparisons [37].

Much of the review is given to categorising, listing, conceptualising and explaining these differences. Most of this detail is not relevant to our purposes.

4.2.2 The APEX Program Threat Models

What is relevant are the conclusions the authors reach from this review and what they did next.

The authors were part of team working for the US Homeland Security Systems Engineering and Development Institute (HSSEDI). This work was commissioned in

support of the US Next Generation Cyber Infrastructure (NGCI) Apex program. Their work comprised a series of papers [37] [41] [42] intended to provide a practical threat modelling capability for FSS institutions in the USA. It was focussed specifically on developing threat models relevant to technology foraging and war gaming outcomes.

From their review [37] the authors noted that many of the 19 models examined were not in fact in common use with many institutions. Either the models were adapted by companies to suit their own institution's security posture or they were foregone entirely in favour of a bespoke institutional model. [37]

The authors concluded that none of the models they reviewed suited their purposes either (which was to support the NGCI APEX program). They then proceeded in that paper [37] to propose and develop their own high-level threat model.

Further, a subsequent paper [41] built on this high-level model to develop an "enhanced" model, again, to support the purposes of the APEX program.

It is necessary below to explain and critique both high-level and enhanced APEX models. This is because while neither is suitable to be adopted for use in answering this thesis's research question, each provides a basis for the development of a threat model of our own.

4.2.2.1 The High-level APEX Model

Based upon NIST SP800-30R1 [40] there are four elements to the model: it's purpose, the notion of a hierarchy of levels, "key modelling constructs" and data with which to populate the model [37].

The purpose of the model is to provide a practical threat modelling capability for FSS institutions in the USA. It focusses on developing threat models relevant to technology foraging and war gaming outcomes. To emphasise, it is intended for FSS *institutions* specifically.

Second, the intention is this model can serve as a basis for the development a hierarchy of models. This has three levels: i) high-level (or sector-wide) uses described in general terms; ii) detailed (focussed on technology and wargaming looking at specific systems or targets); and iii) instantiated (to evaluate technology in use by institutions).

Third, it details a high-level model as a series of "key modelling constructs". The principal constructs of the model are first to develop a threat modelling terminology and then to describe, at various levels of detail, adversary intent, adversary goals, targeting, capabilities, characteristics, threat sources, threat actors, threat events, scenarios, attack vectors and "cyber effects". The relationships between these constructs are illustrated in Figure 6.

Figure 6: Key Modelling Constructs

Source: [41]

Fourth, the paper populates its constructs with long lists of data drawn either from its review of other models or from existing standards, such as NIST SP800-30R1.

4.2.2.2 The Enhanced APEX Model

This approach is developed in a subsequent paper by a team that included the authors of the High-level Apex Model. It proposes a more applied approach to threat modelling termed the "Enhanced Cyber Threat Model for Financial Services Sector (FSS) Institutions" [41].

The purpose of the model remains principally to support technology foraging, wargaming scenarios and technology test case validation for the APEX program [41].

The paper retains a hierarchy of three model levels but re-casts these as strategic, intermediate and detailed level models. Strategic modelling comprises "high-level classes of adversaries and attacks". Intermediate modelling (also called "enhanced") is the identification of tactics, techniques and procedures (TTP[11]), allowing for

[11] MITRE define these terms as follows: "**Tactics** represent the "why" of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access. **Techniques** represent "how" an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access. **Procedures** are the specific implementation the adversary uses for techniques or sub-techniques. For example, a procedure could be an adversary using PowerShell to inject into lsass.exe to dump credentials by scraping LSASS memory on a victim." [43]

scenario testing. Detailed modelling requires “as much as can be known about the detail of any attack, if one is to counter an attack with a coherent defence or mitigation” [41].

Turning to modelling constructs, the paper distinguishes between strategic (high-level) and intermediate (enhanced) level models.

In developing a high-level model for FSS institutions the paper focusses on three matters, adversary characteristics (their goals, capabilities, targets, timeframe, persistence and “concern for stealth”), attack vectors (”the paths by which an adversary might mount an attack on the defended system”) and threat events (“the individual steps or behaviors (sic) that an adversary can use in conducting an attack”) [41].

It next proposes an enhanced FSS threat model that includes these three elements with two additions. First, the threat events are populated from existing “common attack repositories”, specifically the three MITRE matrices (PRE-ATT&CK, ATT&ACK and Mobile) and the Common Attack Pattern Enumeration and Classification (CAPEC) system [44]. Second, a set of “generic scenarios” are proposed which can be applied to FSS institutions in developing specific scenarios for testing.

This enhanced model is then populated with data from various sources including MITRE and ODNI (see Table 6 earlier). This is set out in an Appendix 1 which runs to 61 closely typed pages of text. It need not be reproduced here.

Finally, in articulating the levels of detail at which the model might apply, the paper offers a generalised model of a breach scenario followed by two detailed “real world cyber-attack scenarios” (brief expositions of the Carbanak (2013) and Buhtrap (2016) attacks on FSS institutions, principally banks) [41].

4.2.2.3 Critique of the APEX Program Threat Models

The difficulties with the high-level model are several.

The first concerns the purpose of the model. To be critical, the paper seems to have begun with the intention of developing a model that can be applied to the APEX program but ended up more developing a “model of models” which needed further work. It may be better suited to the APEX program where it can focus on technology foraging and war gaming outcomes but it is otherwise limited.

Second, how is the model to be applied? Much of the material that comprises the model is both complex yet overly general and not particularly helpful. That is, it is too general and too detailed at the same time. It does not for example offer any case studies that demonstrates the practicability of the model.

Least helpful of all, like the 19 models it has reviewed, the APEX model focusses only on the “institution”, for example a company, as the subject of inquiry. It does not consider either the investor (at home or on the move making financial transactions) or the FSS infrastructure companies and services that supports and enables financial or investment processes (for example, such as payment transfer or clearing systems).

Real world cyber attacks in contrast can be complex and diverse spanning many different settings. To detail one recent example [#28] from May 2019, the gang that used the GozNym malware to steal over $100 million operated across the U.S., Bulgaria, Germany, Georgia, Moldova, and Ukraine. They stole from over 40,000 victims, including the bank accounts of small businesses, law firms, international corporations, and non-profit organizations. The APEX high-level model doesn't really lend itself well to threat modelling this type of scenario.

The difficulties with the extended model are both similar and different.

Like the high-level model its purpose is principally to support the APEX program. That this limits its relevance is acknowledged in the paper: "a limitation of the expanded threat model is that it does not go so extensively into attacks specific to the FSS…it does not define purely financially -orientated attacks." [41]

In articulating the enhanced model detailed thought is given to the tactics and techniques for attack (as used in the MITRE ATT&CK repository) but there is no treatment detailing prevention or mitigation of attacks. The research question for this thesis is to examine both threats to investors' assets and how to prevent or mitigate these threats. This is a significant omission from the enhanced model.[12]

As with the high-level model, both the strategic and enhanced APEX models focus only on the one setting, the FSS institution, to the exclusion of investor or FSS infrastructure settings. Again, this confounds answering the research question that is the basis of this thesis.

4.3 Developing the New FSS Threat Model

Despite their constraints there are three valuable lessons to take forward from the APEX models.

First, any new model needs to be clear at which level, or "flight altitude"[13], the model is intended to function, i.e., strategic, intermediate or detailed. A strategic model should be suitable for understanding threats and testing scenarios, but a more detailed model would also be needed to examine the specifics of any attack and to propose prevention and mitigation measures.

Second, it is important to identify the core "modelling constructs" that comprise the model and consider how they are to be populated. From reviewing both APEX programs there are certainly at least three central interconnected requirements of a high-level threat model, without any of which the model loses its capacity to adequately explain the nature of a threat; these are i) the threat source; ii) threat event and iii) threat scenario.

Third, the model should be applicable across all three settings of our actual threat landscape: the investor landscape, the FSS institution landscape, and the FSS infrastructure landscape. This needs to be a fourth characteristic of a new threat

[12] It seems that defence and mitigation was to be considered in the detailed model. However, while recognising that three levels of threat model (strategic, intermediate, detailed) would be appropriate only two (strategic and enhanced) were developed.

[13] Grateful thanks to an anonymous contributor for this notion.

model if the model is to be able to explain, and thus prevent or defend against, attack.

4.3.1 The New FSS Strategic Threat Model

There are four components to the new strategic model. This model will be tested in Chapter 6. Terms in *italic* are defined as they will be used in the model.

Threat Landscape: these are the different settings or environments in which attacks can occur. These are sometimes referred to as predisposing environment factors. An important point to emphasise is that different landscapes can have different *attack surfaces*, that is, opportunities for attackers to exploit a device, system, network, data or people. For example, a user at home on their desktop or mobile device is a landscape, an FSS institution, with its web presence, servers and networks is a landscape; a brokerage company that provides support to an FSS institution and is therefore part of FSS infrastructure is a landscape.

Threat source: the concern is with malicious behaviours, not accidental or unintentional incidents. *Threat actors* are the person or people who perpetrate these harms. They attack specific *targets* and have various *motivations*, usually but not always financial gain. Threat actors may be motivated directly (e.g. personal gain) or indirectly (e.g. as state proxies). They have differing *capabilities* or technical skills. The other adversary characteristics of timeframe, persistence and "concern for stealth" might also feature here [37].

Threat event: the technical nature of the incident and what else is known about how it was done. This approach conjoins two more common terms, *attack vectors* ("the paths by which an adversary might mount an attack on the defended system") and *threat events* ("the individual steps or behaviors (sic) that an adversary can use in conducting an attack") [41].

Threat Scenarios: a general approach to undertaking an attack, setting out what broad objective is being pursued and telling a high-level story of how the attack is followed through. Scenarios typically result in *harms* (adverse impacts) to one party or another. For example, in a fraud scenario, a criminal attacks a company's financial database, exploits a weakness in the Identity and Access Management function (IDaM) to harvest customer data which can then be used to rob personal accounts.

4.3.2 The New FSS Intermediate Level Threat Model

The purpose of this level of model, as noted earlier, is to examine the specifics of any attack and to propose prevention and mitigation measures. It adds to the strategic level model and is built upon it. This model will be tested using a case study in Chapter 7.

The components of the model are, *for each threat landscape*:

- To articulate the scenario;
- To describe the threat source;
- To analyse the threat event by setting out attack vectors and threat events (e.g. in one column) *and* to propose prevention and mitigation measures for each (e.g. in another column). It will use MITRE ATT&CK tactics and techniques to populate these fields.

Further narratives can be added to the model as needed, as employed in the APEX extended threat model [41].

4.4 Chapter Summary

Having reviewed the most well-known threat models in use in information security it was a surprise to find that none specifically addressed the threats facing investors. The focus in research literature is overwhelmingly on FSS institutions. A new threat model therefore was proposed.

First, two specialist threat models designed particularly for US FSS institutions were analysed and deconstructed.

This paper then proposed two new models, both of which are original contributions to the literature: i) a strategic level threat model, as a means of understanding and responding to threats to investors, FSS institutions and FSS infrastructure services; and ii) an intermediary level threat model, able to propose specific prevention and mitigation measures in response to real-world threat scenarios.

Chapter 5: Creating a Dataset to Populate the New Threat Model

The next step in the threat modelling process is to source the data that can be used to populate the threat model. This chapter asks what data is needed and examines the data available. It finds, surprisingly, there is no readily available detailed UK-specific data.

Consequently, in an original contribution to the research literature, it draws on existing published data sources to create a synthesised proxy dataset. It next populates the threat model with real-world attack data of the principal cyber-attacks on FSS institutions globally since 2005. (This is given in Appendix A.) It is argued that from this new dataset inferences can broadly be made, sufficient to use the new threat model.

5.1 Data requirements

The ideal dataset for a model focussed on threats to UK FSS threat landscapes would have the following properties:

Generally, disaggregated but anonymised data would be collected from the UK financial services sector and be regularly updated; it would be validated and come from a credible, central and authoritative source such as the FCA or the NCSC; and it would be of sufficient detail to populate both the new FSS strategic and intermediate level threat models.

Specifically it would include data detailing as much as is known regarding:

For threat landscapes: in what setting specifically an attack took place, separating out for example if the attacks were on individuals, on FSS institutions, or on FSS infrastructure services;

For threat sources: the threat actors, their targets, motivations and capabilities. Detail for targets should include which financial sector was attacked (e.g. ”pensions savings and retirement income”) and if any targets were investment platforms or brokerages;

For threat events: the type of incident, the path taken in commencing an attack and the steps taken in conducting the attack. Where known, information detailing how the proceeds of the crime were monetised would be useful. Further, a standardised technical means of describing the attacks would be helpful to support sharing of information between FSS stakeholders. One solution would be to use a common attack repository such as MITRE which describes attacks in terms of tactics and procedures used. Another example would be to use the CAPEC system [44].

For threat scenarios: sufficient detail to compile a narrative identifying the broad approach taken, the stages progressed in undertaking the attack and the harm caused [42].

5.2 Data availability

From the literature review it seemed that there were three approaches to finding the data needed. From government sources, from FSS institutions themselves and from searching the internet. It was not assumed that an ideal dataset would be available but it was thought that there would be sufficient data to populate a UK threat model. This turned out to be incorrect.

5.2.1 Data from Government Sources

Both the FCA and the NCSC collect data on cyber-attacks on UK FSS institutions.

The FCA legally requires of the (at least) 59,000 companies it regulates [6] that they must report a cyber incident to it if is deemed "material" under Principal 11 of the FCA handbook [45][14]. However finding detailed information on these incidents is very difficult. A search of the FCA website and documentation for example finds much general information on cyber resilience and references to increases in cyber incidents. Search the reports for evidence of this however and references point only to FCA "internal analysis" [6] [13]. To note, the best summary of FCA data found, reported in section 3.1.2, was made available following a Freedom of Information request [24]. Direct approaches made by the author to the FCA for information were not answered.

The NCSC will have data from at least two sources: first from support they provide to FSS victims of a cyber-attack (there is a link to the NCSC on the FCA website) [45]. Second, it maintains a Cyber Security Information Sharing Partnership (CiSP). CiSP is "a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business" [46]. Finding further information on this data was not possible. Direct approaches to the NCSC made by the author for more detail about CiSP were answered with a polite refusal[15]. To note, cyber security incidents reported to the NCSC are exempt from Freedom of Information requests [47].

Two further possible sources were explored. The Police's "National Fraud Intelligence Bureau" website [48] shows data on fraud, which would be relevant to our threat model. Unfortunately this shows summary data only. The Information Commissioner's Office publishes decision notices on data breaches which could also be relevant. However exploring this resource would better suit a longer piece of research as it would require examination of 8,889 such notices [49].

Relevant data from government sources was therefore unavailable.

---

[14] "Under Principle 11 of the FCA Handbook, you must report material cyber incidents. An incident may be material if it: 1) results in significant loss of data, or the availability or control of your IT systems; 2) affects a large number of customers; 3) results in unauthorised access to, or malicious software present on, your information and communication systems" [45].

[15] Source is email correspondence from author to NCSC, June 2020.

5.2.2 Data from FSS institutions

Data from FSS institutions directly on cyber incidents could not be sourced. The author asked five cyber security consultants who previously worked for clients in the financial sector what was possible. The universal view was not to expect any company to want to share data on cyber-attacks.

The reasons given broadly were that data is both commercially sensitive intelligence and is also security-sensitive information of probable use to cyber criminals. Further, some financial institutions do not follow industry best practice (rather they use "bespoke" solutions) and might therefore be culpable for negligence claims were they compromised by an attack and this became publicly known.

More than one consultant also noted that the use of Non-Disclosure Agreements is a common practice in the industry and this limits what people are allowed to disclose, including consultants.

5.2.3 Data from Internet Searches

Internet searches, using common search terms (cyber, attack, security, finance, financial, hack, investment, platform, UK, bank etc.) revealed a numerous disparate collection of different incidents. The terms "cyber attack bank" for example on Google revealed 24,500,000 results[16]. Sources included Mendeley's search facility, the University library and Google Scholar.

The searches returned a very wide range of information from generalised summaries of attacks to detailed White Papers [50]. There was data for different times and places, measured differently and for different purposes. Collectively however *as a body of data* the information was either not consistent, comparable or sufficiently detailed.

There were two exceptions: the "Carnegie Endowment for International Peace" [51] and the "Information is Beautiful" (IIB) [52] websites. The information from these sites were used to assemble a proxy dataset with which the new threat models could be populated.

5.3 Assembling a Proxy Database and Populating the New Threat Model

The dataset at Appendix A comprises 153 major cyber-attacks on financial institutions worldwide since 2005. It was produced by first combining then synthesising two separate datasets, one from the Carnegie Foundation, the other from the IIB website. Of the two datasets the principal source is the Carnegie dataset with 128 records while the IIB dataset contributes a further 25 records. Eleven IIB duplicates are not counted.

To show how the dataset was created the section below describes the content and format of the original datasets, then it shows how the combined dataset was reconfigured for use in threat modelling. It then explains how the fields in the dataset have been mapped to the new FSS threat model developed in Chapter 4.

[16] As at 14.08.2020.

5.3.1 The Original Datasets

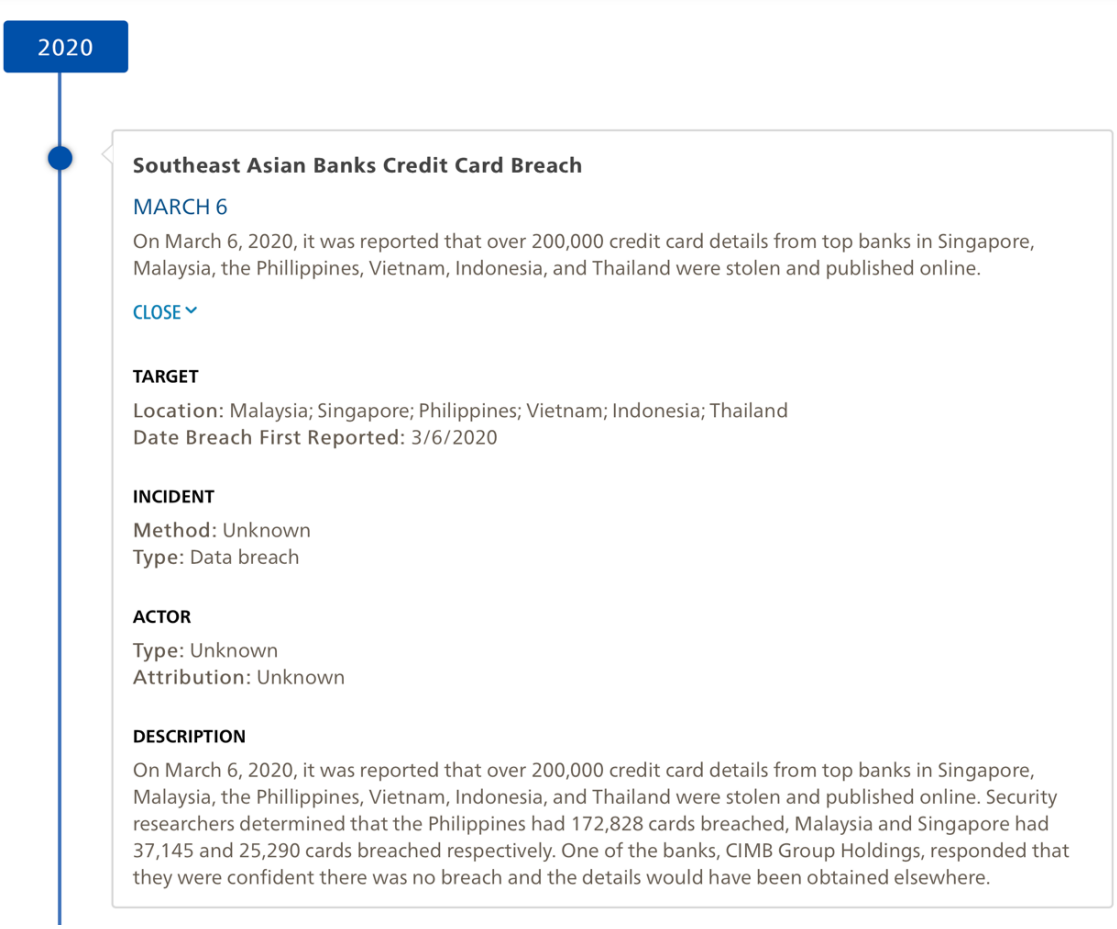
5.3.3.1 The Carnegie Dataset

The Carnegie Dataset was created by the Carnegie Endowment for International Peace [51]. It is a database of 123 known major attacks in the financial sector worldwide since 2007. It is maintained in association with the Cyber Threat Intelligence Unit of BAE Systems (British Aerospace Engineering) and is updated monthly.

The methodology in compiling and maintaining the dataset is explained in a White Paper, *Toward a Global Norm Against Manipulating the Integrity of Financial Data*, (2017) [53]. The purpose in creating and maintaining the dataset is to provide a consistent, standardised and global dataset of attacks on the financial services sector. It is an excellent source for the purposes of supporting threat modelling.

Figure 7 shows an example of an entry in the Carnegie dataset. A less detailed example has been chosen for brevity as the intention is to show the structure of their records.

Figure 7: Carnegie Dataset Record



Source:[51]

Each record starts with a title and short summary then lists country targeted, date of attack(s), type and method of incident, type of actor and strength of attribution to

the actor. Much of the detailed information is in a free text description field that contains further information known about each attack.

5.3.3.2 The IIB Dataset

This information is taken from the "Information is Beautiful" database [52]. The dataset was filtered for "financial" breaches, which produced 36 records (of which 11 were duplicates to the Carnegie entries and 25 new records).

The IIB dataset collects data by name of the victim of the breach, the year, sector, method of breach, number of records lost and the sources of the data. Each record also contains a description of the breach, which often provides good quality data on the detail of the breach.

5.3.2 The Synthesised Attacks Dataset

The objective was to create a dataset that could be mapped to the new FSS threat model constructs (established in chapter 4). There were two steps.

The Carnegie dataset was the more complex dataset and was therefore considered first. The approach was to examine the contents of every field and from that create a new structure that more closely matched the threat model. Table 7 below shows how this was done. Information from the IIB database was then similarly reconfigured. (In the SAD database in Appendix A IIB data is shown in blue text.)

Table 7: Synthesis of Carnegie Dataset to Synthesised Attacks Dataset

Fields in Carnegie Dataset	Fields in Synthesised Attacks Dataset (SAD)
Title	• Incident description
Introductory summary	• Not used
Country targeted	• Geography
Date of attack(s)	• Year, Date
Type of incident	• Type of incident
Method of incident	• Method of incident
Type of actor	• Threat Actor
Strength of attribution	• Not used
Description field	• Summary • Setting • What exactly was compromised? • What else do we know about *how* they did it? • What else known about *who* did it?

Source [Compiled by Author]

The second step was for every record in the database to be assessed, its contents dissected, edited and reconfigured to match the new fields in the SAD.

5.3.3 Populating the new FSS model with data

The next step was to map the fields in the SAD Dataset to the threat modelling constructs in the new FSS threat model. The following structure was created as offering the "best fit" between the SAD dataset and model.

Table 8: Mapping Fields from Synthesised Attacks Dataset to the Threat Model

Constructs in Threat Model	Fields in Synthesised Attacks Dataset
Threat landscape	• Setting • What exactly was compromised? • Summary
Threat source	• Incident description *(target of attack)* • Geography *(where the attack took place)* • Threat Actor • What else do we know about who did it?
Threat event	• Type of incident • Method • What else do we know about how they did it?
Threat scenarios	• Incident description • Summary *(and other fields where appropriate)*
(Not mapped)	• *Year* • *Date* • *Source* • *Secondary source* • *Link*

Source [Compiled by Author]

In this manner both databases were deconstructed and synthesised to enable mapping between the data and the new threat model. The outcome in Appendix A is a threat model populated with real-world data of the principal cyber-attacks on FSS institutions globally since 2005.

5.4 Drawing inferences from the data

It remains to clarify the extent to which we can draw inferences from the dataset to make statements about the UK FSS threat landscapes.

Given the data available a significant assumption needs to be made. That is, broadly, if the assets of *technologically equivalent targets* (i.e. financially services companies and banks) are being attacked using *comparable attack vectors and threat events* (e.g. malware used to access databases holding personal account data, DDoS to

effect ransomware extortion etc.), then this data can, broadly, serve as a **proxy** for potential similar attacks on UK financial services sector threat landscapes.

This limits the degree of confidence with which one can draw any conclusions from the dataset to the real-world circumstances of UK FSS threat landscapes. But, on the whole, such conclusions should not be significantly in error for the purpose of threat modelling attacks or devising countermeasures to them.

5.5 Chapter Summary

It was found, unexpectedly, that it proved not possible to access existing datasets of attacks on UK FSS landscapes.

The solution was to explore other sources and create a synthesised proxy dataset from two existing published datasets. The new dataset contained real-world data of the principal cyber-attacks on FSS institutions globally since 2005. It was argued that from this international dataset inferences can broadly be made sufficient to use in the new threat model. The synthesised dataset was then used to populate the new threat model.

The difficulty obtaining data underlines the importance of data sharing [54], principally from the FCA. The absence of information also significantly disadvantages investors who cannot then assess whether the investment platforms they use are more secure or not.

Chapter 6: Analysing Attacks using the New Threat Model

This chapter uses the new threat model as a structure to analyse the real-world attack data from the SAD dataset. It examines what can be learned from previous attacks.

First, threat landscapes are defined and examined. Second, threat source and threat event data is analysed. Threat scenarios, which seek to anticipate and prevent future attacks, are addressed in the next chapter.

6.1 Analysis of Threat Landscapes

All 21[17] threat models reviewed in chapter 4 took the FSS institution (e.g. a bank) as the assumed setting for a threat model. They do not generally consider other types of settings.

In an innovation to the literature the new threat model proposes two improvements, first it creates a new setting, "the investor landscape"; second, it brings together into one model three distinct threat landscapes: the investor landscape, the FSS institution landscape and the FSS infrastructure landscape.

What this means and the evidence to support this approach is considered next.

6.1.1 Defining Threat Landscapes

Each record in the SAD dataset at Appendix A is assigned to one of the three landscapes. This section explains the rationale for this selection.

The principal argument is that each threat landscape is distinct. The attack surface for investors, it is suggested, is quite different to that of institutions. For example, a model designed around the needs of an enterprise FSS company will need to consider the devices, applications, networks, data and personnel in that company. This, it is suggested, is not an approach best suited to anticipate and prevent attacks on individuals, perhaps trading from a room in their home or on their mobile 'phone.

A similar argument can be made for infrastructure landscape services. While in many respects they may be similar to FSS institutions they are different insofar as they demonstrate different attack surfaces and vulnerabilities to that of a bank. For example as shown in chapter 3, attacks on payments and inter-banking systems (such as SWIFT) use different attack vectors and threat events to an attack on a bank.

6.1.1.1 The FSS Investor Landscape

By investor landscape this study takes to mean the setting of individual investors who, at home or in transit, use applications and devices to make transactions on investment platforms. Currently this would typically be via a website or an app on a computer, tablet or mobile. Over time as the attack surfaces develop new attack vectors may be found.

[17] The 19 models in Table 6 and the two APEX models.

The structure of the SAD dataset did not initially capture attacks on such investor landscapes but instead identified FSS institutions or infrastructure services. Therefore some proxy was needed for such a landscape to be identified.

The threat to persons in the investor landscape is principally theft. This was established previously in sections 2.3 and 2.4 which argued there are a growing number of investors in the UK using investment platforms and that both the individual and the platform present, and will increasingly present, a lucrative target to criminals.

From the SAD dataset it is readily possible to identify theft from individuals' accounts. While a different attack vector is used in the actual data (e.g. credentials are stolen from the company as opposed to an individual) it demonstrates that *the focal point* of the attack is on the *individual* and not the institution.

An attack is considered to be in an investor landscape therefore if the focal point of the attack is on individual accounts. For example in attack #3 in Appendix A ("PayPal Accounts Linked to Google Play Abused", February 2020) the target was customers' personal accounts, used by criminals to carry out unauthorised purchases.

By contrast, theft of individuals' data from an institution is not considered an investor landscape as the focal point is the institution. For example, in attack #14 ("Turkish Card Details for Sale") credit card and PII data from over 460,000 customers was stolen and offered for sale online. This attack would be classified in the SAD dataset as being an FSS institution landscape.

6.1.1.2 The FSS Institution Landscape

This is the default landscape considered in most threat models. It has been defined as an "institution-centric view, taking into consideration institutional links to partners, suppliers and customers" [42]. In the SAD dataset these are predominantly banks but would include building societies or investment platforms.

6.1.1.3 The FSS Infrastructure Landscape

Some threat modelling literature recognises the need for modelling above the level of the institution, either at a "system of systems" [42] level or in addressing systemic risk from the perspective of protecting FSS as critical national infrastructure [55].

Working from the SAD data however it is proposed that the infrastructure landscape could be more broadly defined to include the companies, services or institutions that support and enable FSS institutions to trade. Examples of these services [42] [55] [56] include payment transfers (e.g. SWIFT) and central clearing systems; securities depositories and central counterparties; central banks; stock exchanges, brokerages[18] and other companies which manage the "order-execution" process; deposit, consumer credit and payment systems; and credit and liquidity products.

6.1.2 Evidence from the SAD Dataset

The outcome of applying these definitions to real-world attacks in the SAD dataset is given in Table 9.

[18] A brokerage in the finance sector is typically a company that acts as a "middleman" connecting buyers and sellers of shares in stock markets to make trades. [57]

Table 9: Diversity of Threat Landscapes

Threat Landscape	#	% (rounded)
Investor	18	12%
FSS Institution(s)	90	58%
FSS Infrastructure	45	30%
	153	100%

Source: [Compiled by Author from Appendix A]

Two points emerge. First, the method works. The data and the definitions sit well together. They are clear and logically discrete.

Second, a focus on the three landscapes should allow for greater insight. A focus on FSS institutions alone negates the fact that 42% of the attacks occurred in different settings.

Having postulated the value of examining the data by threat landscape the analyses below will test this idea by looking at data by landscape (i.e., as the control variable).

6.2 Analysis of Threat Sources data

The interest in threat source data is to understand what the targets are and who is undertaking the attacks. Table 10 details types of threat actors by threat landscape for the dataset overall.

Table 10: Types of Threat Actors by Threat Landscape

	State-Sponsored	Non-State actor	Unknown	Totals
Landscape				
Investor	0	9	9	18
FSS Institution(s)	17	34	39	90
FSS Infrastructure	11	11	23	45
Threat Landscape Total	27 (18%)	54 (35%)	71 (47%)	153 (100%)

Source: [Compiled by Author from Appendix A]

6.2.1 Investor Landscape

6.2.1.1 Targets

For the investor landscape specifically all incidents are of theft from personal accounts. Examples include:

- Money is transferred ("wired") out of the account. It is usually either sent to the criminals' accounts or is cashed by mules in ATMs. (See Appendix A examples #28, #50, #88, #107, #123, #142);
- Credit cards are used to make unauthorised payments for purchases (#3, #38, #40);

- Credit or debit bank cards are used to withdraw cash from accounts, e.g. using mules at ATMs (#31, #77, #114, #134);
- Tokens (e.g. loyalty vouchers) that can be monetised are stolen (#49).

Interesting to note from the view of a personal investor, attacks have already been made on high value individuals (#107) and on brokerage (investment trading) personal accounts (#123).

6.2.1.2 Threat actors

There are no attacks by state sponsored actors. Attacks are from non-state actors (typically criminals). Looking into the dataset three points emerge:

- A number of attacks (see examples #28, #31, #106, #116, #132, #133) are the work of organised and technologically sophisticated criminal gangs;
- The attacks are predominantly in East and West Europe, North and South America and Pakistan; and
- The gangs (those apprehended) tended to come from Eastern Europe (Bulgaria, Georgia, Albania, Russia).

However as just under half (47%) of attacks are of "unknown" origin we cannot draw any firm conclusions.

6.2.2 FSS Institutions landscapes

6.2.2.1 Targets

Targets are predominantly banks but other institutions are attacked also. These are detailed in Table 11. The range of targets is wide which suggests attackers are adept at identifying high value opportunities.

Table 11: FSS Institutions Attacked

Target	Attacks identified in SAD Dataset
Banks	#1, #2, #5, #10, #13-15, #20-22, #29, #30, #32, #33, #35, #37, #47, 48#, #51, #55-57, #59, #62, #66, #75, #79, #81, #83-85, #92, #94, #96, #98, #100, #103, #109, #111, #116, #119, #122, #124, #125, #128, #130, #131, #136, #140, #141, #143
Credit agencies	#4, #73
Currency exchange	#6
Crypto-currency exchanges	#19, #23, #24, #68
Commercial stores	#7
General financial services	#26, #27, #34, #63, #67, #70, #80, #99, #106, #113, #115, #127, #135, #137, #138, #145, #148
Investment banks and brokers	#41, #151
Government payments systems	#42

Target	Attacks identified in SAD Dataset
Health financiers	#89
Education financiers	#126

Source: [Compiled by Author from Appendix A]

6.2.2.2 Threat actors

Where attribution is possible half the attacks are state sponsored. Nothing definitive can be concluded however as there are as many unknown actors as known. Geographically the attacks are world-wide.

6.2.3 FSS infrastructure landscapes

6.2.3.1 Targets

Three types of targets stand out: payments systems, central banks and exchanges. Again, the breadth and variety of targets suggest resourceful and creative threat adversaries. These are detailed in the table below.

Table 12: FSS Infrastructure Services Attacked

Target	Attacks identified in SAD Dataset
Payments Systems	• Electronic payment systems [#18, #51, #111, #132]; • Management systems [#25]; • Switch and processor systems [#77,131]; • Interbank and transfer payment systems (such as SWIFT) [#35, #57, #60, #63, #70, #86, #89] (including the world's largest ever bank robbery, the Bangladesh Bank Hack, #81); • Clearing houses [#104].
Central Banks	• The European Central Bank [#16, #94] and the banks of Mauritius [52], Chile [59] and Mexico [60].
Exchanges	• The Nasdaq [#101, #109, #120], Hong Kong [#17], Shanghai [#85, #107], the New York Stock Exchange [#117, #128]. • Related attacks have targeted the Russian Exchange Rate [90], the world's largest Futures Exchange [#100], the US Securities Exchange Commission [71] and the US Federal Reserve [119]. Brokerages are also targets [#122, #143, #145].

Source: [Compiled by Author from Appendix A]

6.2.3.1 Threat actors

Where attribution is possible as many attacks are state sponsored as non-state sponsored. Nothing definitive can be concluded however as there are as many unknown actors as known. Geographically the attacks are world-wide.

6.3 Analysis of Threat Events data

The data in Table 13 below confirms what we already suspect from looking at threat source data. For investor landscapes the principal threat is from theft. For both FSS institution and FSS infrastructure landscapes the data is more complex. Theft accounts for roughly 40% to around half the cases. Motivations for data breach, disruption and espionage incidents could include state sponsored, state proxy or hacktivist interest. There are further nuances. Disruption (DDoS for example) is sometimes used to obscure thefts. These assertions are supported by a close examination of the data in Appendix A. Consideration of attribution and false flag issues need also be made before any conclusions should be drawn.

Table 13: Type of Incident by Threat Landscape

Threat Landscape	Theft	Data Breach	Disruption	Espionage	Unknown
Investor	16	1	1	0	0
FSS Institution(s)	35	36	12	2	5
FSS Infrastructure	25	11	7	1	1
Totals	75 (49%)	48 (31%)	20 (14%)	3 (2%)	6 (4%)

Source: [Compiled by Author from Appendix A]

The SAD dataset is variable in detailing how the attacks were progressed. The principal attack vectors overall are:

- Unknown (41) (31% of the attacks)
- Malware (25);
- DDoS (20);
- Other (12);
- Multiple (11); and
- Phishing (5).
- In addition, the IIB database annotates
    - "hacked" (9); and
    - "inside job" (9).

The high incidence of "multiple" and "other" attacks, on closer inspection, represent complex (some APT) multi-vector attacks. These attacks are not always technologically complex, but rather the way in which the attack is conducted is. Attacks by APT Group 41 for example use common network commands such as ping, FTP and pwdump alongside the more complex Cobalt Strike and China Chopper malware exploits [58].

That around a third of attacks are "unknown" limits any conclusions we can draw.

Looking specifically at the attack vectors for the investor landscape does not offer any particular insight: The data shows:

- Malware (4);
- Cards (3)
- Multiple (2);
- Unknown (2);
- “Hacked” (1);
- “Inside job” (1); and
- “Poor security” (1).

6.4 Chapter Summary

Analysing real-world attack data it became clear that it is important to conceptualise and distinguish between different threat landscapes. The investor landscape is different from that of FSS institutions. Similarly, a sole focus on “institutions” does not provide sufficient granularity in distinguishing between significantly different types of institutions. For example, those which are ‘customer facing’, such as banks or investment platforms, from those which provide the infrastructure to support such services, such as payments systems or exchanges.

This paper therefore i) developed the notion of threat landscapes by identifying three FSS threat landscapes, for the investor, the institution and for infrastructure services; and ii) integrated all three distinct landscapes into the new threat model.

Analysing the data by each threat landscape (i.e., as a control variable) revealed particularly rich data. Specifically for the investor landscape it suggested that the motivation for nearly all attacks is theft, that it is carried out by organised criminal gangs (i.e., non-state actors), mostly working from Eastern Europe. The targets are personal accounts and the principal attack vectors are malware, forms of card theft and “multiple” vector attacks.

A limitation on available data overall was that 31% of attack vectors and 47% of threat sources were “unknown”. This constrains any conclusions that can be drawn. Further, deeper research would be valuable.

Chapter 7: Threat Scenarios and Protecting Investors on Investment Platforms

Having identified probable threats to investors this chapter looks at how they can be managed.

Focussing on the investor landscape it first examines possible strategic level threat scenarios. It then takes one of those scenarios and details both how an attack could proceed and how it might be prevented or mitigated. It does this using the intermediate level threat model developed previously.

Last, this chapter explores asks how likely investors are to be victims of cybercrime and what do they understand about the risks in using investment platforms. A survey of investors conducted specifically for this paper provides some insight.

7.1 Threat Scenarios for FSS Institution and FSS Infrastructure Landscapes

The following section, 7.2, develops threat scenarios for the investor threat landscape. It is also important to recognise that the new threat model can also be used to examine threats to FSS institution and infrastructure landscapes. Examples of such threat landscape scenarios have therefore been created. This is not however the focus for this chapter and so these scenarios are set out in Appendix C.

Specifically, for *strategic* level threat scenarios, Appendix C1 details scenarios for the FSS infrastructure threat landscape only. Scenarios for FSS institution landscapes are not developed as these are common in the literature [37] [41] [42].

For *intermediate* level threat scenarios Appendix C2 details scenarios for both FSS institution and FSS infrastructure threat landscapes, as examples of these scenarios are not (as far as can be found) available in the literature.

Taken together with the investor threat landscape examples in section 7.2 below, the scenarios collectively give a more holistic view of the suitability of the new threat model to defend against threats across the whole threat landscape. The conclusion drawn is that the model appears readily applicable for all landscapes.

7.2 Threat Scenarios for Investor Threat Landscapes

Having developed a threat model (chapter 4), populated it with data (chapter 5) and used the model and data to analyse real world attacks (chapter 6) it remains to propose scenarios relevant to the threats [37].

In chapter 4 two models were developed:

1) A strategic level threat model which is suitable for developing general threat scenarios (section 4.3.1); and
2) An intermediate level model which, it was argued, could be employed to illustrate both how an attack might occur and how the attack could be prevented or mitigated (section 4.3.2).

While the analysis (chapter 6) appropriately considered all threat landscapes the motivation for the thesis remains how to protect individual investors from cyber

crimes. The case studies below therefore principally address the investor threat landscape.

7.2.1 Strategic Threat Scenarios

There are a number of sources in the FSS research literature [37] [56] [58] setting out different types of high level scenarios, some generic, some specific. These are summarised in Table 14.

While all are relevant either to FSS institution or FSS infrastructure landscapes they are not, with arguably two exceptions, (fraud and identify theft) applicable to investor landscapes.

Table 14: Strategic Threat Scenarios in Research Literature

Focus of Scenario	Scenario
Generic [37]	▪ Breach ▪ Fraud ▪ Misuse ▪ Destruction ▪ Friendly fire ▪ Upstream attack ▪ Reputational damage ▪ Stepping-stone attack ▪ Extortion.
Systemic Risk [56]	*High Impact Scenarios* ▪ Locking malware or ransomware attack on a financial institution ▪ Large wire transfer fraud ▪ Data breach and targeted Information Leaks ▪ Placing malware in trading systems ▪ A large-scale cyber-attack on a global messaging network for financial transactions ▪ Simultaneous cyber-attacks on systemically important institutions *Upstream infrastructure scenarios* ▪ Disruptions to central clearing ▪ Attack disrupts payment-processing gateways ▪ Massive malware infection ▪ Cloud provider fails ▪ Utilities disruption causes knock-on effects

Focus of Scenario	Scenario
	External Shock and Other Scenarios ▪ Sanctions retaliation via cyber attack ▪ Armed conflict
Deepfakes & Synthetic Media Attacks [59]	*Scenarios Targeting Individuals* ▪ Identity Theft ▪ Imposter Scam ▪ Cyber Extortion *Scenarios Targeting Companies* ▪ Payment Fraud ▪ Stock Manipulation via Fabricated ▪ Stock Manipulation via Bots ▪ Malicious Bank Run Scenarios Targeting Financial Markets ▪ Malicious Flash Crash *Scenarios Targeting Central Banks and Financial Regulators* ▪ Fabricated Government Action ▪ Regulatory Astroturfing

Source: [37] [56] [59]

Therefore, in another contribution to the research literature, this paper proposes new threat scenarios for the investor threat landscape.

These are set out in Table 15 below and are put forward as a starting point for the future development of other scenarios in further research.

The scenarios are derived from the findings in chapters 2 and 3 of this paper (which looked at investors, investment platforms, UK FSS cyber-attacks and what we know of evolving criminal organisation and capabilities); and the analysis of threat source and threat event data in chapter 6.

Table 15: Investor Threat Landscape Scenarios

Scenario	Typical Threat Actor	Ultimate Target	Intermediary Target
Attack individual investors on their home networks or devices[19].	Lower-skilled criminal, affiliates or gang of criminals.	Investment platforms and accounts.	• Any vulnerability that allows exploit of

[19] A similar example from the dataset is 'Operation High Roller' in 2012 [ID#106] where criminals specifically targeted high balance bank accounts in Europe.

Scenario	Typical Threat Actor	Ultimate Target	Intermediary Target
Attacks can be automated and at scale to minimise cost and maximise likelihood of a "payout" to the criminal(s).		Banking transactions and other financial data, both from banks and non-banks. E.g. Financial services databases, FS transaction message traffic, customer information databases.	Investor assets, such as devices (computer tablets, phones); apps and programs, OS systems and networks. • Attacks on people (phishing, whaling, etc.) to download malware, e.g. a banking trojan virus.
Card-based trading apps (e.g. Revolut) are compromised. As for other card scams, they can be used for direct transfer to criminal accounts, or cloned and used, or sold on the dark web.	Low-medium skill criminals with suitable ecosystem support, e.g., an affiliate group.	Investment platforms and accounts. Financial services databases.	• Application programming interfaces (APIs). • Digital platforms.
An exploit is discovered in the use of open banking & open-finance technology. By sharing your personal finance data across different institutions and systems an attacker has found a vulnerability.	Higher-skilled criminal or gang of criminals. APT level groups.	Consumer banking or investment transactions and other financial data, both from banks and non-banks. E.g. Financial services databases, FS transaction message traffic, customer information databases.	• Application programming interfaces (APIs). • Applications (e.g. the HSBC "Connected Money" app launched in May 2018.

Source [Compiled by Author]

7.2.2 Case Study: An Intermediate Level Threat Scenario

To protect investors on investment platforms a further step is needed. The following case study in Table 16 is offered as an example of how threat modelling can be used practically to develop appropriate prevention and mitigation measures to counter expected threats.

This is a small but significant innovation to existing threat-centric modelling approaches [37] [41] 42] which, while they detail threats, stop short of proposing actual preventative or mitigation measures. The inspiration for this approach is taken from Shostack [27] whose work on threat modelling for software development offers a robust example of how to develop defences against possible threats.

The intermediate level threat model sets out, for a threat landscape, threat scenario, threat source and threat event data, taking care to propose preventative measures for each attack vector or threat event identified.

The case study develops the first scenario outlined in Table 15 earlier, an attack on a home network. The scenario uses a real exploit, DefensorID, which would effect the attack.

Threat event data is taken directly from MITRE ATT&CK. The attack vector / threat events column use MITRE tactics and techniques (explained earlier in a footnote in section 4.2.2.2 [43]). The layout of the table adapts the format used in Fox's paper [41].

Table 16: DefensorID Mobile Banking Trojan Case Study

Scenario: An attack is being made on an investor on their home devices to access their funds in an online investment platform. In this example the attack is via an android device (e.g. mobile phone or tablet running the OS). Malware was downloaded while visiting Google Play, an authorised App store. The exploit is Defensor ID, a banking trojan, which can steal from both bank or other accounts and cryptocurrency wallets.	
Threat Source ▪ *Target*: To access an investors account and transfer funds to the attacker's dummy account. ▪ *Threat Actor*: Non-state actor, i.e., a criminal or group of criminals. ▪ *Capability*: A medium level of skill is required to execute the attack successfully. ▪ *Monetisation*: Direct cash payout, via transfer of funds to dummy accounts.	
Threat Event: Theft	
Attack Vector / Threat Events	**Prevention / Mitigation**
Initial Access • Deliver malicious App via Authorised App store	• Application vetting • User guidance
Execution	

• Broadcast receivers	• Use recent OS version
Persistence • Broadcast receivers	• Use recent OS version
Defence Evasion • Application discovery • Input injection	• Application vetting • Enterprise Policy • User guidance
Discovery • Application discovery	• Application vetting
Collection • Screen capture	• Application vetting • Enterprise Policy • User guidance • Application Developer Guidance
Command and Control • Standard application layer protocol	• "This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features."
Exfiltration • Standard application layer protocol	• As above
Impact • Input injection	• Application vetting • Enterprise Policy • User guidance

Source [Table compiled by author; threat event data from 60]

The model could be developed or extended further as needed. For example, a narrative could be added in a column explaining the attack vector / threat event (e.g., that "broadcast receivers" means that the exploit abuses the accessibility service to auto-start the malware on device boot). Additionally a further column could be added to explain the precise procedures to implement preventative measures, such as "application vetting" and so forth, specific to devices, networks and systems.

7.3 Protecting Investors on Investment Platforms

Having identified threats to investors from cyber-crime does existing evidence suggest they are in fact at risk? And if they are, do they understand that?

7.3.1 Evidence of likelihood of crime

Available evidence from the UK Police force National Fraud Information Bureau, summarised in Table 17 shows data for cyber-crime fraud over the past 12 months (data is collected on a rolling 12-month basis).

It records 28,831 persons have been victims of all cyber frauds and lost a total of £2.1m. As with other forms of cyber crime, it is likely that this figure is underreported [61]. Some of these victims may also be investors although the data does not show this. It does detail the attack vectors for the frauds: in order of prevalence, social media and email hacks, malware, hacking personal accounts, extortion and hacking the server.

Table 17: National Cyber-crime Fraud Data (August 2020)

Data	Individual	Organisation
Number of reports	28,831	3,482
Reported losses	£2.1M	£5.7M
Hacking – social media and email	13.8k	2.1k
Computer virus – malware – spyware	7.2k	327
Hacking personal	4.5k	163
Hacking extortion	3.2k	300
Hacking server	36	307

Source: [48]

That the majority of 'hacks' are from social media and email suggests that individual cyber safety, such as awareness of phishing, is at least as important as defences put in place by companies [19]. Are investors aware of this joint responsibility?

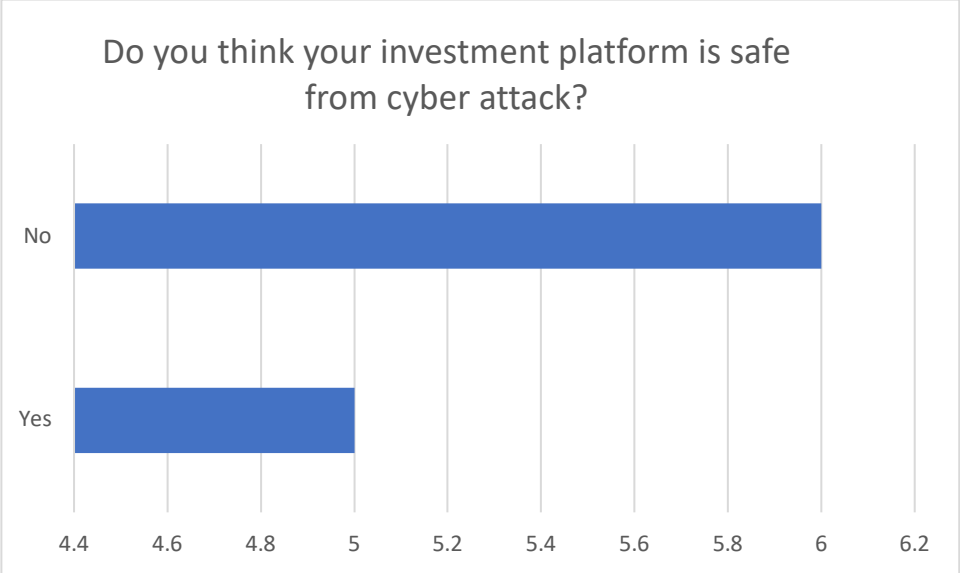
7.3.2 Investor Survey

An un-scientific survey of a cross section of investors, undertaken for this thesis, suggests that investors are vulnerable to cyber theft. Appendix D shows the questions asked and the methodology used.

The responses to questions 3, 6 and 8 are of particular interest. Figures 8, 9 and 10 show the results graphically. To take each in turn:

Question 3 below asks if respondents believe their investment platform is safe from cyber-crime. Nearly half do. This seems at odds with the detailed evidence of attacks on personal accounts from the analysis in section 6.2.1.1.

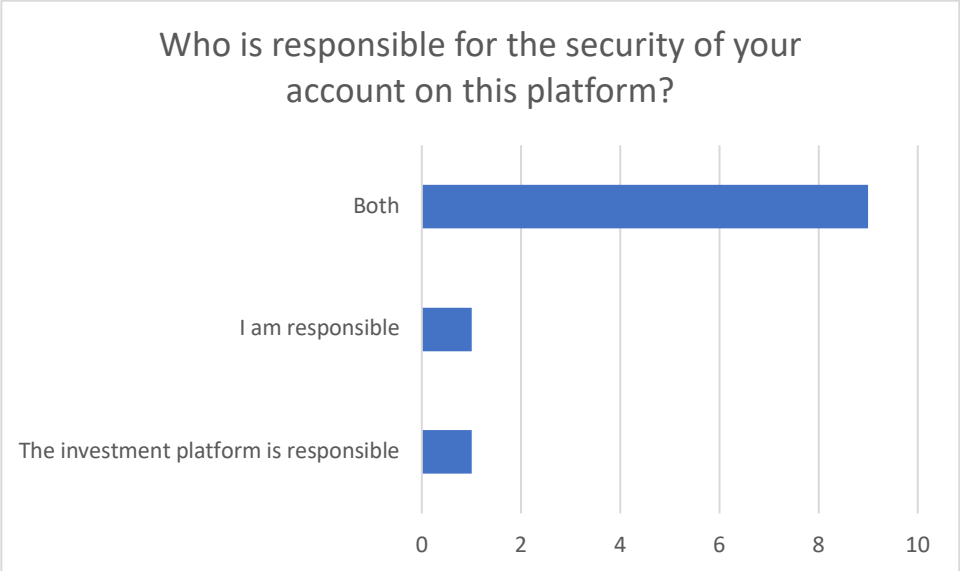
Figure 8: Survey Question 3. Is Your Platform Safe?



Source: [62]

Responses to question 6 show that most people accept that the safety of their investment platform is the responsibility of both themselves and the investment platform. This is encouraging.

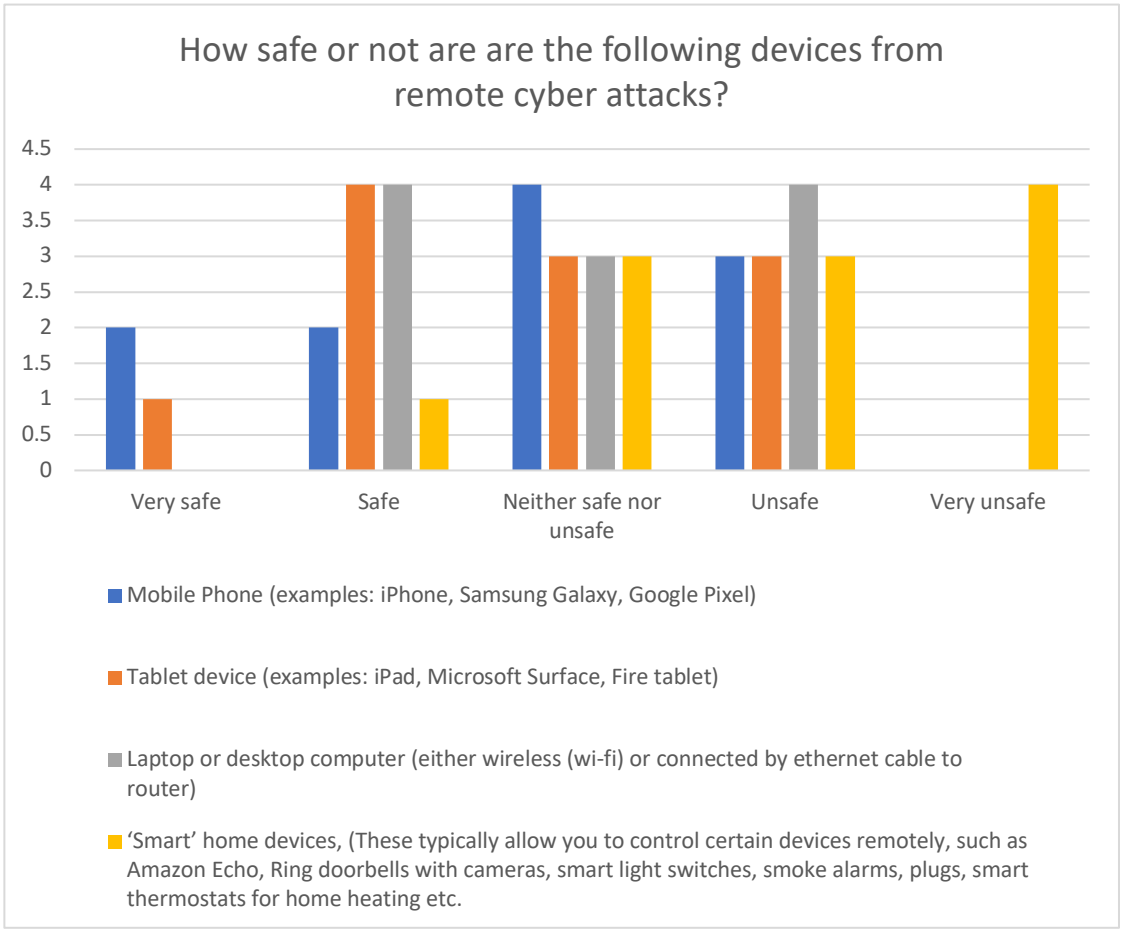
Figure 9: Survey Question 6. Responsibility for Account Safety



Source: [62]

Most surprising were the answers to question 8 which revealed that people believed some devices to be more safe than others. (The choices were mobile 'phones/tablets, computers and IoT – smart home - devices). Specifically, 36% of respondents thought mobile 'phones and tablet devices were very safe. This is not correct, as the DefensorID case study clearly demonstrated earlier.

Figure 10: Survey Question 8. Security by Device



Source: [62]

If these results were representative of the wider investment community there would be two clear conclusions worthy of further study.

First, that some people believe their investment platforms are safe may lead to a false sense of security regarding the real risk to them of crime.

Second, most people realise IoT devices present risks to their security, which is realistic. However the 36% who do not realise their 'phones and tablets are a significant attack vector for mobile banking trojans [2] [18] [19] [20] [33] suggests a vulnerability to crime that many cyber criminals could exploit.

This reinforces the conclusions reached in chapter 3, that education and support of investors to develop safer cyber skills is needed. Both the FCA and investment platforms could take a lead here.

7.4 Chapter Summary

A review of existing strategic threat scenarios revealed two different problems. First, almost none addressed scenarios relevant to the investor landscape. Second, no threat-centric scenarios (as far as could be found) included prevention or mitigation measures to defend against threats.

Consequently this paper developed a new set of strategic threat scenarios for the investor landscape and, as a case study, developed and applied an improved intermediate level investor landscape threat scenario that included prevention and mitigation measures. The paper also demonstrated how this model could be developed in further work. It is recommended that more strategic and intermediate-level scenarios should also be developed in future research.

Investors are twice vulnerable. First, a preliminary review of current Police evidence on cyber fraud crime confirms that investors are at risk from criminals. Second, an initial survey of investors undertaken specifically for this paper illustrates that investors have a limited understanding of the risks to them using investment platforms. If anything, they rely on "others" (the investment platform, the device manufacturer etc.) to keep them safe. This could result in investor complacency and a failure to appreciate that they personally are targets for criminals who would steal their account credentials.

Chapter 8: Conclusions

The research question set in this paper is "What are the principal cyber threats to investors' assets on UK investment platforms and what can be done to prevent or mitigate these threats?"

The motivation for the research question came from an initial perception that there was little in the literature, or in cyber security practice, that examined these threats from the point of view of an individual investor.

The literature review provided a context for the research. It found there are a distinct class of people can be identified, investors, who present and will increasingly present a lucrative target for cyber criminals. These investors are increasingly using a new technology (investment platforms) which are developing and melding with other new forms of technologies (e.g. open banking) that together increases the attack surface. At the same time criminals are likely to have an increasing capability and capacity to target investors and investment platforms, not least due to the continuing development of the criminal ecosystem that supports them. From the pattern of historical attacks and an analysis of the SAD dataset, it appears criminals as a group are clever, flexible, imaginative, resourceful and highly differentiated. They will adapt to new opportunities and these need to be anticipated by the cyber security community.

Subsequent data analysis and threat modelling revealed that there are several threats that need to be addressed. In particular:

Existing attacks targeting investor landscapes accounted for 12% of attacks in the SAD dataset.

- The motivation for almost all attacks is theft;
- It is carried out by organised criminal gangs (i.e., non-state actors), mostly working from Eastern Europe;
- They target personal customer accounts; and
- the principal attack vectors are malware, forms of card theft and "multiple" vector attacks.

Future scenarios for attacks include:

- High volume and automated attacks on individual investors on their home networks or devices;
- Targeting hybrid card-based trading apps (e.g. Revolut). These are new to the market and, as technology develops, more hybrids can be expected;
- Targeting open banking and finance technologies which share personal finance data across different provider platforms (perhaps multiple platforms could be attacked per investor).

These threats present a growing challenge to financial services sector institutions to develop new practices that can enable investors to feel secure and trust the newly emerging investment platforms designed for them.

The research found there were four significant barriers to understanding the threats to investors. First, no existing threat models could be found that had an investor-focused framework. Second, appropriate UK data, while collected by the FCA, was not available. Third, threat landscapes only considered the "FSS institution" setting and not investor or (specifically) infrastructure landscapes. Fourth, there were no threat-centric scenarios that sought to anticipate and defend against threats to investors.

One of the main reasons for these gaps is that research to date is designed to understand threats to FSS institutions and not investors. Clearly there is a growing need to design new solutions.

The solutions proposed in this paper were first to develop a new threat model that allowed for consideration of cyber threats to investors, institutions and infrastructure services by developing threat landscapes for each. The model achieves this at both a strategic level and an intermediate level.

Having developed the model it was next necessary to validate it by creating a synthesised (proxy) dataset and using that to populate the model.

Using real-world attack data with the new model an analysis of threat source and threat event data brought out the principal existing threats to investors. It also confirmed that it was important to separate out the three threat landscapes i) the investor landscape; ii) the FSS institution landscape; and iii) the infrastructure landscape. The reason for this is that the types of threats vary for each landscape, relative to the attack surface. This degree of granularity is mostly overlooked by other models.

New strategic and intermediate level scenarios specifically for investors were then proposed based on the paper's research and analysis. Using an illustrative case study it was demonstrated how prevention and mitigation measures can be integrated into an intermediate level scenario, thus defending against specific threats.

Having overcome these initial barriers demonstrates that threat modelling can be adapted to become an effective security tool to anticipate and counter threats. A number of challenges however have been identified for further research:

- Better data is needed to populate threat models, particularly on incidents (and threat event data) involving investors, particularly on UK specific data;
- Better and more threat scenarios need to be developed for the investor landscape. This is needed both at the strategic level, and particularly for intermediate level scenarios, which is where the detail of prevention and mitigation measures can be put in place.

To conclude, people using investment platforms should expect and insist that investment platforms provide good quality industry comparable data on how secure their platforms are. Based on the initial survey conducted here, investors show a limited understanding of how they are at risk, of how the platforms work and what the potential cyber security threats are. One innovation would be that investment platforms be accredited to an agreed ISO standard, such as ISO27015. Investors can

then use this information when choosing a platform. Investment platforms should also support investors to become better at cyber security and so minimise the attack surface to criminals.

Finally, the FCA in particular could share more information, suitably anonymised, with the cyber security industry so collectively more can be done to improve cyber security for everyone who has an interest in the UK's financial services sector.

Bibliography

Please note. References in the thesis annotated with a hash # refer to the ID numbers in the Synthesised Attacks Database in Appendix A. For example, [#1] refers to the Southeast Asian Banks Credit Card Breach.

[1] The Council of the European Union, "EU Council Directive 2008/114/EC," Off. J. Eur. Union, no. 8 December, 2008.

[2] Her Majesty's Government, "National Cyber Security Strategy 2016-2021," p. 43, 2016.

[3] Centre for the Protection of National Infrastructure, "index @ www.cpni.gov.uk." [Online]. Available: https://www.cpni.gov.uk/. [Accessed: 11-Aug-2020].

[4] House of Commons Library, "Financial services: contribution to the UK economy," Commons Brief. Pap., no. 6193, p. 10, 2018.

[5] The City UK, "Key Facts About the UK as an International Financial Centre," TheCityUK.com, October, 2018.

[6] Financial Conduct Authority, "FCA Sector Views 2020."

[7] "The FCA and its labyrinthine rulebook need a serious shake-up," Financial Times. [Online]. Available: https://www.ft.com/content/8438983c-abb4-11e9-8030-530adfa879c2. [Accessed: 11-Aug-2020].

[8] "UK regulators delay two-thirds of new measures in response to Covid-19." ," Financial Times. [Online]. Available: https://www.ft.com/content/299d47ef-8d43-49de-8749-4322aa880672. [Accessed: 11-Aug-2020].

[9] Bank of England, "Senior Managers Regime," June, 2020. Available: https://www.fca.org.uk/publication/corporate/applying-smr-to-fca.pdf

[10] Which?, "Revolut launches free stock trading: should you invest?" [Online]. Available: https://www.which.co.uk/news/2019/08/revolut-launches-free-stock-trading-should-you-invest/. [Accessed: 11-Aug-2020].

[11] Finder.com, "Investment statistics: How many Brits are investing in stocks and shares?" [Online]. Available: https://www.finder.com/uk/investment-statistics. [Accessed: 11-Aug-2020].

[12] Office for National Statistics, "Ownership of UK quoted shares: 2018." [Online]. Available: https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/labourproductivity/articles/sicknessabsenceinthelabourmarket/2018. [Accessed: 21-Aug-2020].

[13] Financial Conduct Authority, “Investment Platforms Market Study,” Market Study MS17/1.3. March, pp. 1–60, 2019.

[14] “Assets Under Administration (AUA).” [Online]. Available: https://www.investopedia.com/terms/a/assets-under-administration.asp. [Accessed: 13-Aug-2020].

[15] Which?, “Investment platforms reviewed.” [Online]. Available: https://www.which.co.uk/money/investing/investment-platforms/investment-platforms-reviewed. [Accessed: 11-Aug-2020].

[16] The Motley Fool, “The best online share dealing accounts for 2020.” [Online]. Available: https://www.fool.co.uk/mywallethero/share-dealing/buy-shares/. [Accessed: 11-Aug-2020].

[17] Financial Times, “Surge in investment account openings on UK platforms.” [Online]. Available: https://www.ft.com/content/b476c95e-22c8-49db-a0c8-42d48eac0bd2. [Accessed: 11-Aug-2020].

[18] W. A. Carter, “Forces Shaping the Cyber Threat Landscape for Financial Institutions,” October, pp. 1–31, 2017.

[19] A. Rashid, H. Chivers, G. Danezis, E. Lupu, and A. Martin, “The Cyber Security Body of Knowledge (CyBoK) 1.0,” 2019.

[20] Adrian Nish and Saher Naumaan, “The Cyber Threat Landscape - Confronting Challenges to the Financial System,” Cyber Policy Initiative Working Paper Series, Carnegie Endowment for International Peace, 2019.

[21] “Society for_Worldwide_Interbank_Financial_Telecommunication @ en.wikipedia.org.” [Online]. Available: https://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecommunication. [Accessed: 13-Aug-2020].

[22] “Exploit Database.” [Online]. Available: https://www.exploit-db.com/. [Accessed: 13-Aug-2020].

[23] R. and C. for S. Information and Technologies (CSIT), “Department for Digital , Culture , Media and Sport UK Cyber Security Sectoral Analysis and Deep-Dive Review,” June, 2018.

[24] “uk-fca-receive-900-cyber-incident-reports @ www.kroll.com.” [Online]. Available: https://www.kroll.com/en-ca/insights/publications/cyber/uk-fca-receive-900-cyber-incident-reports. [Accessed: 20-Aug-2020].

[25] Financial Conduct Authority, “Cyber and technology resilience in UK financial services,” Speech by Megan Butler., pp. 1–5, 2018. Available:

https://www.fca.org.uk/news/speeches/cyber-and-technology-resilience-uk-financial-services [Accessed: 13-Aug-2020].

[26] “Insights from the Cyber Coordination Groups | FCA.” [Online]. Available: https://www.fca.org.uk/publications/research/insights-cyber-coordination-groups#lf-chapter-id-ccg-insights-malicious-emails. [Accessed: 12-Mar-2020].

[27] A. Shostack, ‘Threat Modeling: Designing for Security’, Indiana: John Wiley and Sons, 2014.

[28] G. Stringhini (pp241-241) A. Rashid, H. Chivers, G. Danezis, E. Lupu, and A. Martin, “The Cyber Security Body of Knowledge (CyBoK) 1.0, Chapter 7, Adversarial Behaviour”, 2019.

[29] “Feds Dismantled the Dark-Web Drug Trade—but It’s Already Rebuilding.” [Online]. Available: https://www.wired.com/story/dark-web-drug-takedowns-deepdotweb-rebound/. [Accessed: 13-Aug-2020].

[30] “Typical Threat Landscape c.2016.” [Online]. Available: https://projectswiki.eleceng.adelaide.edu.au/projects/index.php/Projects:2016s1-160a_Cyber_Security_-_IoT_and_CAN_Bus_Security. [Accessed: 20-Aug-2020].

[31] “Threats Have Evolved—Has Your Security Program?” [Online]. Available: https://www.siemworks.com/Solutions-Security.asp. [Accessed: 13-Aug-2020].

[32] “WannaCry ransomware attack.” [Online]. Available: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack. [Accessed: 13-Aug-2020].

[33] J. Poppy, “The Hacker’s Economy,” 2019. [Online]. Available: https://www.bulletproof.co.uk/blog/the-hackers-economy. [Accessed: 17-Jul-2020].

[34] Digital Shadows Security Engineering Team, “The Ecosystem of Phishing : From Minnows to Marlins | Digital Shadows,” pp. 1–13, 2020.

[35] Barlclays Bank, “Digital Eagles.” [Online]. Available: https://www.barclays.co.uk/digital-confidence/eagles/. [Accessed: 13-Aug-2020].

[36] “Barclays spends £10m to tackle the ‘digital safety gap.’” [Online]. Available: https://www.itpro.co.uk/security/28618/barclays-spends-10m-to-tackle-the-digital-safety-gap. [Accessed: 25-Aug-2020].

[37] D. J. Bodeau, C. D. Mccollum, and D. B. Fox, "'Cyber Threat Modeling: Survey, Assessment, and Representative Framework'," PR 18-1174," *HSSEDI, Mitre Corp.*, no. 18, 2018.

[38] ISO27005, "BS ISO 27005: Information technology — Security techniques — Information security risk management," 2011.

[39] ISO31000, "BS ISO 31000 : 2018 BSI Standards Publication Risk management — Guidelines," BSI Stand. Publ., p. 26, 2018.

[40] R. S. Ross, "Guide for Conducting Risk Assessments," Spec. Publ. (NIST SP) - 800-30 Rev 1, no. September, p. 95, 2012, doi: 10.6028/NIST.SP.800-30r1.

[41] D. B. Fox, E. I. Arnoth, C. W. Skorupka, C. D. Mccollum, and D. J. Bodeau, "Enhanced Cyber Threat Model for Financial Services Sector (FSS): Institutions Threat Model ATT&CK/CAPEC Version," *HSSEDI, Mitre Corp.*, no. 18, 2018.

[42] D. J. Bodeau and C. D. Mccollum, "System-of-Systems threat model," *HSSEDI, Mitre Corp.*, no. 1, p. 50, 2018.

[43] "Frequently Asked Questions @ attack.mitre.org." [Online]. Available: https://attack.mitre.org/resources/faq/. [Accessed: 14-Aug-2020].

[44] "CAPEC." [Online]. Available: https://capec.mitre.org/. [Accessed: 14-Aug-2020].

[45] "FCA Cyber-Resilience." [Online]. Available: https://www.fca.org.uk/firms/cyber-resilience. [Accessed: 14-Aug-2020].

[46] NCSC."Cisp @ Www.Ncsc.Gov.Uk," 2017. [Online]. Available: https://www.ncsc.gov.uk/cisp. [Accessed: 14-Aug-2020].

[47] "Reporting a cyber security incident - NCSC." [Online]. Available: https://report.ncsc.gov.uk/. [Accessed: 14-Aug-2020].

[48] "NFIB Fraud and Cyber Crime Dashboard." [Online]. Available: https://colpolice.maps.arcgis.com/apps/opsdashboard/index.html#/60499304565045b0bce05d2ca7e1e56c. [Accessed: 14-Aug-2020].

[49] "ICO Decision notices." [Online]. Available: https://icosearch.ico.org.uk/s/search.html?collection=ico-meta&profile=decisions&query. [Accessed: 14-Aug-2020].

[50] "SANS Whitepapers @ cyber-defense.sans.org." [Online]. Available: https://cyber-defense.sans.org/resources/whitepapers. [Accessed: 14-Aug-2020].

[51] “Timeline of Cyber Incidents Involving Financial Institutions.” [Online]. Available: https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide. [Accessed: 25-June-2020].

[52] Information is Beautiful website. Available: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ [Accessed: 14-Aug-2020].

[53] T. Maurer, A. Levite, and G. Perkovich, “Toward a global norm against manipulating the integrity of financial data,” Econ. Discuss. Pap., Cyber Policy Initiative Working Paper Series, Carnegie Endowment for International Peace, March, 2018.

[54] E. D. Borghard, “Protecting Financial Institutions Against Cyber Threats : A National Security Issue,” Cyber Policy Initiative Working Paper Series, Carnegie Endowment for International Peace. September, 2018.

[55] “Financial market infrastructure supervision.” [Online]. Available: https://www.bankofengland.co.uk/financial-stability/financial-market-infrastructure-supervision. [Accessed: 15-Aug-2020].

[56] L. Kaffenberger and E. Kopp, “Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment” Cyber Policy Initiative Working Paper Series ‘Cybersecurity and the Financial System’ #4,” September, 2019.

[57] Investopedia.Com, “Brokerage-Company.” [Online]. Available: http://www.investopedia.com/terms/b/brokerage-company.asp. [Accessed: 14-Aug-2020].

[58] “APT41 Software.” [Online]. Available: https://attack.mitre.org/groups/G0096/. [Accessed: 16-Aug-2020].

[59] Bateman. J, “Deepfakes and Synthetic Media in the Financial System : Assessing Threat Scenarios,” Cyber Policy Initiative Working Paper Series “Cybersecurity and the Financial System” #7, July, 2020.

[60] “DefensorID Navigator Layer.” [Online]. Available: https://mitre-attack.github.io/attack-navigator/mobile/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fsoftware%2FS0479%2FS0479-mobile-layer.json. [Accessed: 16-Aug-2020].

[61] Steven Kemp et al., “The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain,” European Journal on Criminal Policy and Research, 2020.

[62] Phillips. G, “RHUL Thesis Investors’ Survey,” Internet survey on suveymonnkey.com. July - August 2020.

[63] “Marriott Data Breach 2020: 5.2 Million Guest Records Were Stolen.” [Online]. Available: https://securityboulevard.com/2020/04/marriott-data-breach-2020-5-2-million-guest-records-were-stolen/. [Accessed: 17-Aug-2020].

[64] “9 in 10 Financial Institutions Targeted by Ransomware.” [Online]. Available: https://invenioit.com/continuity/financial-services-ransomware/. [Accessed: 17-Aug-2020].

[65] “Protect yourself.” [Online]. Available: https://www.youinvest.co.uk/security-centre/protect-yourself. [Accessed: 21-Aug-2020].

Appendix A Part 1: Synthesised Attacks Database

Please note: due to the size of the database it is presented in two parts.

- Both parts have the same ID reference number (ID#) at the leftmost column.
- Part 1 includes columns up to and including “Threat Landscape”
- Part 2 includes columns from “Threat Source” to “What Else Do We Know about Who Did it?”
- Example: The complete record for #ID1 will be in two tables, Synthesised Attacks Database Part 1 and Synthesised Attacks Database Part 2, identified by row “#ID1”.

			Threat Scenario		**Threat Landscape**	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
1	2020	06 March 2020	Southeast Asian Banks Credit Card Breach	Over 200,000 credit card details from 'top banks' were stolen and published online.	Institution	Customers' credit card details
2	2020	25 February 2020	Australian Banks and other financial institutions DDoS Extortion	Australian banks and other financial institutions were being extorted by the Silence group with DDoS attacks unless they paid a ransom.	Institution	Banks networks
3	2020	21 February 2020	PayPal Accounts Linked to Google Play Abused	Hackers targeted PayPal accounts to carry out unauthorized purchases, estimated to be worth tens of thousands of euros, by exploiting PayPal’s Google Pay integration. The purchases were made at a variety of Target stores in the United States. Most of the victims appear to be German PayPal users.	Investor	Customers' Personal accounts used to carry out unauthorised purchases
4	2020	20 February 2020	Loqbox Data Breach	Loqbox, a UK-based credit score builder startup, was the victim of a data breach in which customer details were compromised. This included names, dates of birth, addresses, and phone numbers.	Institution	Customer details

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
5	2020	02 January 2020	Sub-Saharan African Banks Targeted	The general outline of such an attack involved phishing emails being sent with the malware, data gathering, and then withdrawing large amounts of cash in one go via ATMs.	Institution	ATM machines
6	2019	31 December 2019	Travelex Hit with Sodinokibi	Company systems were infected with Sodinokibi ransomware and the attackers demanded $6 million to remove it. This also impacted the exchange services of many major banks including Lloyds, Barclays, and RBS, who all use Travelex. The attackers also claimed to have exfiltrated 5GB of personal customer data that they threatened would be released if they did not receive payment. The attackers are believed to have used a VPN exploit that remained unpatched to access the firm's systems. As of the end of January it has taken over a month for Travelex to restore its site and even then, only partially.	Institution	Company system
7	2019	10 December 2019	Wawa Inc. Card Data Breach	On December 10, 2019, Wawa Inc., a U.S.-based convenience store chain, discovered that its payment card processing systems had been breached for a 9-month long period in which customers in any of its worldwide locations could have had their card data stolen. On January 27, 30 million card details believed to be part of the breach posted for sale online, including card numbers and expiration dates. Pins and CVV records were not exposed.	Institution	Customers' payment card details
8	2019	10 December 2019	Iranian Debit Card Breach - Iran's three largest banks	On December 10, 2019, it was reported that Mellat, Tejarat, and Sarmayeh, Iran's three largest banks, had been breached and that the attacker had published 15 million bank debit cards on social media in the aftermath of anti-government	Institution	Customers' bank debit card details

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
				demonstrations. Iran's information and telecommunications minister denied this was due to attackers but an inside contractor who had access to the data. Researchers are disputing this and suggest it was likely a nation state actor.		
9	2019	21 November 2019	Edenred Malware	On November 21, 2019, Edenred, a payment solutions provider, reported that it was infected by malware that affected a number of the organization's computers. Edenred's payment platform operates across 46 countries and in 2018 they managed 2.5 billion payment transactions. According to a statement released by the organization, as soon as the incident was detected they implemented countermeasures to prevent further infections. The number of computers effected and the extent of the attack is still currently unknown.	Infrastructure	Cannot tell, but Edenred manages payment transactions
10	2019	18 November 2019	Cayman National Bank and Trust Data Theft	On November 18, 2019, the Cayman National Bank and Trust Company confirmed it had been breached and had confidential data stolen. The Cayman National Bank did not elaborate on the extent of the breach but confirmed it was working with law enforcement. This announcement corroborated an earlier claim by Phineas Fisher, a vigilante hacker persona, who publicized the hack to encourage similar hacktivism. Phineas Fisher offered $100,000 USD to hacktivists who breach and leak documents from bank, oil companies, surveillance spyware vendors, and others.	Institution	Confidential data stolen - no further information.
11	2019	13 November 2019	Cardplanet Fraud	On November 13, 2019, the United States charged a Russian man for running 'Cardplanet,' a card trading platform worth almost $20 million USD	Infrastructure	Proxy for stolen payment card details

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
				that buys and sells stolen payment card details. He is facing a number of charges including access device fraud, identity theft, and computer intrusion.		
12	2019	16 November 2019	BriansClub Data Theft	On October 16, 2019, it was reported that 'BriansClub', one of the largest underground markets for stolen credit card and payment details, was hacked by a competitor who stole 26 million card details. The credit card data was added to BriansClub between 2015-2019, representing 30 percent of the total cards that are currently being sold on the underground market.	Infrastructure	Peoples' stolen credit card and payment details A proxy for the original 'harm'. This was theft from a thief.
13	2019	04 October 2019	Sberbank Data Leak	On October 4, 2019, it was reported that Sberbank, one of Russia's largest banks, was investigating a suspected data leak that affected at least 200 customers, and potentially data on 60 million credit cards. Sberbank is working with law enforcement to investigate the incident further.	Institution	Presumed data leak that affected at least 200 million customers, and potentially data on 60 million credit cards.
14	2019	28 September 2019	460,000 Turkish Card Details for Sale	On December 11, 2019, it was reported that 463,378 Turkish payment cards from Turkish banks had been posted for sale online between late October and late November, for an estimated total value of USD $500,000. Full card details were available as well as personal data including emails and phone numbers.	Institution	Customers' payment card details
15	2019	23 September 2019	Indian ATMs Targeted with ATMDtrack Malware	On September 23, security researchers reported that North Korean hackers had developed and inserted malware to steal payment information from Indian ATMs and banking institutions.	Institution	Customers payment information from Indian ATMs and banking institutions.
16	2019	16 September 2019	ECB BIRD Site Data Breach	On September 16, the European Central Bank (ECB) shut down its Banks' Integrated Reporting	Infrastructure	Peoples email addresses, and titles may have been accessed by hackers

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
				Dictionary (BIRD) site after routine maintenance uncovered a cyberattack compromising the information of the site's newsletter subscribers. The ECB reported that no market-sensitive data was compromised in the attack, and it planned to contact the 481 individuals whose names, email addresses, and titles may have been accessed by hackers.		
17	2019	06 September 2019	Hong Kong Exchanges and Clearing Limited DDoS Attack	On September 6, 2019, Hong Kong Exchanges and Clearing Limited (HKEx), a Hong Kong-based stock exchange, suffered a distributed denial-of-service attack (DDoS) and discovered a technical bug, forcing them to suspend trading.Although services resumed once the issues were resolved, this is the second time that HKEx has suffered an attack of this kind. In 2011 a DDoS attack forced the organizations to suspend their services, and the individual behind the attack was later sentenced to nine months in prison.	Infrastructure	Hong Kong Exchange forced to suspend trading.
18	2019	02 September 2019	Himalayan ATM Heist	On September 2, Nepalese police arrested five Chinese nationals in connection with cyberattacks that cost Nepalese banks more than 35 million rupees (over $300,000). The attackers targeted the Nepal Electronic Payment System, which was established to coordinate cash withdrawals at 17 Nepalese banks, and inserted malware that directed ATMs to process withdrawal requests without first verifying with member banks. Staff at one Nepali bank discovered the theft when ATMs began running out of cash sooner than expected and informed authorities. Police recovered 12.63 million rupees (more than $110,000) during the	Infrastructure	The Nepal Electronic Payment System; manipulated to allow cash withdrawals at 17 Nepalese banks.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
				arrests.		
19	2019	06 August 2019	Binance Ransomware	On August 6, Malta-based cryptocurrency exchange Binance became the victim of ransomware when attackers demanded 300 bitcoin (around $3.5 million at the time) in exchange for a Know Your Customer (KYC) database containing the personal information of around 10,000 users. The company contested the authenticity of the documents, claiming that they lacked digital watermarks, refused to pay the ransom, and contacted law enforcement for assistance in pursuing the attacker(s).	Institution	A Know Your Customer (KYC) database containing the personal information of around 10,000 users. The KYC database allegedly contained personal identification information and photographs of users with documents like passports.
20	2019	29 July 2019	Capital One Data Breach	On July 29, Capital One announced that it had suffered a data breach compromising the credit card applications of around 100 million individuals. Upon gaining access, the hacker posted about it on GitHub, and an unidentified individual notified Capital One about the presence of the database on GitHub. Authorities arrested one individual in connection with the data theft.	Institution	The credit card applications of around 100 million individuals. The applications contained names, dates of birth, credit scores, contact information, and some American and Canadian social security numbers.
D	**2019**	**July 2019**	**Capital One**	**Jul 2019. The massive data breach included personal information from credit card applications over a 14-year period. A former Amazon employee, Paige Thompson, awaits trial for fraud.**		**100,000,000.00**
21	2019	25 July 2019	Banco Pan Data Breach	On July 25, security researchers found a file containing 250GB of personal and financial information, mainly tied to Brazilian financial	Institution	250GB of personal and financial information exposed online. The information, which Banco Pan

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
				institution Banco Pan, exposed online.		claims is owned by a commercial partner, contained scans of identification cards and social security cards, proof of address documents, and service request forms.
22	2019	23 July 2019	Jana Bank Data Breach	On July 23, a security researcher reported that Jana Bank, an Indian small finance bank, left exposed a database containing information on millions of financial transactions. Jana Bank immediately secured the database upon learning of its exposure.	Institution	'Know Your Customer' database containing information on millions of financial transactions left exposed.
23	2019	12 July 2019	Remixpoint Inc. Crypto Theft	On July 12, Remixpoint, a Japanese cryptocurrency exchange, halted services after it discovered the theft of $32 million in digital currencies. After an error appeared in the exchange's outgoing funds transfer system, Remixpoint discovered that the funds had been taken from a "hot" wallet (one that is connected to the internet). No funds had been stolen from "cold" wallets (those not connected to the internet). The company promised to investigate the incident and provided no further details.	Institution	Funds had been taken from a "hot" wallet (one that is connected to the internet)
24	2019	25 June 2019	Crypto Exchange Theft	On June 25, Europol, British law enforcement, and Dutch law enforcement officials arrested six individuals for cryptocurrency theft amounting to €24 million (over $26 million).	Institution	Online cryptocurrency exchange attacked. Money stolen from people. The attack affected more than 4,000 individuals in at least 12 countries.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
25	2019	22 June 2019	Bangladesh Switch System Cyberattack	In June 2019, at least three private Bangladeshi banks were compromised by major cyberattacks, with one, Dutch Bangla Bank Limited (DBBL), losing as much as TK 25 crore (around $3 million). NCC Bank and Prime Bank were also targeted, but both banks reported no financial losses associated with the attack.	Infrastructure	DBBL's Switch payment management system
26	**2019**	**June 2019**	**Desjardins Group**	**June 2019. An employee of the Canadian financial firm leaked customer information outside the organisation: names, addresses, birthdates, social insurance numbers & transaction habits.**	**Institution**	**4,200,000**
27	2019	24 May 2019	First American Financial Corp.	On May 24, First American Financial Corp. suffered a data breach compromising around 885 million files related to mortgage deeds. Although the company took down the website, many of the pages remained accessible on archive.org. As of August 2019, the U.S. Securities and Exchange Commission had begun an investigation into the data breach.	Institution	Around 885 million files related to mortgage deeds. The documents, which dated back as far as 2003, contained bank account numbers and statements, mortgage and tax records, social security numbers, wire transaction receipts, and images of drivers' licenses.
D	**2019**	**May 2019**	**First American Financial Corporation**	**May 2019. Anyone with a web browser could access these First American insurance documents dating back to 2003. Bank details, mortgage & tax records, social security numbers, drivers license images.**		**885,000,000.00**

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
28	2019	16 May 2019	GozNym Gang Arrested	On May 16, 2019, Europol, the U.S. Department of Justice (DoJ), and six other countries, dismantled a group of international cyber criminals that used the GozNym malware to steal over $100 million. Following a law enforcement investigation across the U.S., Bulgaria, Germany, Georgia, Moldova, and Ukraine, ten members were charged for the crime. Although some members of the gang are still on the run, the initial charges have been seen as a success for law enforcement in their efforts to combat international cybercrime.	Investor	The group stole from over 40,000 victims, including the bank accounts of small businesses, law firms, international corporations, and nonprofit organizations.
29	2019	13 May 2019	FirstBank Breach	In May 2019, a Colorado bank suffered an external security incident resulting in the cancellation and redistribution of customer debit cards. FirstBank, Colorado's largest locally-owned bank, issued a security notice on May 13 informing customers of the breach and instructing them to report any suspicious behavior.	Institution	'An external security incident' involving customers' debit cards.
30	2019	02 May 2019	Retefe Malware Resurfaces in Germany and Switzerland	In May, U.S. security company Proofpoint reported the return of the Retefe banking Trojan in Germany and Switzerland. In the past, Retefe campaigns have targeted several European countries. In November 2016, Retefe **targeted Tesco Bank and other UK financial institutions.** In September 2017, an updated version of Retefe leveraged the EternalBlue exploit in a campaign against Swiss targets. Since April, the Trojan has reemerged in German and Swiss banks.	Institution	Unknown. Incident only reports 'return' of a banking trojan software.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
31	2019	04 April 2019	Romanian ATM Skimmer Gang Arrested in Mexico	On March 31, Mexican law enforcement arrested two senior members of a Romanian cyber criminal group allegedly behind an ATM skimming operation in Mexico.	Investor	Peoples' PINs and card data was stolen remotely through ATMs.
32	2019	22 March 2019	Royal Bank of Scotland Security Flaw	In early 2019, the Royal Bank of Scotland's (RBS) customer accounts were exposed to a security flaw after introducing a new customer security service. Hedimal Security has since released an update to fix the security flaw and insisted that only 50,000 computers were effected. They claim that there were no intrusions as a result of the security flaw.	Institution	Customer accounts were exposed to a security flaw. Researchers discovered a software flaw that enabled access to customer emails, banking details and internet history.
33	2019	12 March 2019	Ursnif Malware Attack on Japanese Banks	Between 2016 and 2017, researchers at Palo Alto Networks observed millions of infected emails sent to banks in Japan.	Institution	Infected emails.
34	**2019**	**February 2019**	**Coinmama**	**Feb 2019. Part of the theft of 127 million online account details from 8 hacked websites. They were put up for sale on the dark web 1 week after a similar tranche of 617 million records from 16 other websites.**	**Institution**	**450,000**
35	2019	13 February 2019	Bank of Valletta	On February 13, the Bank of Valletta (BOV), Malta's largest and oldest bank, shut down operations after an attempted theft of €13 million. The bank's employees discovered the fraudulent activity during their daily reconciliation of international orders. In a statement, BOV said it was working with local and international police authorities to track down the attackers.	Infrastructure	Transfer requests amounting to attempted theft of €13m. The bank shut down operations to prevent the theft. Within the hour, BOV notified other banks in an attempt to freeze the transactions. It also closed all its branches, shut down its ATMs and point-of-sale system, and stopped all other electronic services, which were restored the following day.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
36	2019	08 February 2019	U.S. Credit Union Spear-Phishing	Multiple credit unions in the United States were hit by spear-phishing emails impersonating compliance officers from other credit unions. Under the Bank Secrecy Act (BSA), financial institutions are required to have dedicated compliance personnel responsible for reporting suspicious transactions and potentially fraudulent activity to the U.S. government. Emails sent to these compliance officers contained a PDF with a malicious link. While it is believed that no employee clicked the link, there is speculation as to how the attackers obtained the email addresses of the compliance officers.	Institution	Emails sent to Credit Unions' compliance officers contained a PDF with a malicious link. Purpose of link not stated.
37	2019	04 February 2019	SBI Breach	The State Bank of India, the country's largest, has denied claims that its servers were compromised during a recent intrusion. Despite the claims, the bank said their investigation revealed that SBI's servers remained fully protected and that no breach had occurred.	Institution	Multiple media outlets reported an SBI server was unprotected, and as a result attackers were able to gain access to the system and steal users' personal information.
38	2019	02 February 2019	Metro Bank 2FA Breach	UK-based Metro Bank became the first major bank to suffer from a new type of cyber intrusion that intercepts text messages with two-factor authentication codes used to verify various customer transactions. A spokesperson for the bank stated that only a small number of those defrauded were Metro Bank customers.	Investor	Text messages intercepted, despite two-factor authentication verification.
39	2019	10 January 2019	Chile ATM Attack	In December, hackers infiltrated Chile's ATM interbank network, Redbanc. Redbanc claims the event had no impact on its business operations.	Infrastructure	Redbanc, ATM interbank network infiltrated.
40	2019	10 January 2019	Fuze Cards	The U.S. Secret Service has identified a number of	Investor	Credit cards of personal customers,

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
				criminal rings turning to Fuze cards in an attempt to avoid detection by U.S. law enforcement.		using a new form of 'multiple' credit card.
41	2018	23 December 2018	Evercore Breach	In November, hackers breached Evercore gaining access to thousands of sensitive documents from the **global investment bank**. A source at the bank believes the motivation for the breach was to access the administrator's address book to send more phishing emails. The source also claims no data had been misused in result of the breach.	Institution	Company data including documents, diary invitations, and emails.
42	2018	18 December 2018	Government Payment Portals	In August 2017, **Click2Gov**, an online bill-payment portal used to pay for local government services in the United States, was the victim of a data breach. Threat intelligence firm Gemini Advisory discovered that several users' card details were sold on the dark web for approximately £10. Gemini identified 294,929 compromised payment records, resulting in at least $1.7 million in earnings for the criminals.	Institution	Not stated but the breach exposed customer data including payment card details and log-in credentials of users in over forty U.S. cities.
D	**2018**	**December 2018**	**Click2Gov**	**Dec 2018. Vulnerabilities in government payment software allowed hackers to access financial records and personal data across 46 US cities.**		**300,000.00**
43	**2018**	**September 2018**	**GovPayNow.com (Government Payment Service Inc)**	**Sep 2018. A company used by US government agencies to accept online payments exposed personal records via a standard web browser, including addresses, phone numbers and credit card digits.**		**14,000,000.00**

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
44	2018	13 December 2018	Brazilian Mobile Malware	In mid-December, a report revealed that over 2,000 mobile banking users in Brazil downloaded an Android-based Trojan through Google Play applications. Reports suggest that the malware also targeted apps such as Uber, Netflix, and Twitter using phishing tactics.	Investor	Mobile banking app. Victims unknowingly downloaded the malware, allowing attackers to gain access to user devices and data.
45	2018	11 December 2018	ThreadKit Exploit	Executed phishing schemes utilizing Microsoft Office documents. Used the Threadkit exploit. APT group 'Cobalt' attributed.	Institution	Not stated
46	2018	06 December 2018	Eastern European Banks Targeted From the Inside	In 2017 and 2018, eight banks in Eastern Europe were targeted by attackers who connected electronic devices directly to the banks' infrastructure. The attacks are believed to have caused tens of millions of dollars in damages.	Infrastructure	Once they gained access to the target bank's infrastructure, the attackers scanned its networks to collect valuable information, such as account details for making payments.
47	2018	14 November 2018	Rapid Raids Jackpotting	Hackers installed malicious software or hardware on ATMs. From February to March, the duo stole $125,000 from four ATMs in Indiana, Kentucky, Wisconsin, and most recently Michigan, where they were apprehended.	Institution	ATM machines
48	2018	06 November 2018	HSBC U.S. Breach	In November, HSBC reported that hackers had gained access to customer data. When HSBC discovered the compromised accounts, they suspended online access for affected customers to prevent further entry to the accounts. At the time of release, HSBC did not provide details on the number of customers	Institution	Customer data accessed including names, addresses, phone numbers, and account details. Online access to accounts was suspended so possibly they were being robbed.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
				affected. However, claims estimate that less than 1 percent of the bank's U.S. online accounts were potentially compromised.		
49	2018	02 November 2018	Magecart Payments Breach	In early November, Lloyds Banking Group and other UK banks were forced to replace payment cards after the breach of numerous retail sites. Websites for retailers, including Ticketmaster and British Airways, were manipulated to skim card information from hundreds of thousands of customers using the Magecart toolset.	Investor	Retail sites, allowing skimming from customers
50	2018	29 October 2018	Bank Islami	The bank uncovered suspicious transactions from payment cards outside of Pakistan and immediately shut down its international payment scheme. The bank confirmed that around 2.6 million Pakistani rupees (roughly $19,500) were withdrawn from customer accounts. Following the incident, the State Bank of Pakistan (SBP) issued directives to all banks, encouraging them to ensure the security of all payment cards and monitor card activity on a real-time basis.	Investor	Cyber attack on the bank's international payment card network. Breach of payment card system. Money stolen from customer accounts.
51	2018	27 October 2018	Pakistan Data Theft	On October 27, cybersecurity firm Group-IB reported a spike in sales of card details from Pakistani customers on Joker's Stash, a popular online marketplace for stolen information. Group-IB identified more than 150,000 card details from at least three Pakistani banks. The Pakistani Federal Investigation Agency revealed that almost all the nation's banks had been affected. However, the State Bank of Pakistan has disputed the scale of the incident.	Institution	Breach of payment card system. Card details being sold on darkweb.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
52	2018	23 October 2018	AXA Targeted in Mexico	On October 22, 2018, unknown hackers attacked insurance firm AXA, causing problems to the SPEI interbank payment matching system. This incident prompted Mexico's central bank to raise the security alert level on its payments system. AXA reported no client information or money was affected by the incident.	Infrastructure	SPEI interbank payment matching system
53	2018	02 October 2018	State Bank of Mauritius	In October 2018, the Indian subsidiary of the State Bank of Mauritius was targeted by attackers who attempted to steal $14 million through compromised IT systems. The bank managed to recover $10 million in the days following the attack and said no customers would lose money as a result.	Infrastructure	Compromised IT systems
54	2018	05 September 2018	Silence	First reported in 2018, Russian-speaking hackers, dubbed Silence by researchers at Group IB, targeted Russian banks, stealing $550,000 within a year.	Institution	ATM machines
55	2018	17 August 2018	Banco de la Nacion	Over the weekend of August 17–19, 2018, an attack took place on Peruvian banks that forced at least one bank to take down its internet banking services and some card transactions. There were reports that a new strain of ransomware was involved. The extent of the damage done remains unclear, but there were no indications in the weeks afterward that the attack targeted payment systems, or was a smokescreen for other activity.	Institution	Internet banking services and some card transactions taken down.
56	2018	11 August 2018	Cosmos Bank SWIFT Heist	In August 2018, it was reported that Cosmos Bank, the second-biggest cooperative bank in India, lost $13.5 million through ATMs in twenty-eight countries as well as through unauthorized	Institution	ATM machines Unauthorised interbank transactions (SWIFT)

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
				interbank transactions. The attack left Cosmos's online banking service offline for more than a week, and the funds have not been recovered. There were signs that an attack on a bank was coming. Two days before the incident, the FBI issued a warning to banks about an imminent ATM cash-out scheme, without providing further public details.		Stolen Cards
57	2018	24 July 2018	National Bank of Blacksburg	In May 2016 and January 2017, the National Bank of Blacksburg, based in the state of Virginia, was hit by phishing emails that enabled intruders to install malware and pivot into the Star Network, a U.S. bank card processing service. The 2017 attack gave wider access to bank networks and enabled the thieves to withdraw $1.8 million over the course of a weekend, taking total losses to $2.4 million.	Institution	The Star Network, a U.S. bank card processing service. Also ' wider access to bank networks'.
58	2018	19 July 2018	PIR Bank Attacked	On July 3, 2018, attackers targeted Russia's version of the SWIFT interbank network, the Automated Workstation Client, to siphon around $1 million from PIR Bank.	Infrastructure	Russia's version of the SWIFT interbank network, the Automated Workstation Client
59	2018	28 May 2018	Data Breach Involving Canadian Banks	In 2018, it was revealed that up to 90,000 clients of the Canadian banks Simplii and Bank of Montreal (BMO) had been exposed by a data breach that the organization blamed on unidentified fraudsters. Bank of Montreal said there was a threat to make the data public from the group, which it thinks is behind the thefts from both banks. Simplii and BMO are now facing a class action lawsuit, with those involved arguing that the banks failed to properly protect sensitive	Institution	Not stated. Presumably bank servers.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
				information.		
60	2018	24 May 2018	Banco de Chile Incident	In May 2018, Banco de Chile suffered a $10 million theft. Added to the growing ranks of Latin American banks suffering cyber attacks.	Infrastructure	
61	2018	12 May 2018	Mexican Bank Theft	Banco de Mexico warned a dozen banks to upgrade their security following $15 million in fraudulent cash withdrawals from five institutions linked to the central bank's electronic payments system, SPEI. The investigators have not made clear whether each victim bank was compromised, or whether the attackers moved between them following the initial breach. It is also unclear whether the gang had insider help to clear large transactions through the banks' security checks. The incidents delayed legitimate transfers but the central bank said client money and the SPEI infrastructure were unaffected. Following the thefts, Banco de Mexico set up a new cybersecurity unit and asked its members to move to an in-house, encrypted software with SPEI. The incident came five months after Bancomext, the state-owned trade bank, blocked attempts to siphon off $110 million via a compromise in the network that granted attackers access to the global SWIFT interbank system.	Infrastructure	Institutions linked to the central bank's electronic payments system, SPEI.
62	2018	01 April 2018	DDoS-for-Hire	In April 2018, it was revealed that authorities in five countries worked together to take down	Institution	

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
				Webstresser, a DDoS-for-hire site The site was used to launch a coordinated attack on seven UK banks in November 2017, according to the UK's National Crime Agency.		
63	2018	23 March 2018	Mabna Iranian Hack on the United States	Two financial firms were among the various U.S. targets of a hacking group operating under the guise of the Mabna Institute, which used password spraying to access information.	Institution	The actors are accused by the United States of stealing 31 terabytes of academic and commercial information in a campaign dating as far back as 2013.
64	2018	18 February 2018	City Union Bank SWIFT Attack	In February 2018, City Union Bank in India suffered a breach that allowed $1 million to be transferred to a Chinese institution. The attackers tried to make three transactions totaling $2 million, sending money to Dubai and Turkey, but were thwarted by City Union Bank and the corresponding bank on the receiving end of the transfer. Two years earlier, attackers attempted but failed to make a $170 million SWIFT transfer out of the Union Bank of India.	Infrastructure	SWIFT money transaction system was the mechanism.
65	2018	07 February 2018	Infraud Gang	The Infraud Organization, law enforcement officials say sells stolen personal and financial information. More than half a billion dollars was lost by the victims, the U.S. Department of Justice said, with a trail going back to October 2010.	Infrastructure	Customers were victims of fraud. Multple means used to steal around half a billion dollars.
66	2018	29 January 2018	Dutch DDoS Attack	In January, ABN Amro, Rabobank, and ING suffered disruptions to online and mobile banking services, while the Dutch tax authority website was taken down for several minutes.	Institution	Disruptions to online and mobile banking services The Dutch tax authority website was taken down for several minutes.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
67	**2018**	**2017**	**Mount Olympus (mortgage lender)**	**A former employee of Mount Olympus Mortgage stole client information and loan files and took them with him when he went to work at Guaranteed Rate. Mount Olympus was awarded $25m in damages.**	**Institution**	**188,000**
68	2017	01 December 2017	Youbit Hacked	The attack in December led to the loss of 17 percent of Youbit's digital currency and forced it to stop trading. The thefts came weeks after a $70 million bitcoin heist at NiceHash, a cryptocurrency mining service in Slovenia, at a time when the price of the currency had soared above $15,000.	Institution	Cryptocurrency stolen. The bitcoin exchange Youbit was hacked twice in 2017, forcing it to file for bankruptcy.
69	**2017**	**December 2017**	**TIO Networks (Owned by Paypal)**	**Dec 2017. The company has not revealed what type of information was stolen.**	**Institution**	**1,600,000**
70	2017	05 November 2017	Paradise Papers	The Paradise Papers, covering the law firm Appleby's business as far back as 1950, shone a light on offshore tax affairs in thirty jurisdictions, including Bermuda and the Cayman Islands, the heart of the global hedge fund industry.	Institution	Not stated. In November 2017, an unknown whistle-blower leaked a trove of secret records on offshore companies to the German newspaper Süddeutsche Zeitung, which shared the details with 380 journalists around the world.
71	2017	01 October 2017	Far Eastern International Bank	In October 2017, Far Eastern International Bank in Taiwan became the victim of a $14 million theft. Most of the stolen money was recovered, and two men were arrested in Sri Lanka after they attempted to withdraw funds.	Infrastructure	hackers planted malware in the company's systems to access a SWIFT terminal, which was then used to make fraudulent transfers.
72	2017	21 September 2017	SEC Edgar Hack	The commission did not realize the intrusion, which took place in 2016 through a software vulnerability in a test filing component, could have leaked company secrets until August 2017.	Infrastructure	The Securities and Exchange Commission announced in September 2017 that hackers might have accessed inside information from the Edgar database, which contains market-

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
						sensitive filings for companies listed on U.S. stock exchanges, and used it to make illegal profits on share trades.
D	**2017**	**September 2017**	**Equifax**	**Sep 2017. If you have a credit report, there's a good chance that you're one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies.**	**Institution**	**143,000,000.00**
73	2017	07 September 2017	Equifax Hack	Equifax has spent $439 million on redressing the data loss and, a year after disclosure, its share price remained below the pre-breach level. However, the company has avoided fines from the banking regulators in eight U.S. states after agreeing to a deal in June 2018 to improve its cybersecurity oversight. The indictment states that the attackers were targeting the private data of millions of Americans, along with Equifax trade secrets, such as 'data compilations and database plans'.	Institution	More than 150 million customer records had been compromised, including some sensitive data such as birth dates and 12,000 U.S. social security numbers.
74	**2017**	**April 2017**	**Wonga**	**Apr 2017. Customers from the UK and Poland look to have been affected.**	**Institution**	**270,000**

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
75	2016	02 December 2016	Russian Banks DDoS Attack	In December 2016, after a number of DDoS attacks on Russian banks throughout the previous month, the Russian Federal Security Service (FSB) announced that it had discovered pending cyber attacks intended to impact a range of major Russian banks. On December 9, Rostelecom, Russia's telecom operator, said in a statement that it had blocked DDoS attacks against the five biggest banks and financial institutions in Russia on December 5. The FSB stated that it expected the DDoS attacks to be accompanied by text messages, agitating social network publications, and blog statements about a "crisis in the Russian credit and financial system, bankruptcy and withdrawal of licenses of leading federal and regional banks," and that "the campaign [would be] directed against several dozen Russian cities." Presumably, this would be an attempt to create a run on Russian banks, initiating a financial crisis. No evidence exists that such action, complementary to the DDoS attacks, was attempted.	Institution	Attack failed. In December 2016, after a number of DDoS attacks on Russian banks throughout the previous month, the Russian Federal Security Service (FSB) announced that it had discovered pending cyber attacks intended to impact a range of major Russian banks.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
76	2016	01 December 2016	Insider Trading Hack	In late 2016, the Securities and Exchange Commission (SEC) sued three Chinese traders, arguing that they had installed malware on the networks of two law firms to steal confidential, market-moving information on mergers and acquisitions.	Infrastructure	Confidential, market-moving information on mergers and acquisitions.
77	2016	05 November 2016	Tesco Bank Card Theft	Tesco Bank, a retail bank based in the UK, was the target of thieves who used vulnerabilities in its card issuing process to guess bank card numbers and steal £2.26 million in November 2016. Tesco Bank halted all online and contactless transactions after a day of struggling to block all the fake purchases reported in the United States, Spain, and Brazil. In October 2018, Tesco was fined £16.4 million by the UK's Financial Conduct Authority for deficiencies in its bank card policies and its response to the incident.	Investor	Customers bank cards. Almost 9,000 accounts were affected, or 6.6 percent of the bank's entire customer base. One customer had twenty-two fraudulent transactions totaling £65,000 on his account. Visa and Mastercard had both previously warned of an increase in the type of fraud seen in this case, which used the magnetic strip to verify the transaction. On November 5, 2016, as the weekend began, the gang started making fraudulent transactions with the card details it had calculated.
78	2016	20 October 2016	Indian ATM Breach	In mid-2016, a number of Indian banks replaced or changed security codes on 3.25 million debit cards after uncovering a breach in Hitachi's payment switch systems, which link into the ATM network. Visa, Mastercard, and India's Rupay cards were all affected by the compromise.	Infrastructure	3.25m Consumers debit cards.
79	2016	04 May 2016	Central Banks DDoS Attack	In May 2016, hacktivists briefly took down the Bank of Greece's website, and later did the same to the central banks of Mexico, Panama, Kenya, and Bosnia and Herzegovina.	Institution	Varous central banks sites 'taken down'.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
80	2016	03 April 2016	Panama Papers	In April 2016, an anonymous source leaked 2.6 terabytes of information from the Panamanian law firm Mossack Fonseca to the German newspaper Süddeutsche Zeitung. The revelations had far-reaching effects, including the resignation of the Icelandic prime minister, a number of tax evasion investigations, and the closure of Mossack Fonseca.	Institution	The journalists shared the 11.5 million leaked documents with a dozen global news organizations to simultaneously print stories about the money-laundering, tax affairs, and financial secrecy within.
81	2016	22 February 2016	Belgian National Bank Incident	On February 22, 2016, a hacking group called DownSec Belgium shut down the website for Belgium's National Bank for most of the morning using DDoS attacks.	Institution	Bank's web site shut down for a morning.
82	2016	01 February 2016	Bangladesh Bank SWIFT Hack	In February 2016, media outlets reported that hackers had breached the network of the Bangladesh central bank and sent thirty-five fraudulent transfer requests to the Federal Reserve Bank of New York, totaling nearly $1 billion. Four of these fraudulent requests succeeded, and the hackers were able to transfer $81 million to accounts in the Philippines, representing one of the largest bank thefts in history. A fifth request for $20 million to be sent to an account in Sri Lanka was stopped due to the recipient's name, Shalika Foundation, being misspelled "fandation." The remaining transfers, which totaled somewhere between $850 and $870 million, were also stopped before they could be completed due to a stroke of good fortune: the name of the destination bank branch included the word "Jupiter," which was the name of an unrelated company on a sanctions blacklist.	Infrastructure	SWIFT money transaction system was the mechanism. The Bangladesh central bank's server. The intruders had monitored the bank's routine activity in order to create money transfer requests that appeared genuine. Furthermore, they timed the thefts so that it would be the weekend in Bangladesh when the Federal Reserve reached out to confirm the transactions, and then it would be the weekend in New York when the Bangladesh central bank employees instructed the Federal Reserve to cancel the transactions.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
83	**2015**	**December 2015**	**Invest Bank (United Arab Emirates bank)**	**Dec 2015. Hacker breached a United Arab Emirates bank, demanding a ransom of $3m in bitcoin to stop tweeting data, mostly about corporate accounts. The hacker dumped files on the website of a basketball team, which he hacked for storage. The bank, Invest Bank, won't pay the ransom.**	**Institution**	**40,000**
84	2015	30 November 2015	Greek Banks DDoS Attack	In late 2015, hackers threatened to disable systems at three Greek banks unless they paid a bitcoin ransom. When the banks refused, they had their sites repeatedly knocked out for several hours.	Institution	Greek banks' web sites.
85	2015	06 November 2015	Swedbank and Nordea DDoS Attack	In November 2015, a teenager was sentenced to community service after carrying out four DDoS attacks against Nordea and Swedbank. The attacks blocked customers from the banks' websites for hours at a time.	Institution	Bank websites.
86	2015	12 June 2015	Shanghai Composite Index Suspected Manipulation	Beginning on June 12, 2015, the Shanghai Composite Index began to plummet, and by June 19 it had fallen by 13 percent. Chinese stock markets continued to fall throughout July and August, and again in January and February 2016. Although there is no public evidence, some have speculated that the initial sudden crash may have been caused by a cyber attack.	Infrastructure	A stock exchange, the Shanghai Composite Index
87	2015	15 May 2015	Tien Phong Commercial Joint Stock Bank	In May 2015, the Vietnamese bank Tien Phong announced it had blocked a fraudulent SWIFT transaction worth €1m several months before attackers successfully stole from the Bank of Bangladesh using the same method. Tien Phong did not name the bank that had been the source of	Infrastructure	SWIFT money transaction system was the mechanism.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
				the fraudulent transfer request.		
88	2015	02 April 2015	Dyre Wolf Campaign	In April 2015, a threat group twinned malware with a sophisticated social engineering tactic to steal more than $1 million from businesses.	Investor	Consumers - via emails. Credentials harvested and money stolen.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
89	2015	04 February 2015	Health Insurer Hacks	In February 2015, reports indicated that records for almost 80 million customers were stolen from Anthem, a U.S. healthcare insurer. The stolen data was taken over the course of several weeks and included personal information, such as social security numbers. The California Department of Insurance pointed to a national government as the likely culprit for the attack, and suggested the initial breach occurred in February 2014, meaning Anthem was exposed for a year before the compromise was discovered. Anthem ended up settling a lawsuit relating to the data loss for $115 million. Several weeks after the incident was disclosed, fellow insurer Premera Blue Cross announced that around 11 million customer accounts had been compromised by attackers, and rival CareFirst admitted 1.1 million current and former members may have had their information stolen. Some researchers believe the thefts were carried out by the same group. In September 2015, Excellus announced a data loss, with 10 million customers' data exposed by a breach that initially occurred in December 2013.	Institution	Health records of around 80 million customers of Anthem healthcare insurers.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
90	2015	12 January 2015	Ecuadorian Banco del Austro	In January 2015, thieves transferred $12 million out of Banco del Austro and routed most of the proceeds to twenty-three companies registered in Hong Kong. The same method has been used in several thefts in the preceding years including the $81 million Bank of Bangladesh heist in 2016. Banco del Austro said it recovered around $2.8 million of the stolen money. The heist came to light in a lawsuit Banco brought against Wells Fargo, which it alleged failed to spot red flags when it approved the fraudulent transaction. The litigation was settled in February 2018 but no details were disclosed.	Infrastructure	SWIFT money transaction system was the mechanism.
91	2015	01 January 2015	Metel Malware Attack on Russian Banks	The Metel banking Trojan, which was discovered in 2011, was repurposed by a criminal gang in 2015 to steal directly from bank ATMs and even manipulate the Russian exchange rate. In February 2015, Energobank fell victim to a Metel infection that allowed attackers to place some $500 million in currency orders, sending the ruble swinging with extreme volatility between 55 and 66 rubles per dollar for a period of fourteen minutes. However, there is no evidence the attackers profited from the movement. Metel had infected 250,000 devices and more than 100 financial institutions in 2015, according to researchers at Group IB.	Infrastructure	Money stolen from ATMS. Russian exchange rate was manipulated.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
92	2014	07 October 2014	Tyupkin ATM Malware	October 2014	Institution	Criminals had written malware to infect Windows-based ATMs and steal millions from machines primarily in Eastern Europe.
93	2014	01 October 2014	Warsaw Stock Exchange Breach	In October 2014, a group claiming to be affiliated with the so-called Islamic State hacked the internal networks of the Warsaw Stock Exchange and posted dozens of login credentials for brokers online.	Institution	Login credentials for brokers were posted online
D	**2014**	**October 2014**	**JP Morgan Chase**	**Oct 2014. The US's largest bank was compromised by hackers, stealing names, addresses, phone numbers and emails of account holders. The hack began in June but was not discovered until July, when the hackers had already obtained the highest level of administrative privilege to dozens of the bank's computer servers.**		**76,000,000**
94	2014	01 August 2014	JPMorgan Chase Data Breach	JPMorgan discovered the breach after reportedly finding the same group on a website for a charity race that it sponsors. The size of the incident prompted the National Security Agency and the FBI to join the investigation. A Russian national was extradited from Georgia to the United States in September 2018, although he denied that he was the central hacker in the attacks. The federal authorities in New York said the man worked with an international syndicate from 2012 to 2015 to steal customer information, which was used in numerous crimes including a spam email campaign to **falsely tout stocks and shares to ramp up the price.**	Institution	Account information and home addresses for 83 million customers were exposed after attackers stole login credentials from a JPMorgan Chase employee. Other companies targeted in the attacks included **Dow Jones, Fidelity, E*Trade, and Scottrade**. The U.S. authorities believe the harvested information was used in securities fraud, money laundering, credit-card fraud, and fake pharmaceuticals.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
95	2014	24 July 2014	European Central Bank	The ECB said most of the stolen data was encrypted, and no internal systems or sensitive market data had been compromised as the database was separate to those systems. The bank informed the German police, although no further information is available about the investigation.	Infrastructure	A database holding email addresses and other contact data submitted by people registering for events at the bank. Approximately 20,000 people had their information exposed in non-encrypted form.
D	**2014**	**July 2014**	**European Central Bank**	**Jul 2014. The ECB received an anonymous call requesting money in return for the stolen data. The bank didn't say how much the blackmailer asked for, but did say that it refused to pay anything.**		**4,000,000.00**
96	2014	08 July 2014	Ukrainian Bank Data Breach	It is believed that CyberBerkut targeted PrivatBank because the bank's co-owner, Igor Kolomoisky, had offered a $10,000 bounty for the capture of Russian-backed militants in Ukraine. The group warned PrivatBank customers to transfer their money to state-owned banks.	Institution	In July 2014, the pro-Russian group called CyberBerkut hacked into PrivatBank, one of Ukraine's largest commercial banks, and published stolen customer data on VKontakte, a Russian social media website.
97	**2014**	**January 2014**	**Korea Credit Bureau**	**Jan 2014. An employee from personal credit ratings firm Korea Credit Bureau (KCB) has been arrested and accused of stealing the data from customers of three credit card firms while working for them as a temporary consultant.**	**Infrastructure**	**20,000,000**
98	2013	19 December 2013	People's Bank of China DDoS Attack	In December 2013, the People's Bank of China (PBOC) was bombarded with DDoS traffic. The week before the attack, PBOC had warned that bitcoin was "not a real currency" and that Chinese institutions would not accept bitcoin deposits. With China the largest source of bitcoin trading at the time, the announcement sent the	Institution	Not stated. Presumably bank servers.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
				value of the currency down by around 40 percent.		
99	**2013**	**October 2013**	**Court Ventures (Experian)**	**Oct 2013. A lawsuit against the Vietnamese identity theft service contends that the theft of up to 3 million records began in 2010 and was orchestrated by a then-teenager in Vietnam, Hieu Minh Ngo. Ngo, posing as private investigator based in Singapore, gained access to a database of consumer information. He has since been sentenced to 13 years in prison.**	**Institution**	**200,000,000**
100	2013	01 September 2013	Ploutus Malware	In September 2013, the malware Ploutus was built to be installed directly on ATMs in order to give an attacker privileged rights, including the ability to dispense cash on demand via SMS or using a keyboard attached to the machine. Ploutus has resulted in numerous attacks in Mexico and later other countries, including the United States.	Institution	ATM machines.
101	2013	01 July 2013	CME Group	In July 2013, CME Group, which operates the world's largest futures exchange, announced in November 2013 that its ClearPort **clearing service** had been compromised the previous July.	Infrastructure	The firm said some customer information was compromised but that trading was not affected. While large financial firms are generally under no obligation to make data breaches public, the company informed affected customers and announced that it was working with the authorities.
102	**2013**	**July 2013**	**NASDAQ (Nasdaq OMX Group)**	**Jul 2013. Nasdaq forum website hacked by hacking ring, email addresses and passwords compromised**	**Infrastructure**	**500,000**

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
103	2013	01 June 2013	Carbanak Malware	In 2013, the source code for the Carbanak banking Trojan was leaked online. Since then, the malware has been used by several gangs to steal from dozens of financial institutions. The attack strategies have changed many times in order to avoid detection. Fin7, the most prolific group using Carbanak, has stolen more than €1 billion from banks in more than thirty countries over the past three years, according to Europol. The United States claims the group stole the details of 15 million payment cards by attacking more than 120 U.S. companies, including the Chipotle and Arby's restaurant chains. Another Trojan, which is named Odinaff and bears a resemblance to Carbanak, was spotted attacking banking, trading, and payroll companies in 2016. It is unclear whether this is the work of Fin7 or another gang. While Fin7 appears to have gone quiet, it is unclear whether this is because activity stopped following the arrests or its techniques have changed again.	Institution	ATM fraud Payment cards Not stated - banking, trading, and payroll companies

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
104	2013	20 March 2013	South Korea Attacked III	In March 2013, almost exactly two years since the last DDoS attack on South Korea, the Shinhan, Nonghyup, and Jeju banks were targeted by a Trojan that deleted data and disrupted ATMs, online banking, and mobile payments. After six months of attacks, South Korean politicians said this wave cost the country almost $650 million in economic damage, making it far larger than the two previous campaigns.	Institution	Banks networks - ATMs, online banking, and mobile payments.
105	2013	19 February 2013	Bank of the West DDoS Attack	On Christmas Eve 2013, Bank of the West was the victim of a DDoS attack used to disguise $900,000 in fraudulent transfers out of accounts belonging to Ascent Builders, a Californian construction firm.	Infrastructure	
106	2012	18 September 2012	Operation Ababil	In September 2012, a group called the Cyber Fighters of Izz ad-Din al-Qassam launched several waves of DDoS attacks against U.S. financial institutions. Naming the campaign Operation Ababil, the group justified their attacks as retribution for an anti-Islam video released by the U.S. pastor Terry Jones. The campaign launched two additional waves of attacks on December 10, 2012, and March 5, 2013.	Institution	Not specified. Just 'US financial institutions'.
107	2012	25 June 2012	Operation High Roller	In June 2012, U.S. security researchers uncovered a fraud ring attempting to execute high-value transactions worth between €60 million and €2 billion by using a customized Trojan spyware tool. Its targets were chiefly high-balance bank	Investor	'High-balance' bank accounts in Europe

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
				accounts in Europe.		
108	2012	04 June 2012	Shanghai Composite Index Suspected Manipulation	In June 2012, the Shanghai Composite Index saw a severe drop on the anniversary of the Tiananmen Square massacre of 1989. The Chinese censors blocked online references to the Shanghai Composite Index and several other terms on the anniversary.	Infrastructure	
109	2012	16 April 2012	Iranian Banking Data Breaches	In April 2012, a security researcher, Khosrow Zarefarid, dumped online the names, card numbers, and PINs of 3 million people across twenty-two Iranian banks after his reports on vulnerabilities were ignored by the companies involved. Google took down the blog containing the information, and the banks urged customers to change their PINs.	Institution	The names, card numbers, and PINs of 3 million people across twenty-two
D	**2012**	**April 2012**	**Three Iranian banks (Saderat, Eghtesad Novin, & Saman)**	**Apr 2012. After finding a security vulnerability in Iran's banking system, software manager Khosrow Zarefarid wrote a formal report and sent it to the CEOs of all the affected banks across the country. When the banks ignored his findings, he hacked 3 million bank accounts, belonging to at least 22 different banks, to prove his point.**		**3,000,000.00**
110	2012	01 February 2012	U.S. Financial Exchange DDoS Attacks	In February 2012, financial exchange operators Nasdaq, CBOE, and BATS were hit by DDoS attacks for several days, resulting in patchy access to company websites but with no disruptions to trading.	Infrastructure	

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
111	2012	30 January 2012	Brazil Banks DDoS Attacks	In January 2012, the hacktivist collective Anonymous used DDoS attacks to bring down numerous Brazilian banking websites to protest corruption and inequality in the country. Banco do Brasil, Itaú Unibanco, Citibank, and Bradesco were among those affected by the #OpWeeksPayment campaign.	Institution	Banking websites brought down,
112	2012	01 January 2012	Brazilian Payments System Attack	From 2012 to 2014, Boleto Bancario, a payments system used for almost half of non-cash transactions in Brazil, was targeted by malware that manipulated the victim's browser to reroute payments to attacker-controlled accounts. The technique compromised $3.75 billion in payments within a two-year period.	Infrastructure	A payments system.
113	**2011**	**July 2011**	**Morgan Stanley Smith Barney**	**Jul 2011. Morgan Stanley mailed a CD containing sensitive data about investors in tax-exempt funds and bonds to the New York State Department of Taxation and Finance. The package arrived at the building but when it arrived at the relevant desk the data CD was missing.**	**Institution**	**34,000**
114	2011	08 June 2011	Citigroup Data Theft	In June, Citigroup announced that 360,000 card details in the United States were exposed. The bank later settled lawsuits with the states of California and Connecticut over the breach. The website vulnerability was present as early as 2008, according to Connecticut authorities.	Investor	Customers card deetails. The attackers stole names, account numbers, and contact information but were not able to access the card security codes needed to clone the cards, Citigroup said.
D	**2011**	**June 2011**	**Citigroup**	**Jun 2011. Less than 1% of Citbank card holders' names, account numbers, and contact information such as e-mail addresses were stolen.**		**360,083.00**

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
				Card security codes were not stolen.		
115	2011	01 June 2011	Global Payments Breach	In June 2011, bank and retail payment processor Global Payments was hit by a major data breach. The company said unknown attackers had stolen the details of around 1.5 million cards from a handful of servers, with enough information to counterfeit the cards although not customer names or addresses. Details of the intrusion remain scarce, although Vons supermarkets said it detected compromised prepaid credit cards around the same time that appeared related to the Global Payments breach. The incident prompted Mastercard and Visa to warn card-issuing banks about the potential fraud.	Institution	Servers containing customer card details.
D	**2012**	**April 2012**	**Global Payments (Credit, debit and check processing for merchants (Visa, Mastercard, etc.))**	**Apr 2012. 1.5 million credit card numbers from its systems may have been exposed after detecting "unauthorized access" into its processing system.**		**7,000,000.00**
116	2011	01 March 2011	South Korea Attacked II	In March 2011, South Korea was hit by a widespread DDoS attack, almost two years after a similar campaign in 2009. Targets included Hanabank, Jeilbank, and Wooribank as well as government websites and the network of U.S. Forces Korea.	Institution	Banks, but not stated what aspect of. Also government websites and the network of U.S. Forces in Korea
117	2011	27 February 2011	Multinational Prepaid Card Heist	In February 2011, a criminal gang breached at least three payment processors to take card information during a $55 million stealing spree. The gang's second operation resulted in $5 million in withdrawals in twenty countries. In February 2013, the gang carried out its third and largest	Investor	Payment processors, with customers details of card and PIN numbers. Cards cloned. Money taken.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
				operation, taking just hours to withdraw $40 million from twenty-four countries.		
118	2011	01 January 2011	Iranian DDoS Attacks on U.S. Banks	On March 24, 2016, the United States unsealed an indictment of seven Iranians allegedly responsible for the DDoS attacks targeting U.S. financial institutions across a two-year period on behalf of the Iranian government and Islamic Revolutionary Guard Corps.	Infrastructure	U.S. financial institutions targeted. The indictment followed the landmark international deal to limit Iran's nuclear capabilities in July 2015. Over forty-six financial organizations were targeted over the course of 176 days between December 2011 and mid-2013, the indictment said. The victims, which included Bank of America, the **New York Stock Exchange**, and Capital One, spent tens of millions of dollars to counteract the attacks, which at their height were occurring on a near-weekly basis.
119	2011	01 January 2011	Lebanese Banks Espionage Operation	In early 2011, a virus named Gauss was used to steal inside information from multiple Lebanese banks.	Institution	Inside information stolen from banks.
120	2010	19 November 2010	U.S. Federal Reserve Bank of Cleveland Breach	Hacking into Federal Reserve Bank in Cleveland and a range of other U.S. firms. Several organizations including Fed Comp, a data processor for federal credit unions, were breached. However, the Federal Reserve said none of its production data was accessed, and that the hacker had only accessed test computers, but the intrusion nevertheless caused thousands of dollars in damage	Infrastructure	Customer's card data. Over 400,000 credit and debit card numbers stolen.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
121	2010	01 October 2010	Nasdaq Intrusion	In October 2010, the FBI detected an intrusion on servers used by financial markets operator Nasdaq. Further investigation by several U.S. agencies found that hackers had been in the network for around a year. Nasdaq said no data was taken, and there was reportedly no evidence of suspicious trades that could be based on information in the system. At the same time, a group of criminals penetrated Nasdaq in an incident that some investigators believed was linked. In 2013, following a sprawling investigation, the United States charged four Russians and a Ukrainian man with a string of online break-ins at Nasdaq and other companies dating back to 2005. Carrefour, 7-Eleven, Heartland Payment Systems, and JC Penney were among their other targets, together losing $300 million as a result of the scheme. Breaching Heartland exposed more than 100 million payment cards, ultimately costing the firm $12 million in fines and fees.	Infrastructure	The hackers helped steal more than 160 million credit card numbers from the companies they breached, according to U.S. prosecutors Nasdeq, Carrefour, 7-Eleven, Heartland Payment Systems, and JC Penney were among their other targets.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
D	**2013**	**July 2013**	**Massive American business hack (7-Eleven, JC Penney, Hannaford, Heartland, JetBlue, Dow Jones, Euronet, Visa Jordan, Global Payment, Diners Singapore and Ingenicard)**	**Jul 2013. From 2005 to 2012, a hacking ring targeted banks, payment processors and chain stores, to steal more than 160 million credit and debit card numbers, targeting more than 800,000 bank accounts**		**160,000,000.00**
122	2010	15 April 2010	PNC Bank ATM Skimming	In mid-2010, it was reported that over $200,000 in fraudulent transactions took place in New York and Washington, DC. The transactions were traced back to compromised accounts and withdrawals in Pittsburg.	Institution	Fraudulent transactions. ATM skimming for card details.
123	2010	07 April 2010	Charles Schwab Hack	Stealing and laundering more than $246,000 through Charles Schwab brokerage accounts in 2006.	Investor	
124	2010	01 April 2010	Bank of America ATM Fraud		Institution	Computer fraud. Hacker installed malware on 100 ATMs to steal $304,000 over seven months.
125	2010	18 March 2010	National City Bank Breach	National City Bank identified a number of former debit accounts that had been compromised. The breach was only discovered after PNC Financial Services acquired the bank in 2008, highlighting the importance of assessing cybersecurity during large mergers and acquisitions.	Institution	Former debit accounts had been compromised. While the new owners announced the breach, they did not reveal the number of customers affected or the amount of money stolen.
126	**2010**	**March 2010**	**Educational Credit Management Corp (US student loan guarantor)**	**Mar 2010. A contractor for the US Department of Education stole the records of 3.3 million people. Data included names, addresses, Social Security numbers and dates of birth of borrowers, but no financial or bank account information.**	**Institution**	**3,300,000**

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
127	2010	28 February 2010	Morgan Stanley Break-In	Morgan Stanley detected a very sensitive network break-in that lasted six months in 2009, according to leaked emails. The bank believed the incident was part of Operation Aurora, carried out by the same state-sponsored attackers that targeted Google, Rackspace, Northrop Grumman, and Yahoo earlier that year.	Institution	Not stated
128	2010	24/02/2010	Latvian Bank Leak	In early 2010, a hacker leaked financial details of banks, tax records, and state-owned firms to a TV station, to raise public awareness of lucrative public sector salaries during a period of austerity in Latvia.	Institution	Financial details of banks, tax records, and state-owned firms were leaked to a TV station.
129	2009	04/07/2009	South Korea and United States Attacked	In July 2009, financial institutions in the United States and South Korea were among several targets of a widespread DDoS attack. The incident, which began over a U.S. holiday weekend, comprised three waves of attacks spanning six days.The New York Stock Exchange website was reportedly affected, as well as those for the Nasdaq, the White House, and the Washington Post. Several days later, the sites of Shinhan Bank, the newspaper Chosun Ilbo, and the National Assembly were hit in South Korea.	Infrastructure	In total, there were around thirty-five sites targeted by the attacks. A botnet of up to 65,000 compromised computers blocked and slowed government and commercial websites for several hours at a time.
130	2009	01/03/2009	Zeus Malware Attacks	Its source code was made public in 2011 after its purported creator announced his retirement, which allowed multiple versions to spread In March 2009, a security firm discovered an online data trove of stolen information from 160,000 computers infected by Zeus malware, including devices at Metro City Bank. A criminal gang also used Zeus in a global scheme to wire millions of	Institution	Zeus was widely traded on criminal forums as a way to harvest online credentials. Also used in ATM fraud. Variant: Gameover Zeus. Among its many uses was as a platform to infect systems with Cryptolocker

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
				dollars from five banks to overseas accounts, according to U.S. and UK officials who made more than 100 arrests in October 2010. The gang recruited mules to launder the stolen funds and withdraw money from ATMs around the world. The variant Gameover Zeus was controlled by a group of hackers in Russia and Ukraine from October 2011 onward, according to the FBI. Operation Tovar, an international law enforcement effort in June 2014, resulted in the seizure of key Gameover Zeus infrastructure and the release of up to 1 million victim machines from the botnet. The authorities believe the gang stole more than $100 million.		ransomware.
131	2009	01/03/2009	Skimer ATM Malware Attack	The malware has continued to evolve with later variants still in use around the world.	Institution	Skimer is capable of executing over twenty malicious commands, including withdrawing ATM funds and collecting customer information such as bank account numbers and payment card PINs.
132	**2009**	**January 2009**	**Heartland (Independent payment processor)**	**Jan 2009. The biggest credit card scam in history, Heartland eventually paid more than $110 million to Visa, MasterCard, American Express and other card associations to settle claims related to the breach. A hacker was sentenced to 20 years in prison for his role in this & other cases.**	**Infrastructure**	**130,000,000**
133	**2009**	**January 2009**	**CheckFree Corporation (Provider of online banking, online bill payment and electronic bill payment services for the financial**	**Jan 2009. Customers who went to CheckFree's Web sites between 12:35 a.m. and 10:10 a.m. on the day of the attack were redirected to a Ukrainian Web server that used malicious software to try and install a password-stealing**	**Infrastructure**	**5,000,000**

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
			services industry)	**program on the victim's computer.**		
134	2008	01/11/2008	RBS WorldPay Hack	Toward the end of 2008, Atlanta-based credit card processing company RBS WorldPay was breached by an international crime ring.	Investor	Encryption protecting Payroll debit cards was broken and counterfeit cards used to withdraw money in ATMs The investigation of the incident identified over 1.5 million customers whose confidential information was compromised.
135	**2008**	**December 2008**	**RBS Worldpay (the U.S. payment processing arm of The Royal Bank of Scotland Group)**	**Dec 2008. The hack primarily effected U.S. prepaid and the gift card issuing business of RBS Worldpay. Actual fraud has been committed on approximately 100 cards. Certain personal information of approximately 1.5 million cardholders and other individuals may have been affected and, of this group, Social Security numbers of 1.1 million people may have been accessed.**	**Institution**	**1,500,000**
136	2008	09/09/2008	United Arab Emirates ATM Fraud	In September 2008, six banks in the UAE alerted customers to change their PINs after concerns over a spike in ATM fraud in the region.	Institution	ATM fraud
137	**2008**	**August 2008**	**Countrywide Financial Corp (Mortgage financer)**	**Aug 2008. A former employee was sentenced Tuesday to eight months in prison & ordered to repay $1.2 million after pleading guilty to downloading millions of borrower files on thumb drives & selling the information to other loan officers**	**Institution**	**2,500,000**
138	**2008**	**August 2008**	**Countrywide Financial Corp (Mortgage financer)**	**Aug 2008. Rene Rebollo, a former senior financial analyst at Countrywide, stole & sold customer data over a 2 year period.**	**Institution**	**2,600,000**

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
139	2008	20/07/2008	Russian Cyber Attacks on Georgia	Between July and August, Georgia became the victim of a coordinated defacement and DDoS campaign that disrupted government and bank websites during the lead up to a war with Russia. The first incident occurred on July 20, when the website of then Georgian president Mikheil Saakashvili was disrupted by a DDoS attack, just weeks before Russia invaded the country. As part of the conflict and war that took place from August 7 to 12, 2008, numerous Georgian government and media sites were defaced and disrupted, including depictions of Saakashvili next to Hitler on the president's website.	Infrastructure	Numerous Georgian government and media sites were defaced and disrupted. The only impact on the financial sector throughout this campaign was the defacement of the National Bank of Georgia's website.
140	2008	07/07/2008	HSBC Insider Fraud	On April 18, a clerk at HSBC's headquarters in London fraudulently wired €90 million to accounts in Manchester and Morocco. He was caught when he forgot to leave the original accounts with zero balances, which HSBC staff in Malaysia spotted over the weekend.	Institution	Tranfer of €90m funds from HSBC to other accounts.
141	**2008**	**May 2008**	**BNY Mellon Shareowner Services (Wealth management)**	**May 2008. A back-up tape, containing over 12 million customers records were lost.**	**Institution**	**12,500,000**
142	**2008**	**March 2008**	**Compass Bank**	**Mar 2008. A former employee stole a hardrive containing 1m account details from the bank between May & July 2007, then used it to defraud cutomers of nearly $32,000.**	**Investor**	**1,000,000**
143	2008	07/01/2008	Citibank ATM Theft	In early 2008, a Russian hacking ring stole $2 million after penetrating a network of Citibank-affiliated ATMs across New York City.	Institution	A server that processed ATM withdrawals within 7-Eleven stores This enabled theft from ATMs; specifically this enabled them to steal

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
						debit card numbers and PINs from 2,200 machines, which they used to withdraw the $2 million
144	2008	01/01/2008	Société Générale Rogue Trader	In January 2008, a junior trader at the French bank Société Générale executed fraudulent transactions to cover up $7.2 billion in losses from risky futures trades. At one point, the portfolio of unauthorized trades was worth over €50 billion, approximately the same value as the entire firm. The bank suffered one of the biggest trading losses on record due to the incident, and the French banking regulator imposed a $6 million penalty for its lax controls.	Infrastructure	The bank's system for futures trades. Exact mechanism is unclear.
145	2007	25/12/2007	DA Davidson Data Breach	December 25–26, 2017. The breach was discovered after the perpetrators attempted to blackmail the firm several weeks later. Following the breach, the Financial Industry Regulatory Authority issued a $375,000 fine to DA Davidson for its failure to protect confidential customer information.	Institution	Confidential information from 192,000 customers was stolen from financial services holding company DA Davidson.
146	2007	14/09/2007	TD Ameritrade Data Breach	On September 14, 2007, online brokerage firm TD Ameritrade revealed that its database was the target of a data breach. The FBI and U.S. financial regulators investigated the incident, but no arrests were reported. On September 13, 2011, TD Ameritrade agreed to pay customers $6.5 million to settle a class action suit in relation to the breach.	Infrastructure	Its database was the target of a data breach that led to the theft of 6.3 million customer account records. According to Ameritrade, sensitive data on the database, such as social security numbers, were not accessed during the breach. No identify theft was detected in the aftermath of the breach. However, customers did claim to have received spam emails.

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
D	**2007**	**September 2007**	**TD Ameritrade (US online broker)**	**Sep 2007. TD Ameritrade settled a class action lawsuit to compensate as many as 6.3 million TD Ameritrade customers whose data was stolen by hackers costing the Nebraska online brokerage firm less than $2 per victim.**		**6,300,000.00**
147	**2007**	**July 2007**	**Fidelity National Information Services**	**Jul 2007. Employee sold customer information to a data broker, including names, addresses, birth dates, bank account and credit card information.**	**Infrastructure**	**8,500,000**
148	**2007**	**May 2007**	**JP Morgan Chase**	**May 2007. The personal information of approximately 2.6 million current and former holders of a Chase-Circuit City credit card had been mistakenly identified as trash and thrown out in garbage bags outside five branch offices in New York.**	**Institution**	**2,600,000**
149	2007	26/04/2007	Estonian DDoS Attacks	Following the contentious relocation of a Soviet-era statue in Tallinn, Estonia fell victim to a series of coordinated DDoS attacks. Estonia accused the Russian government of ordering the attacks but was unable to produce definitive proof.	Infrastructure	A series of coordinated DDoS attacks were launched against government, bank, university, and newspaper websites that lasted three weeks. The attack forced two major Estonian banks to suspend online banking, disabling bank card transactions and ATM withdrawals.
150	**2006**	**July 2006**	**Automatic Data Processing (Business outsourcing, payrolls, benefits)**	**Jul 2006. Automatic Data Processing, one of the world's largest payroll service companies, confirmed that it was swindled by a data thief looking for information on hundreds of thousands of American investors.**	**Investor**	**125,000**
151	**2005**	**April 2005**	**Ameritrade Inc. (online broker)**	**Apr 2005. Computer backup tape containing personal information was lost.**	**Institution**	**200,000**

			Threat Scenario		Threat Landscape	
ID #	Year	Date	Incident Description	Summary	Setting (Focal point of attack)	What exactly was compromised?
152	**2005**	**June 2005**	**Citigroup**	**Jun 2005. Blame the messenger! A box of computer tapes containing information on 3.9 million customers was lost by United Parcel Service (UPS) while in transit to a credit reporting agency.**	**Institution**	**3,900,000**
153	**2005**	**June 2005**	**Cardsystems Solutions Inc. (Third-party payment processor for Visa, Mastercard, Amex, and Discover)**	**Jun 2005. CardSystems was fingered by MasterCard after it spotted fraud on credit card accounts and found a common thread, tracing it back to CardSystems. An unauthorized entity put a specific code into CardSystems' network, enabling the person or group to gain access to the data. It's not clear how many of the 40 million accounts were actually stolen.**	**Investor**	**40,000,000**

Appendix A Part 2: Synthesised Attacks Database

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
1	Unknown		Data breach	Unknown	
2	Unknown	Silence Hacking Group	Disruption (motivation was theft)	DDoS	
3	Unknown	'Hackers'	Theft	Unknown	Exploiting PayPal's Google Pay integration.
4	Unknown		Data Breach	Unknown	
5	Non-state actor	Silence Hacking Group	Theft	Malware	Attack involved phishing emails being sent with the malware and data gathering
6	Non-state actor		Theft	Malware	Ransomware The attackers are believed to have used a VPN exploit that remained unpatched to access the firm's systems. Also known as REvil and Sodin. The vulnerability enables the ransomware to gain access to a computer and execute itself with elevated user privileges, so that it can have unrestricted access to all system files.
7	Unknown		Data breach	Unknown	
8	Unknown	Likely a nation state actor. Insider	Data breach	Unknown	
9	Unknown		Unknown	Malware	Malware affected a number of the organization's computers.
10	Non-state actor	Phineas Fisher, a vigilante hacker persona	Data breach	Unknown	
11	Non-state actor	Russian man was charged	Theft	N/A	Involved access device fraud, identity theft, and computer intrusion.

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
12	Non-state actor	'Hacker'	Theft	Unknown	
13	Non-state actor	Sberbank is investigating an internal employee who may be behind the compromise of the database.	Data breach	Unknown	
14	Unknown		Data breach	Unknown	Security researchers from Group-IB speculated the payment card information was stolen from online card payments using a JavaScript-based skimmer, such as Magecart
15	State-sponsored	Thought to be attributable to Lazarus Group, a hacking group that has targeted banks, ATMs, and cryptocurrency exchanges in order to fund North Korea's weapons of mass destruction program.	Espionage (motivation was theft)	Malware	The malware, known as ATMDtrack, began appearing on networks during the summer of 2018
16	Unknown		Data breach	Unknown	Affected the ECBs Integrated Reporting Dictionary (BIRD) site.
17	Unknown		Disruption	DDoS	Attackers sent high volumes of traffic to the organization's website, causing it to slow down and display limited information on exchange prices. Technical bug discovered.
18	State-sponsored	Five Chinese nationals arrested	Theft	Other	Inserted malware that directed ATMs to process withdrawal requests without first verifying with member banks.
19	Unknown		Theft	Ransomware	
20	Non-state actor		Data breach / theft	Other	A software engineer hacked into a cloud-based server. The hacker exploited a misconfigured firewall to gain access to a database of personal information hosted by Amazon Web Services.
D	**Non-state actor**			**hacked**	
21	Unknown		Data breach	Unknown	

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
22	Unknown		Data breach	Unknown	The Know Your Customer verification database was not password-protected, allowing anyone to access, alter, or download the information.
23	Unknown		Theft	Unknown	
24	Unknown		Theft	Malware	The individuals arrested used a technique known as “typosquatting,” in which they duplicated an online cryptocurrency exchange to steal information and gain access to victims’ bitcoin wallets.
25	Unknown		Theft	Malware	Attackers deployed malware to duplicate DBBL's Switch payment management system, allowing fraudulent financial transactions to be executed undetected.
26	**Non-state actor**	**Insider**	**Theft**	**inside job**	
27	Unknown		Data breach	Unknown	The documents were accessible to anyone with a web browser because the company used a standard format for document addresses, meaning that anyone with knowledge of at least one document link could access others simply by modifying the digits associated with the record number.
D			**Data breach**	**poor security**	
28	Non-state actor	The leader of the network was charged in Georgia while another was extradited from Bulgaria to the U.S. to face trial.	Theft	Malware	Used the GozNym malware
29	Unknown		Data breach	Unknown	The bank confirmed that the breach did not occur on its online systems but from other merchants where FirstBank customers made transactions.
30	Unknown		Unknown	Malware	Banking trojan Retefe is a malware that installs the Tor internet browser to redirect infected devices to spoofed banking sites. The Trojan is typically delivered through email attachments and often attempts

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
					to trick users into downloading spoofed mobile Android applications to bypass two-factor authentication.
31	Non-state actor	Two senior members of a Romanian cyber criminal group arrested in Mexico. Insider	Theft	Skimmer	One suspect is believed to be the head of Instacash, a fraudulent ATM service provider operating out of Mexico. The head of Instacash allegedly bribed and coerced ATM technicians to install sophisticated Bluetooth-based skimmers inside competitor's ATMs, enabling the Romanian cyber criminal group to steal PINs and card data remotely from ATMs throughout popular tourist destinations in Mexico.
32	Unknown		Data breach	Software vulnerability	In January, RBS launched a free endpoint security service for customers in partnership with Danish firm Hedimal Security. The security service was intended to detect threats and protect RBS customers from attacks.
33	Unknown	Researchers have not been able to identify the operation behind the campaign, but evidence suggests it may be connected to the Cutwill Botnet, a cyber criminal operation active since 2007.	Unknown	Malware	The Ursnif banking Trojan, which was discovered in 2007, was repurposed in a campaign targeting Japanese banks that began in 2016. Ursnif, also known as Gozi ISFB, is a popular malware that steals information on infected Windows devices. Ursnif has been deployed in a new campaign that specifically targets banks in Japan. The malware terminates itself on devices outside of the country. The campaign uses a distribution network of spam botnets and compromised web servers to deliver the Trojan.
34	**Unknown**		**Theft**	**hacked**	
35	Unknown	On January 30, 2020, the UK's National Crime Agency issued arrests in London and Belfast, suspected to be in connection to the BOV heist.	Theft	Unknown	Attackers made multiple transfer requests from the Maltese bank to accounts in the UK, United States, Czech Republic, and Hong Kong.
36	Unknown		Unknown	Phishing	
37	Unknown		Theft	Unknown	

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
38	Unknown		Disruption	Other	The attackers exploited flaws in the Signaling System 7 (SS7) protocol, which is used by telecommunications companies to route text messages around the world.
39	State-sponsored		Espionage	Other	An employee was tricked into downloading a malicious program during a fake job interview over Skype. It is believed that the Redbanc employee saw a LinkedIn job advertisement and attended a Skype interview where the attackers asked him to download a software program to submit his application form. The attackers tricked the victim into downloading malware on his system, giving them access to Redbanc's network.
40	Non-state actor		Theft	Cards	A Fuze card is a data storage device that looks like a bank card, but can hold account data for up to thirty cards. Using smartcard technology can help criminals avoid raising suspicions at payment points or if stopped by authorities, as it reduces the need for them to carry large numbers of counterfeit cards on their person.
41	Non-state actor		Data breach	Phishing	The attackers used phishing tactics to gain access to an employee's inbox, enabling them to steal around 160,000 pieces of data including documents, diary invitations, and emails.
42	Non-state actor		Data breach	Other	
D				**hacked**	
43				**poor security**	
44	Non-state actor		Theft	Malware	Trojan. The "Android.BankBot.495" malware was designed to read the victim's information when they logged into their mobile banking app.

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
45	State-sponsored		Espionage	Phishing	In late 2018, security researchers uncovered that Cobalt, a state-sponsored threat group that specializes in attacks on financial institutions, had begun employing a new variant of the ThreadKit exploit builder kit to execute phishing schemes utilizing Microsoft Office documents. First observed in October 2017, the new tactics show an evolution of the ThreadKit macro delivery tool and demonstrate the growing range of techniques employed by malicious actors.
46	Unknown	Insider	Theft	Other	Attackers connected electronic devices directly to the banks' infrastructure. Attackers used a range of readily available devices such as netbooks, inexpensive laptops, USB tools, and other devices. The attackers disguised themselves as job seekers or couriers and gained access to the local network from various places inside the victims' central or regional offices, and even from company branches in different countries.
47	Non-state actor	On November 14, two Venezuelan men were found guilty of jackpotting.	Theft	Malware	Attackers installed malicious software or hardware on ATMs to force the machines to dispense huge volumes of cash on demand.
48	Unknown		Data breach	Unknown	
49	Unknown		Theft	Other	Magecart toolset
50	Unknown		Theft	Unknown	
51	Unknown		Data Breach	Unknown	The compromise of card details came weeks after Karachi-based Bank Islami suffered a breach of its payment cards system.
52	Unknown		Data Breach	Unknown	
53	Unknown		Theft	Unknown	The thieves reportedly withdrew the funds using fraudulent messages on the SWIFT interbank messaging network.
54	Non-state actor	Russian-speaking hackers, dubbed Silence	Theft	Multiple	After an unsuccessful attempt to penetrate the Russian Central Bank's automated workstation client, the group attacked ATMs directly and through the supply chain, using phishing emails as its

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
					means of entry to the networks.
55	State-sponsored		Disruption	Ransomware	There were reports that a new strain of ransomware was involved.
56	State-sponsored	The parallels with the CUB heist continued after police arrested several suspects accused of taking the funds from ATMs. Four of the people involved also admitted playing a role in the earlier theft, according to investigators in September.	Theft	Multiple	The attackers seem to have stolen card information and also set up their own proxy server so transactions with stolen details would not trigger alarms. Over the course of just a few hours on August 11, the group coordinated almost 15,000 transactions to cash out funds through ATMs worldwide using compromised Visa and Rupay cards. Two days later, the attackers made further fraudulent transactions through the bank's interface to the SWIFT messaging system—a technique used in numerous bank attacks, including against fellow Indian lender City Union Bank (CUB) in February.
57	Unknown	According to a lawsuit filed by the bank against its insurer to recover more of its losses, an investigation after the second attack concluded that both incidents were by the same group, using tools and servers of Russian origin.	Theft	Multiple	1st attack - Phishing emails enabled intruders to install malware and pivot into the Star Network, a U.S. bank card processing service. 2nd attack - no detail
58	Non-state actor	A report by Group IB, which responded to the incident, attributed it to an established criminal group named MoneyTaker that has targeted more than a dozen banks in the United States, Russia, and the UK since 2016.	Theft	Multiple	After breaching the network through an outdated router, the group attempted to install Powershell scripts to remain on the banks' systems.
59	Unknown		Data breach	Unknown	
60	State-sponsored		Disruption, Theft		The attackers used destructive software as cover for a fraudulent SWIFT transfer.

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
					The bank's 9,000 workstations and 500 servers failed on May 24 as the KillMBR wiper tool rendered them unable to boot up
61	Unknown		Theft	Software vulnerability	A vulnerability in third-party software connected to SPEI was used by unknown attackers to get into the system and make a series of fraudulent transactions before cashing out.
62	Non-state actor	Several people have been arrested, and the U.S. Department of Defense seized the website.	Disruption	DDoS	Webstresser, a DDoS-for-hire site was said to be behind up to 6 million attacks around the world over three years.
63	State-sponsored	The Mabna Institute. Nine Iranians have been charged by the United States, which claims the group acts on behalf of the Islamic Revolutionary Guard Corps and has imposed sanctions on numerous individuals and companies in the country as a result.	Data breach	Password spraying	Used password spraying to access information
64	State-sponsored	While the incidents bear the hallmarks of the group that carried out the Bank of Bangladesh theft in 2016, there is no strong evidence the events are connected.	Theft	Malware	
65	Non-state actor	In February 2018, it was revealed that thirty-six people from seven countries had been indicted in the United States for their alleged involvement in the Infraud Organization	Theft	Multiple	The organization was said to have more than 10,000 registered members who bought and sold illicit products including malware, data from credit card dumps, and information needed for identity fraud.

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
66	Non-state actor	An eighteen-year-old from the Dutch city of Oosterhout was arrested in February for the attack, having claimed online that he bought a "stresser" tool for €40 that enabled him to send a deluge of traffic to victim websites.	Disruption	DDoS	
67	**Non-state actor**	**Insider**	**Theft**	**inside job**	
68	State-sponsored	The South Korean exchange lost nearly 4,000 bitcoins in a theft in April, which the country's authorities had linked to North Korea, according to local media.	Theft	Unknown	
69	**Unknown**		**Unknown**	**hacked**	
70	Unknown		Data breach	Unknown	Appleby has said it was the victim of a cyber attack, alleging the intruder "deployed the tactics of a professional hacker." The breach came just over a year after the Panama Papers, documents from law firm Mossack Fonseca that were leaked to the same newspaper.
71	State-sponsored	The attack is suspected of being performed by a group that has repeatedly intruded on bank networks to carry out thefts.	Theft	Malware	The attackers used an unusual ransomware variant named Hermes, but this was likely a distraction for their main objective of using administrative credentials to move funds to Cambodia, the United States, and Sri Lanka
72	Unknown	The identity of the hackers is unknown, although reports have suggested the perpetrators are based in Eastern Europe. Insider	Data breach	Software vulnerability	It took place through a software vulnerability in a test filing component.
D	State-sponsored			**hacked**	

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
73	State-sponsored	According to the U.S. government indictments, the breach was carried out by the Chinese People's Liberation Army (PLA) On February 10 2020, the U.S. Department of Justice indicted four members of the Chinese People's Liberation Army (PLA) for a targeted intrusion into the networks of Equifax, a credit reporting agency in the United States. The indictment lists the operators' affiliation with the 54th Research Institute, formerly part of the PLA and now part of the PLA Strategic Support Force (SSF).	Data breach	Web app vulnerability	Exploited a bug in an Apache Struts web application that the company had failed to patch. The attackers scanned Equifax's estate for the vulnerability and gained access to the application, an online dispute portal, days after the bug was made public in March—but did not take any data for several months. Once inside the network, the attackers found unencrypted usernames and passwords for other databases, spent seventy-six days on the network, eventually accessing forty-eight different datasets.
74	**Unknown**		**Unknown**	**hacked**	
75	State-sponsored	No perpetrators were identified, though the FSB claimed that it was organized by foreign intelligence services and speculated it had been done on behalf of Ukraine, due to the servers' location and ownership.	Disruption	DDoS	Servers and command centers purportedly to be used in these attacks were located in the Netherlands and owned by BlazingFast, a Ukrainian hosting company. BlazingFast said it had no information about the asserted attack and that it was unable to find any malicious data. The blocked DDoS attacks of 9 December reached a peak volume of 3.2 million packets per second, which is low compared to the volume of other recent DDoS attacks. The statement further noted that part of the DDoS attacks involved a botnet similar to that used in prior weeks against Germany's Deutsche Telekom and Ireland's Eircom, exploiting a vulnerability in home routers.

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
76	Unknown	Three chinese traders were sued by the USA SEC. The men were ordered to pay $8.9 million in penalties, and the trio were also indicted on criminal charges, which are ongoing. Hong Kong refused a request to extradite one of the men to the United States in 2017. Insider	Data breach	Unknown	Chinese traders, are allegeded to have installed malware on the networks of two law firms to steal confidential, market-moving information on mergers and acquisitions.
77	Unknown		Theft	Card number guessing	The unknown attackers likely used an algorithm to generate bank card numbers that used Tesco's identifying numbers at the start and conformed to the industry-wide Luhn validation scheme that helps protect against accidental errors. There are around 1 billion possible card numbers for each bank, but regulators have said Tesco Bank's cards had deficiencies, such as sequential card numbers, that made guessing the full numbers easier. The bank only used basic checks to assess whether cards were genuine, for example merely inspecting whether the debit card would expire in the future instead of making sure the exact expiration date matched its records.
78	Unknown		Data breach	Unknown	
79	Non-state actor	Anonymous' claimed responsibility as part of Operation Icarus, a campaign against central banks.	Disruption	DDoS	
80	Unknown		Data breach	Unknown	

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
81	Non-state actor	A hacking group called DownSec Belgium. DownSec Belgium claims to fight against corrupt government abuses.	Disruption	DDoS	Little information has been reported about the attack, but it followed similar DDoS attacks by the same group against the websites for the Belgian Federal Agency for Nuclear Control, the country's Crisis Center, and its federal cyber emergency team.
82	State-sponsored		Theft	Malware	The hackers had introduced malware onto the Bangladesh central bank's server and deployed keylogger software that allowed them to steal the bank's credentials for the SWIFT system. The hackers also custom-designed a malware toolkit that compromised SWIFT's Alliance Access system and was designed to cover their tracks. This toolkit allowed them to delete records of transfer requests, bypass validity checks, delete records of logins, manipulate reporting of balances, and stop attached printers from printing transaction logs. Although the malware was custom-designed to steal from the Bangladesh central bank, the toolkit could potentially be used against other banks in the SWIFT system running Alliance Access software.
83	**Non-state actor**		**Theft**	**hacked**	

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
84	Non-state actor	The group claiming responsibility for the extortion said it was part of the Armada Collective, which had previously targeted numerous businesses including Cloudflare and Proton Mail, although some investigators believed it might have been a copycat attack using the same name. Some suspected original members of the collective were arrested in Europol's Operation Pleiades in January 2016, which targeted the group DDoS4Bitcoin that has been active since mid-2014.	Disruption (motivation was theft)	DDoS	
85	Non-state actor	The perpetrator's lawyers said he was "drawn into a circus" where online groups would test the power of botnets.	Disruption	DDoS	
86	Unknown		Data breach & disuption	Unknown	
87	State-sponsored	Possibly North Korea.	Theft	Unknown	
88	Unknown		Theft	Malware	A variant of Dyre malware named Upatre, which spread through victims' email contacts, was used to block hundreds of bank websites on the victim's device. The victim was then prompted to call a helpline number—actually staffed by a member of the gang who would then harvest the victim's banking credentials and subsequently make fraudulent wire transfers.
89	State-sponsored	A subsequent report by the California Department of Insurance pointed to a national government as the likely culprit for the attack.	Data breach	Phishing	Attackers deployed a spearphishing email that gave access to ninety of the company's systems, including its back-end database.

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
90	Unknown		Theft	Unknown	In early 2015, a bank in Ecuador was the first known victim in a series of multimillion dollar heists that used compromised payments systems to then transfer funds over the SWIFT interbank messaging network. If an attacker manages to gain access to a bank's SWIFT terminal, the system can be used to ask other banks to transfer funds.
91	Unknown		Theft	Multiple: malware, phishing and browser vulnerabilities	The group used spearphishing emails or browser vulnerabilities to deliver Metel, also known as Corcow, and access the bank's systems before pivoting into areas that allowed them to roll back ATM transactions. This meant they could withdraw unlimited amounts of money, automatically resetting the account balance after each transaction. Researchers at Kaspersky, who first reported on the operation, said the gang comprised fewer than ten members and had made no infections outside Russia.
92	Non-state actor	Eight Romanian and Moldovan nationals were arrested in connection with the scheme in January 2016.	Theft	Malware	The malware, dubbed Tyupkin, was spread by a CD and once installed it laid low, only accepting commands on Sunday and Monday nights. Mules could type in a randomly generated key allowing them to withdraw 40 banknotes. Similar to the Ploutus campaign in Latin America, the Tyupkin group had an organized gang of mules to access the ATMs and collect the money.
93	State-sponsored	NATO officials later indicated privately that they believed that the hacking group's claim of being affiliated with Islamic militants was a false flag operation, and that in fact the breach was conducted by APT 28, a group widely believed by security researchers to be affiliated with the Russian government.	Data breach	Unknown	APT28 The means by which the group gained access to the exchange's networks are unknown, but they were reportedly able to infiltrate an investment simulator and a web portal for managing the stock exchange's upgrade to a new trading system, as well as render the exchange's website unavailable for two hours. The exchange's employees say that the trading system itself was not breached.

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
D	**Unknown**		**Theft**	**hacked**	
94	Non-state actor	Nine people so far have been charged in the ongoing probe. The Russian In September 2019 pleaded guilty to six felony charges in connection with the data breach and other cybercrimes, and he faces up to a lifetime in prison. In January 2017, a Florida man pleaded guilty to charges linked to funds processed through Coin.mx, an unlicensed bitcoin exchange owned by an Israeli who the United States has alleged masterminded the information stealing campaign. The supposed ringleader was extradited to the United States in 2016 and, according to media reports, entered a plea deal with prosecutors."	Data breach	Stolen Password	The group entered the network through a single-factor authentication server that had not been upgraded with the rest of the firm's estate, before gaining access to more than ninety bank servers for several months. However, the bank said the attackers had not accessed more sensitive information, such as social security numbers.
95	Unknown		Data breach	Unknown	The attack came to light after the supposed perpetrators emailed the ECB demanding a ransom payment on July 21.
D				**hacked**	
96	State-sponsored	CyberBerkut may have connections to the Russian government, but the relative lack of sophistication of their attacks has led some experts to conclude that official links are unlikely.	Data breach	Unknown	The means by which it gained access to the data is unknown.
97	**Non-state actor**	**Insider**	**Theft**	**inside job**	

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
98	Unknown	The perpetrators of the DDoS attack have not been publicly identified. The attack reportedly came from disgruntled bitcoin users who were protesting the country's ban on the decentralized currency.	Disruption	DDoS	
99	**Non-state actor**	**Insider**	**Theft**	**inside job**	
100	Unknown	In the US in 2018 two men were convicted of installing the malware on cash machines in Connecticut and Rhode Island.	Theft	Malware	The malware has been altered several times to enable its use in new ATM models.
101	Unknown	The FBI investigated the incident but has released no further information.	Data breach	Unknown	
102	**Unknown**		**Data breach**	**hacked**	

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
103	Non-state actor	Fin7, the most prolific group using Carbanak, has stolen more than €1 billion from banks in more than thirty countries over the past three years, according to Europol. As well as using Carbanak, the gang is understood to use widely available tools such as the Cobalt Strike framework. The group recruited developers to work for an Israeli-Russian front company named Combi Security, and it is not clear whether the employees knew the nature of the work. The authorities arrested a man thought to be the gang's ringleader in Spain in March 2018, while in August the U.S. Department of Justice arrested three Ukrainian suspects.	Theft	Malware	The malware is often pushed into financial companies by luring employees to click malicious documents, which provide the attackers a foothold to move across the network to remotely manipulate ATMs, known as "jackpotting," or to compromise point-of-sale data. The gangs planned each theft carefully, taking between two and four months to complete each intrusion, ultimately using mules to withdraw the funds from ATMs and transfer them to the criminals' accounts. As well as using Carbanak, the gang is understood to use widely available tools such as the Cobalt Strike framework. The group recruited developers to work for an Israeli-Russian front company named Combi Security, and it is not clear whether the employees knew the nature of the work.
104	State-sponsored	The incident was attributed by some to the DarkSeoul gang, a threat actor linked to the North Korean regime that would later be tied to the Sony breach in 2014.	Disruption	Disk-wiping	Trojan.Jokra was used to wipe disks, but the attack varied from its predecessors in that it did not include a DDoS attack
105	Unknown		Theft	Multiple	The perpetrators made fraudulent, automated clearinghouse and wire transfers before they knocked the bank's website offline. A network of more than sixty mules was reportedly used to transfer the money into criminal accounts, making the funds more difficult to trace.

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
106	State-sponsored	'The Cyber Fighters of Izz ad-Din al-Qassam' Some reports said the group had ties to Anonymous, while others made links to the Iranian government—however, the group claimed it acted independently.	Disruption	DDoS	The attacks were powerful, sending 100 gigabits per second of data to the victim sites, prompting claims that this was beyond the capabilities of a hacktivist group.
107	Unknown	U.S. authorities indicted two men, a Russian and an Albanian, who authored the original SpyEye Trojan in 2011 subsequently used during the operation.	Theft	Malware	Trojan. Operation High Roller, as it was named by the researchers who uncovered it, was the first gang to automate many of the steps in fraudulent transactions. The malware automatically checked balances, found active mule accounts that could receive stolen funds, and deleted emails confirming transfers. It also managed to bypass two-factor authentication and run its command servers on the cloud.
108	Unknown	While there is no confirmation of any wrongdoing in this case, the Shanghai Composite Index opened at 2,346.98 and fell exactly 64.89 points, matching the date of the incident (June 4, 1989). This led to widespread but unproven speculation about a protest hack that had manipulated trading that day.	Disruption	Unknown	
109	Non-state actor	It was a security researcher, Khosrow Zarefarid. However, no funds were stolen in the breach. Zarefarid maintained that he was a whistleblower rather	Data breach	Other	

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
		than a hacker.			
D				**hacked**	
110	Non-state actor	The activist group Anonymous claimed responsibility for the incident, saying it acted out of sympathy for the Occupy Wall Street protests in New York.	Disruption	DDoS	Ddos attacks lasted several days.
111	Non-state actor	Anonymous. The attackers reprised their campaign around the World Cup in 2014, which Brazil hosted.	Disruption	DDoS	
112	Unknown		Theft	Malware	The malware manipulated the victim's browser to reroute payments to attacker-controlled accounts. Also used several different versions of malware including Eupuds, Boleteiro, and Domingo, according to researchers at RSA. The unidentified gang responsible later changed its "bolware" strategy to introduce DNS poisoning as a means to install the malware, lessening the need for spam emails to spread the malware.
113	**Unknown**		**Data breach**	**lost device**	
114	Unknown		Data breach	Other	Attackers exploited a URL vulnerability that allowed them to hop between accounts by slightly changing the website address. The attackers reportedly created a script that would repeat this action tens of thousands of times in order to harvest the information before they were detected by a routine check in early May.
D				**hacked**	

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
115	Unknown		Theft	Unknown	
D				**hacked**	
116	State-sponsored	North Korea is speculated to be behind the ten-day incident.	Disruption	DDoS	Trojan. The Koredos Trojan was used to wipe disks on the computers used as command-and-control servers.
117	Non-state actor	A Turkish man named as the gang's leader, Ercan Findikoglu, was jailed for eight years in the United States in 2017 after extradition from Germany. He has also been convicted in Turkey for conspiring to produce fake cards—with a nineteen-and-a-half-year sentence he is expected to serve upon release in the United States. Three other men were jailed in 2014.	Theft	Multiple	Once inside the processors' networks, the gang used administrator privileges to steal card and PIN details and lift withdrawal limits. The U.S. authorities said the gang then sent the data to "cashing crews" worldwide, who used it to clone cards. The mules withdrew $10 million through 15,000 fraudulent ATM withdrawals in eighteen countries over the course of a weekend.
118	State-sponsored	The men (hackers) worked for two private computer security companies in Iran that allegedly performed tasks for the government. Several were also accused of belonging to hacking groups that have claimed responsibility for attacks on NASA in February 2012. The political fallout from the attack was far-reaching. The U.S. Treasury Department imposed sanctions against eleven individuals and organizations in September 2017 over their links to Iran, some of whom were accused of participating in the DDoS attack.	Disruption	DDoS	Hackers managing several "botnets" consisting of thousands of compromised computers to send malicious traffic to victim website, blocking access for legitimate users. They built the botnet by exploiting a known vulnerability in a popular content management software to install malware.

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
		Meanwhile, U.S. President Donald Trump announced the United States' withdrawal from the Iran nuclear deal in May 2018.			
119	State-sponsored	News outlets have speculated that this cyber surveillance tool was designed by the U.S. and Israeli governments to circumvent Lebanon's strict banking secrecy laws, which have made it difficult for global authorities to access information of suspected wrongdoing. These speculations were fueled by a statement made by the United States in March 2011, accusing a Lebanese bank of laundering money for a Mexican drug ring with links to Hezbollah.	Espionage	Malware	A virus named Gauss. Gauss, which bore resemblances to the Flame and Stuxnet malware, stole passwords, banking credentials, and browser cookies from infected devices. Most of the 2,500 infections detected by researchers at Kaspersky were on personal computers in Lebanon.
120	Non-state actor	A Malaysian national was arrested by the Secret Service. The Malaysian national was jailed for ten years for running the scheme	Theft	Multiple	
121	Non-state actor	Albert Gonzalez, an American known online as Soupnazi, was jailed in 2009 for twenty years. The other indicted men are still at large.	Data breach & disuption	Malware	They had used two zero-day exploits to build their presence in the stock exchange's network, and planted malware on the Director's Desk system, where directors of publicly held companies share confidential information. The malware also included a destructive capability, but it is unclear whether disruption was a goal or simply a tool the attackers might use to cover their tracks.

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
					The gang was said to have found a vulnerability in the password-reminder page of the Nasdaq site that enabled it to steal information, including hashed passwords, from the firm's SQL servers. Used techniques such as "war-driving," or traveling with a laptop to pick up the signal from unsecured networks. These details were sold via middlemen to "cashers," who used the information to create cloned cards.
D				**hacked**	
122	Non-state actor	Two Romanians were jailed for bank fraud, access device fraud, and aggravated identity theft.	Theft	Other	Comprised bank fraud, access device fraud, and aggravated identity theft While this was one of the first instances of ATM skimming for card details in the United States, the technique was already widespread in Eastern Europe.
123	Non-state actor	In mid-2010, a Russian national based in New York was jailed for three years. The hacker and his accomplices sent a portion of the proceeds back to co-conspirators in Russia, according to the FBI.	Theft	Keylogging	The hacker accessed the accounts through a keylogging Trojan, which captured the information of 180 credit cards.
124	Non-state actor	A Bank of America employee was charged in 2010. The man was jailed for twenty-seven months.	Theft	Other	Wrote code that ordered the ATMs to issue cash without a record of the transaction. He withdrew his funds over the seven months, stopping in October 2009 when Bank of America's internal control systems spotted the suspicious transactions.
125	Unknown		Data breach	Unknown	
126	**Non-state actor**		**Data breach**	**lost device**	

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
127	State-sponsored		Data breach / theft	Unknown	
128	Non-state actor	Ilmars Poikans, an IT researcher who used the alias Neo, was arrested shortly afterward and sentenced in 2015 to community service for accessing 7.5 million tax records. He was pardoned in December 2017.	Data breach	Unknown	
129	State-sponsored	While no one was publically attributed to the attack, South Korean intelligence suspects it was the work of a specific criminal or state-sponsored organization.	Disruption	DDoS	The malware spread through email with a time bomb in its code to trigger on July 10, when it would overwrite the victim's hard drive with the string "Memory of the Independence Day." This destroyed the master boot record and made the device unusable. Researchers estimated that the botnet generated 23 megabits of data per second, not enough to cause long-lasting disruption to the targeted sites.
130	Non-state actor	The Russian man accused of authoring both Zeus and Gameover Zeus remains at large.	Theft	Malware	Between 2007 and 2011, a Trojan malware known as Zeus was used in numerous criminal operations to steal data on Windows devices. The Trojan included a keylogger that recorded bank login credentials and a botnet that executed attacks using infected devices.
131	Unknown		Theft	Malware	In 2009, security researchers discovered Skimer, an advanced multifunctional malware employed in several ATM heists across the world. To install Skimer, attackers had to access ATMs and install backdoors in the device's Windows operating system. Then, the attackers could silently siphon card numbers and customer information for later use in fraudulent transactions. Once correct details were entered into the ATM pin pad, Skimer gave attackers a control panel to execute multiple commands from cashing out an

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
					ATM to deleting traces of the infection from the system
132	**Non-state actor**		**Theft**	**hacked**	
133	**Unknown**		**Theft**	**hacked**	
134	Non-state actor	Individuals in Russia, Moldova, Nigeria, and Estonia were indicted from the hack in 2009. To date, U.S. authorities have charged fourteen men.	Theft	Multiple	The group used sophisticated hacking techniques to break the encryption used by RBS WorldPay to protect customer data on payroll debit cards. Once bypassed, the group created counterfeit payroll debit cards and raised their account limits. The group employed a network of individuals to use the cards to withdraw over $9 million from more than 2,100 ATMs in at least 280 cities worldwide.
135	**Unknown**		**Theft**	**hacked**	
136	Unknown	HSBC, one of the affected banks, said the move was in response to counterfeit ATM card usage from abroad, highlighting an early case of financial attacks operating on an international scale.	Data breach	Unknown	
137	**Non-state actor**	**Insider**	**Theft**	**inside job**	
138	**Non-state actor**	**Employee convicted of downloading millions of borrower files and selling the information to other loan officers.** **Insider**	**Theft**	**inside job**	
139	State-sponsored	A group by the name of South Ossetia Hack Crew claimed responsibility for the attacks. However, Georgia would later attribute the attack to the Russia government, which denied the	Disruption	Multiple	The DDoS attack was directed using a strain of Pinch malware frequently used in Russia, which flooded websites with traffic that included the phrase “win love in Russia.”

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
		allegations.			
140	Non-state actor	A clerk at HSBC's headquarters in London. He was jailed for nine years, and the money was returned to its owners. Investigators in the UK would later uncover the gang that masterminded the fraud. Insider	Theft	Other	The employee used passwords stolen from colleagues to execute two transactions on a Friday afternoon.
141	**Unknown**		**Data breach**	**lost device**	
142	**Non-state actor**	**Insider**	**Theft**	**inside job**	
143	Non-state actor	A Russian hacking ring. Three members of the group were arrested and pleaded guilty to numerous counts of fraud and conspiracy later that year. Investigators later linked this theft to a global network of hackers that had stolen card information as early as 2005. A hacker identified as the ringleader by authorities was jailed in 2010. He would also be linked to the Nasdaq intrusion two years later.	Theft	Malware	The group gained access to a server that processed ATM withdrawals within 7-Eleven stores

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
144	Non-state actor	A junior trader at the French bank Société Générale. The employee was arrested and sentenced to three years in prison in 2010. Insider	Theft	Insider threat	The rogue trader hid his losses by booking fake offsetting trades on colleagues' accounts and using knowledge from his previous role in the back office to alter internal risk controls so he would not trigger internal alerts.
145	Non-state actor	The U.S. Secret Service launched an investigation that identified four suspects, three of whom were Latvian nationals, who were extradited from the Netherlands to face charges in the United States.	Data breach	SQL injection	Attackers deployed a SQL injection into the brokerage's website over the Christmas holiday to access customer records.
146	Unknown		Data breach	Phishing	The attackers gained access to Ameritrade's database via investment-themed phishing emails.
D				**hacked**	
147	**Non-state actor**	**Insider**	**Theft**	**inside job**	
148	**Unknown**		**Data breach**	**lost device**	
149	State-sponsored	The attacks were carried out by Russian hacktivists communicating openly on Russian-language chatrooms, where users shared precise instructions on how to conduct the attacks.	Disruption	DDoS	There were three waves. The attacks began on April 26, when government and political party email servers and websites were disrupted. The following week, a second wave began that disrupted access to Estonian news websites. The final wave, which began on May 9, was the heaviest and targeted the Estonian banking sector. The disruption did not end until the attackers' botnet contracts expired on May 19.
150	**Non-state actor**		**Theft**	**poor security**	
151	**Unknown**		**Data breach**	**lost device**	
152	**Unknown**		**Data breach**	**lost device**	

	Threat Source		Threat Event		
ID #	Threat Actor	What else known about who did it?	Type of incident	Method	What else do we know about how they did it?
153	**Unknown**		**Theft**	**hacked**	

Appendix B: How Criminals Monetise Cyber-Attacks

Asset Targeted	Typical technique	How monetised	Comment
Online personal account (e.g. bank) Direct attack on payments transfer system	Malware	• Identity fraud: access victims account then transfer money to attackers (mule) account. • Transfer money to fake accounts • Using mules to transfer money using services such as Paypal, Western Union or other untraceable systems • Sell IDaM credentials on dark web	IDaM (user credentials) typically compromised. E.g.s, Mobile banking trojan, steal credentials – DefensorID. Redirection to fake browser, stealing credentials, Zeus, Retefe etc.

Personal Identifiable Information (PII)	Data breach	• Sell data on dark web, e.g.
		  ○ Sell emails for phishing campaign lists
		  ○ Account information
		• New account fraud: impersonate person as stepping stone to other fraud (e.g. set up fake bank accounts then rob them. In the US, creating false IDs to access healthcare is popular.)
		• Target victims for 'sextortion' and other scams (revelation of some personal data e.g. password on a shopping site, frightens victims into thinking attacker has other data – e.g. screenshots on pcs, personal emails, etc.).
			E.g. SQL injection data dump.
			
			Millions of records have been stolen in the past decade. E.g. Marriott 2018 and 2020, data included passport numbers. In 2020 breach 5.2 million guest records were stolen. Hackers obtained login credentials of two employees. [63]
			
			In the 2020 EasyJet hack over 9 million records containing PII were stolen. [4/1]

Data on a computer	Ransomware (malware)	• Extortion, e.g. victim makes payment in Monero (hacker currency of choice) or Bitcoin crypto currencies to attackers account. Is untraceable.	Ransomware attacks on FSS companies are endemic. E.g. Travelex [64] 2020. $6m dollar ransom demanded. Encrypt files, whole drives or (simpler still)

Asset Targeted	Typical technique	How monetised	Comment
			just the Master Boot Record. Have been several generations of ransomware and continues to evolve. Considered a simpler way to monetise than many others. [4/1]
Credit card data	Card skimming	• Use credit card processors to accept payment • Sell card details on dark web • Clone cards (then use / sell) • Make fraudulent payments for goods (goods sent to attackers' mules then shipped elsewhere and resold) • Make cash withdrawals – 'mules' are typically recruited for this task. (e.g. Zeus 2009)	Criminals can hack a database or trick users into divulging their login credentials themselves. E.g., 300,000 British Airways customers had credit card details stolen. The Magecart APT group. (Javascript in browser redirecting to bogus site.)
FSS Network	DDoS	• Some DDoS attacks come with a demand for money to cease the attack (extortion). 2020 example, the Silence Group attack on Australian banks network. • DDoS has been used to disguise thefts from DDoS'd site. • Also costs money in lost business, system 'down-time' etc.	Is often used for disruption and destabilisation of a bank or sometimes of a country (Georgia, Ukraine, South Korea, United States). Nb: July 2020 Smile Bank (part on the Cooperative Bank in the UK) 'unavailable' to customers. No reason yet given.
Person	Phishing	• Fraud scams: trick a victim into paying money to a criminal; e.g. for counterfeit goods; • Also used as part of 'initial access' in compromising user's security	E.g. email contains click on malware as attachment, click on link to download malware
Person	Whaling	• A victim is tricked into e.g. making a wire transfer of	Study then impersonate 'high value'

Asset Targeted	Typical technique	How monetised	Comment
		funds to attackers account, or paying a fake invoice to the attacker.	individual, e.g. a Chief Financial Officer (CFO) in a company then target a subordinate.
CPU / GPU capacity & power	Cryptojacking	• A computer's resources are used by an attacker specifically to mine for cryptocurrency, which costs the victim both in terms of electricity used and degrades the value of the affected hardware over time	Mining cryptocurrencies is resource intensive and a single computer is inadequate to making any significant money. Cyptojacking is using other peoples' computers to do this work for you. One technique, e.g. for Monero, is to infect a computer via a visit to a website or browser (Drive by Download).
Computer processing	Botnet infection	• A computer's resources are used by an attacker for their own purposes, e.g. phishing, DDoS, cryptojacking, etc.	Botnets can be any computer device. More recently the proliferation of millions of Internet of Things (IoT) devices makes this these a target of choice. (Often poorly secured and few if any patches). These resources can be leveraged by an attacker unknown to the owner of the IoT device. This is very difficult to detect.
ATMs	Malware	• 'Mules' collect money from ATMs. Can be very sophisticated and large scale. E.g. Cosmos Bank SWIFT Heist 2018, covered 28 countries. $13.5m stolen.	Banking infrastructure. Very common attack, e.g. in India 2019 (ATMDtrack), Romania, Nepal, Chile - all 2019. US, Russia in 2018, etc. Known as 'jackpotting'.

Source: Compiled by Author from [33] [34]

Appendix C: Threat Scenarios for FSS Institution and Infrastructure Landscapes

C1 FSS Strategic Infrastructure Threat Landscape Scenarios

As for the scenarios in section 7.2 the source material for these scenarios comes from the findings of chapters 2, 3 and 6. The format for the table comes from Fox [41].

Table 18: Infrastructure Threat Landscape Scenarios

Scenario	Typical Threat Actor	Ultimate Target	Intermediary Target
Exploit Fintech development	Higher-skilled criminal or gang of criminals	Consumer banking or investment transactions and other financial data, both from banks and non-banks. E.g. Financial services databases, FS transaction message traffic, customer information databases [41]	• Digital platforms, in particular, investment platforms, e.g. YouInvest.
Exploit increased sharing of 'big data'	As above.	As above.	• Focus on data mining databases and AI tools (e.g. machine learning) used to interrogate them
Exploit emerging technologies	As above tending to APT skill level. Attackers are developing complex toolsets that are being updated in response to improved defence detection capabilities, targeting particularly payment messaging, payment systems and transaction authorisation functions. [6]	As above, including core banking systems. This area is especially relevant to investment platforms.	• Third-party service providers, including for critical services, such as cloud computing or middleware • DevSecOps (development and security in operations) • Cloud security, in particular that provided by externally managed services

Scenario	Typical Threat Actor	Ultimate Target	Intermediary Target
			• Payment systems security
Specifically target FSS companies that provide brokerage services	Higher-skilled criminal or gang of criminals	Access customer accounts Manipulate stock prices for 'pump and dump' attack Skim percentage on trades made	• IDaM services and data (to gain access to ultimate targets • Directory Services and asset inventories (to identify critical hardware and software components, to identify ultimate targets. *[Source: 41]*
Placing malware in trading systems.[20] Malware can 'induce abnormally large trading volumes that affect price discovery'.	Higher-skilled criminal or gang of criminals	Cause large fluctuations in e.g. commodity prices. Money is to be made on a trading strategy that can predict market movements.	• Stock market trading systems and databases

Source: [Compiled by Author from chapters 2, 3 and 6]

[20] Scenario adapted from Kaffenberger and Kopp's paper [56] looking at systemic risk assessments in the global financial system.

C2 FSS Intermediate Threat Landscape Scenarios

C2.1 FSS Institution Threat Landscape Scenario

The following scenario is derived from a series of actual attacks carried out by the Cobalt Group, a state-sponsored APT known to attack banks and retail sites. Threat event data is taken directly from MITRE ATT&CK.

Table 19: Cobalt Strike Case Study

Scenario An attack is being made on an investment platform. The attackers are using a commercial penetration testing tool, Cobalt Strike as part of their exploit kit. The intention is to access the platform, find the financial accounts databases then, using Command and Control (C2), transfer the funds to accounts of the attackers choosing.
Threat Source Target: To discover and access a platform's account databases (financial services). Threat Actor: State-sponsored proxy, the Cobalt Group. Capability: Very highly skilled. APT. Monetisation: Direct cash payout, via transfer of funds to dummy accounts.
Threat Event: Theft

Attack Vector / Threat Events	Prevention / Mitigation
Initial Access • Valid accounts	• Application developer guidance • Password policies • Privileged account management
Execution	

Attack Vector / Threat Events	Prevention / Mitigation
• Command and scripting interpreter • Native API • System services • Windows management instrumentation	• Anti-virus / anti-malware • Code signing • Disable or remove feature or program • Execution prevention • Privileged account management • Restrict web-based content • Execution prevention • User account management • Restrict file and directory permissions
Persistence • BITS jobs • Create or modify systems process • Valid accounts	• Filter network traffic • Operating system configuration • User account management • Audit • Limit software installation • Restrict file and directory permissions
Privilege Escalation • Abuse elevation control mechanism • Access token manipulation • Create or modify systems process	• Audit • Execution prevention • Operating system configuration

Attack Vector / Threat Events	Prevention / Mitigation
• Exploitation for privilege escalation • Process Injection • Valid accounts	• Privileged account management • Restrict file and directory permissions • User account control • User account management • Limit software installation • Application isolation and sandboxing • Exploit protection • Threat intelligence program • Update software • Behaviour prevention on endpoint • Application developer guidance • Password policies
Defence Evasion • Abuse elevation control mechanism • Access token manipulation • BITS jobs • Indicator removal on host • Obfuscated files or information • Process injection • Use alternate authentication	• Audit • Execution prevention • Operating system configuration • Privileged account management • Restrict file and directory permissions • User account control • User account management

Attack Vector / Threat Events	Prevention / Mitigation
material • Valid accounts	• Filter network traffic • Encrypt sensitive information • Remote data storage • Anti-virus / anti-malware • Behaviour prevention on endpoint • Application developer guidance • Password policies
Credential Access • Input capture • OS credential dumping	• Operating system configuration • Privileged account management • Password policies • Active directory configuration • Credential access protection • Encrypt sensitive information • Privileged process integrity • User training
Discovery • Network scanning service • Network share discovery • Process discovery	• Network Intrusion Prevention • Disable or remove feature or program • Network segmentation

Attack Vector / Threat Events	Prevention / Mitigation
• Remote system discovery	• Operating system configuration
Lateral Movement • Remote services • Use alternate authentication materail	• User account management • Multi-factor authentication
Collection • Data from local system • Man in the browser • Screen capture	• User training • User account management
Command and Control • Application layer protocol • Protocol tunneling • Proxy	• Network Intrusion Prevention • Filter network traffic • SSL / TLS inspection
Exfiltration • Scheduled transfer	• Network intrusion prevention

Source: [Compiled by uthor from chapters 2, 3 and 6. Detail of attack in SAD dataset]

C2.2 FSS Infrastructure Threat Landscape Scenario

A very different example, this case study is based on the METEL malware attack on the Russian currency exchange rate in 2015. Not much detail is known about the threat event, but it is an interesting example with multiple targets and highly complex organisation. Threat event data is taken directly from MITRE ATT&CK.

Table 20: METEL Case Study

Scenario A group of criminals decide to launch multiple attacks on institutions in Russia. The group used spear-phishing emails or browser vulnerabilities to deliver Metel, post-exploit malware that allows attackers to perform actions as if they were legitimate logged-in users. According to researchers at Group IB Metel had infected 250,000 devices and more than 100 financial institutions in 2015. Millions have been stolen from ATM machines. It is the manipulation of the Russian exchange rate however which makes this an attack on FSS infrastructure.	
Threat Source Target: Multiple, including manipulation of the Russian exchange rate and theft from ATMs. Threat Actor: Non-state actor, ie, a criminal or group of criminals. Capability: High; the group has not been caught five years later and analysts remain unclear how this was done. Monetisation: Multiple. The criminals got direct cash payouts via ATMs. However, much more lucrative, if you can manipulate an exchange rate you can make millions without needing to set up fake accounts. If you know how the rate is going to move you can trade as normal, using existing accounts. Simply i) 'hedge' Forex trades (ie, make money by betting on the movement of the currency itself) and ii) trade normally buying foreign shares at optimum buy and sell prices. None of this, however, was ever proved.	
Threat Event: Theft	
Attack Vector / Threat Events	**Prevention / Mitigation**
Lateral Movement • Remote services using PUTTY and VNC for lateral movement.	• User account management • Multi-factor authentication

Source: [Compiled by author from chapters 2, 3 and 6. Detail of attack in SAD dataset]

Appendix D: Investor Questionnaire

Questions in Survey	Options for Answers
1) What investment platform do you use? (If more than one, please chose your main account)	▪ Answer in free text
2) When you decided to invest on this investment platform was cyber security a factor?	▪ Yes / No
3) Do you think your investment platform is safe from cyber attack (being 'hacked' by criminals)?	▪ Yes / No
4) Do you understand the following terms? a. Phishing b. DDoS c. Malware d. Ransomware e. Social engineering f. Keylogging g. Password Spraying h. SQL Injection	▪ Understand / Do not understand
5) You are presented with two scenarios. For each scenario, if you lose money through some form of criminal activity, who is responsible for the losses? a. Scenario 1: I am told by the investment platform that money has been stolen from my account. b. Scenario 2: I notice some money has gone missing from my account. The investment platform are unaware of this. They tell me later my correct password and login details were used to make the transfer.	▪ 'The investment platform is responsible' ▪ 'I am responsible' ▪ 'It depends how much money was stolen.'
6) Who is responsible for the security of your account on this platform?	▪ The investment platform (e.g., YouInvest, Hargreaves Lansdown, i-web etc.) ▪ I am responsible ▪ Both
7) Which of the following actions do you take to protect your account? a. I use anti-virus software and ensure it is kept up to date b. I use secure connections when on wireless networks c. I never tell anyone my password or other account security details d. I am wary of giving any sensitive	▪ Yes ▪ No ▪ Don't know

Questions in Survey	Options for Answers
information to people I don't know, either by telephone or email. e. If I want to send a message to my investment platform I don't send them emails, I use the secure message feature on my online account. f. I keep informed of the latest security threats. g. I keep my personal details on my online account up to date.	
8) How safe or not are the following devices from remote cyber attacks? a. Mobile Phone (examples: iPhone, Samsung Galaxy, Google Pixel) b. Tablet device (examples: iPad, Microsoft Surface, Fire tablet) c. Laptop or desktop computer (either wireless (wi-fi) or connected by ethernet cable to router) d. 'Smart' home devices, (These typically allow you to control certain devices remotely, such as Amazon Echo, Ring doorbells with cameras, smart light switches, smoke alarms, plugs, smart thermostats for home heating etc.	▪ Very safe ▪ Safe ▪ Neither safe nor unsafe ▪ Unsafe ▪ Very unsafe
9) What more do you think could be done to protect your security?	▪ Answer in free text
10) Are there any comments you would like to make or questions you have?	▪ Answer in free text

Survey Detail

- 100% response rate from 11 investors aged 16-85, July-August 2020.
- Method: surveymonkey.com.
- Responses available on request
- Note: Question 7 is taken verbatim from the AJ Bell website Security Centre [65]. The page, "Protect Yourself", proposes these seven measures as "good practice" for investors.