



BAE SYSTEMS

The Evolving Advanced Cyber Threat to Financial Markets



■ Contents

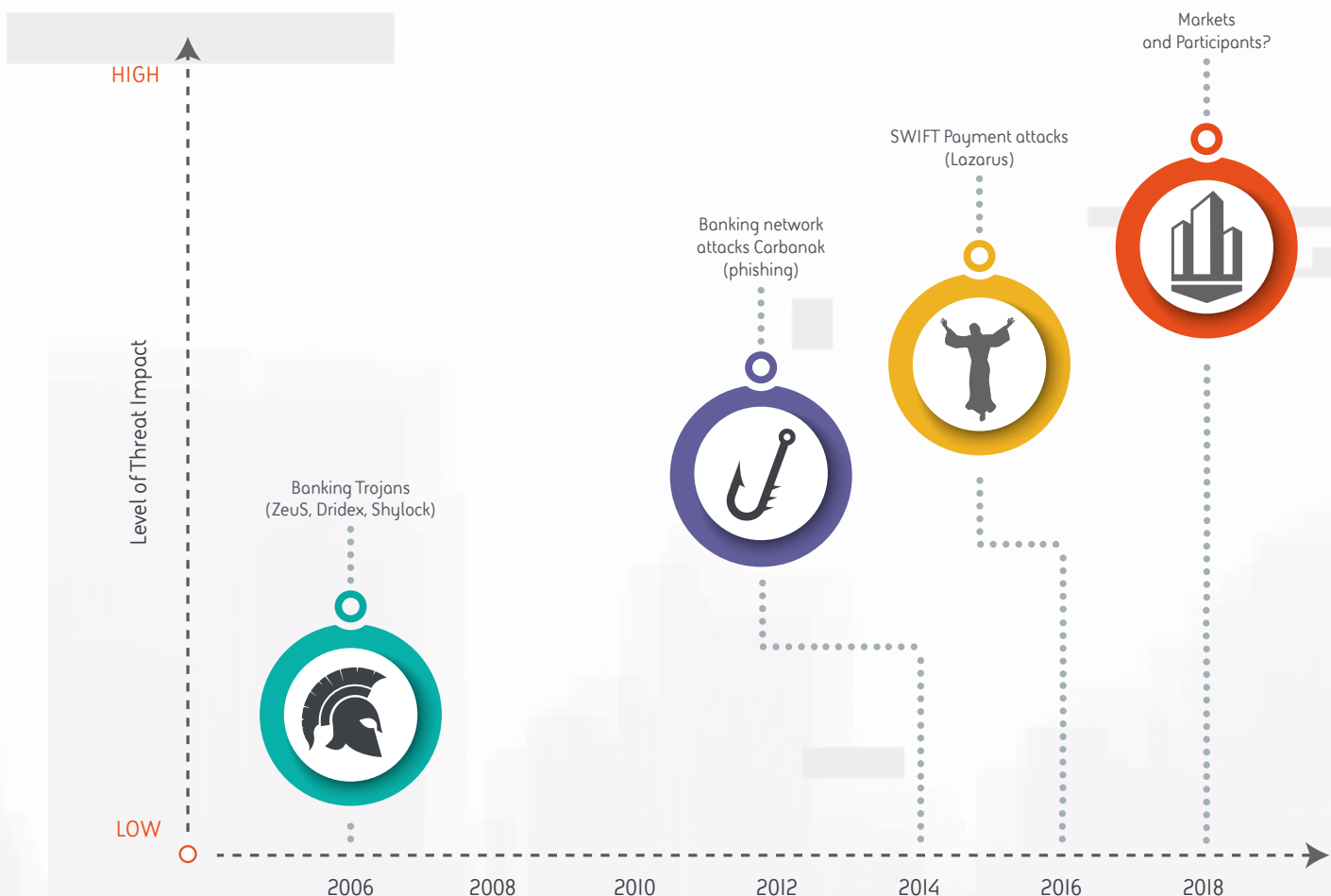
The scale of cyber threat to the financial sector	3
The evolution of financial threats	3
The threat to Market Infrastructure	4
Compare and contrast	4
The Market Infrastructure view	5
The Participants Infrastructure view	5
The cyber threat: key trends and themes	6
The cyber threats facing your business	7
What we recommend	8
What you need to do now	8
All Market Infrastructures and Participants	9
Approach and objectives: introduction	10
Methodology	10
Financial markets cyber threat analysis 2018/19 report	13
Foreign Exchange market overview	14
Foreign Exchange cyber threat view	14
Foreign Exchange Participants	15
Foreign Exchange Market Infrastructure risk scenarios	16
Foreign Exchange Participants risk scenarios	17
Banking and Payments market overview	18
Banking and Payments cyber threat view	18
Banking and Payments Participants	19
Banking and Payments Market Infrastructure risk scenarios	20
Banking and Payments Participants risk scenarios	21
Trade Finance market overview	22
Trade Finance cyber threat view	22
Trade Finance Participants	23
Trade Finance Market Infrastructure risk scenarios	24
Trade Finance Participants risk scenarios	25
Securities market overview	26
Securities Exchange cyber threat view	26
Securities Exchange Participants	27
Securities Exchange Market Infrastructure risk scenarios	28
Securities Exchange Participants risk scenarios	29
Threat factors scoring	30
Susceptibility factors scoring	31
Appendix	31

The **scale of cyber threat** to the financial sector

The cyber threat facing the financial sector has never been greater. From banking trojans affecting individual customers, through systemic threats posed to availability and integrity by ransomware, to targeted attacks from Advanced Persistent Threat (APT) groups, the landscape is evolving on a daily basis.

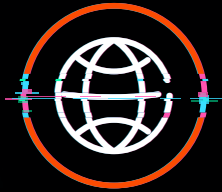
The good news is that the financial sector is responding. Increased awareness to vulnerabilities and cross industry efforts such as SWIFT's Customer Security Programme (CSP) have taken firm root across the digital landscape. As these efforts mature, the questions for the industry now are where will the next potential attack occur? And what can be done about it?

The **evolution of** financial threats



The threat to Market Infrastructure

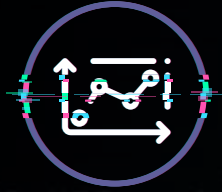
In this paper, we will explore the theory that as the threat evolution occurs, cyber security attacks will target markets such as:



FX Markets



Banking
and Payments



Trade Finance



Securities

Each of these markets has two main groups with differing threat profiles – their **Market Infrastructures** and the **Participants** who make use of these to execute transactions.

We believe the cyber threat is highest to **securities markets participants** in the near term.

Compare and contrast

When comparing four types of Market Infrastructures, FX and banking and payments were viewed as less vulnerable to cyber threats than trade finance and securities. FX and banking and payments Market Infrastructures are also relatively standardised, structured and simple in terms of concept and operation.

By contrast, trade finance and securities are far more complex and have more non-standard and unstructured interactions. They are also underpinned by many more instances of Market Infrastructures – which opens up new windows of opportunity for cyber threat actors to exploit.



The Market Infrastructure view

Market Infrastructures are clearly points of concentration but, in general, they are less susceptible and harder to successfully attack than associated Participants.

This is due to a range of factors, such as:

- **Greater standardisation and structure of interactions:** Market Infrastructures have to serve many Participants efficiently and therefore need to provide a consistent service which helps facilitate better monitoring of anomalous activity.
- **A clearer role and purpose in the market:** Market Infrastructure providers focus heavily on their service and the way it operates.
- **Greater amounts of oversight/regulation:** There is a broad understanding that Market Infrastructures are concentration points and therefore potentially systemically important.
- **One breach will not suffice:** Subverting a Market Infrastructure does not generally lead to a simple cash out and often requires further breaches, usually involving Participants.

The Participant view

Market Participants were generally found to be subject to higher threat and greater susceptibility, particularly in securities, banking and payments and trade finance.

This is driven by factors, such as:

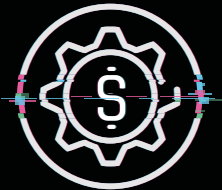
- **No safety in numbers:** The differing cyber maturity of Participants, together with higher numbers of interactions and higher numbers of complex interactions and processes, gives more opportunities for cyber threats to exploit.
- **Less focus on cyber risk:** Participants can interact with multiple markets and multiple operations. Interactions, while important, are only one aspect of what they do. This means there is potentially less focus, expertise and resource on the cyber threat as Participants can't focus everywhere, all of the time.
- **Misplaced trust:** A complex set of ecosystems, as well as manual and automated hybrid processes between Participants, feed into interactions with markets. This generates inherent trust and reliance on the systems and processes that provides ample opportunities for APT groups to exploit.

The cyber threat: key trends and themes

The key trends and themes reshaping the evolving cyber threat are:



Understanding of market practices: Some market practices which require trust, such as delivery free of payment and documentary collection, potentially unsafe practices including confirmations via fax or email, and the long chain of interactions between unrelated Participants, all provide a wide range of opportunities for APT groups to exploit.



Digitisation/Automation: A general trend across all markets is the increasing desire to digitise and automate market operations for greater efficiency and to increase participation and revenue. This trend can be both positive and negative – it can lead to streamlined operations, greater speed and fewer errors but only if designed and implemented to take into account the cyber threat. People can also be lulled into a false sense of security and trust the machine which cyber attackers will exploit.



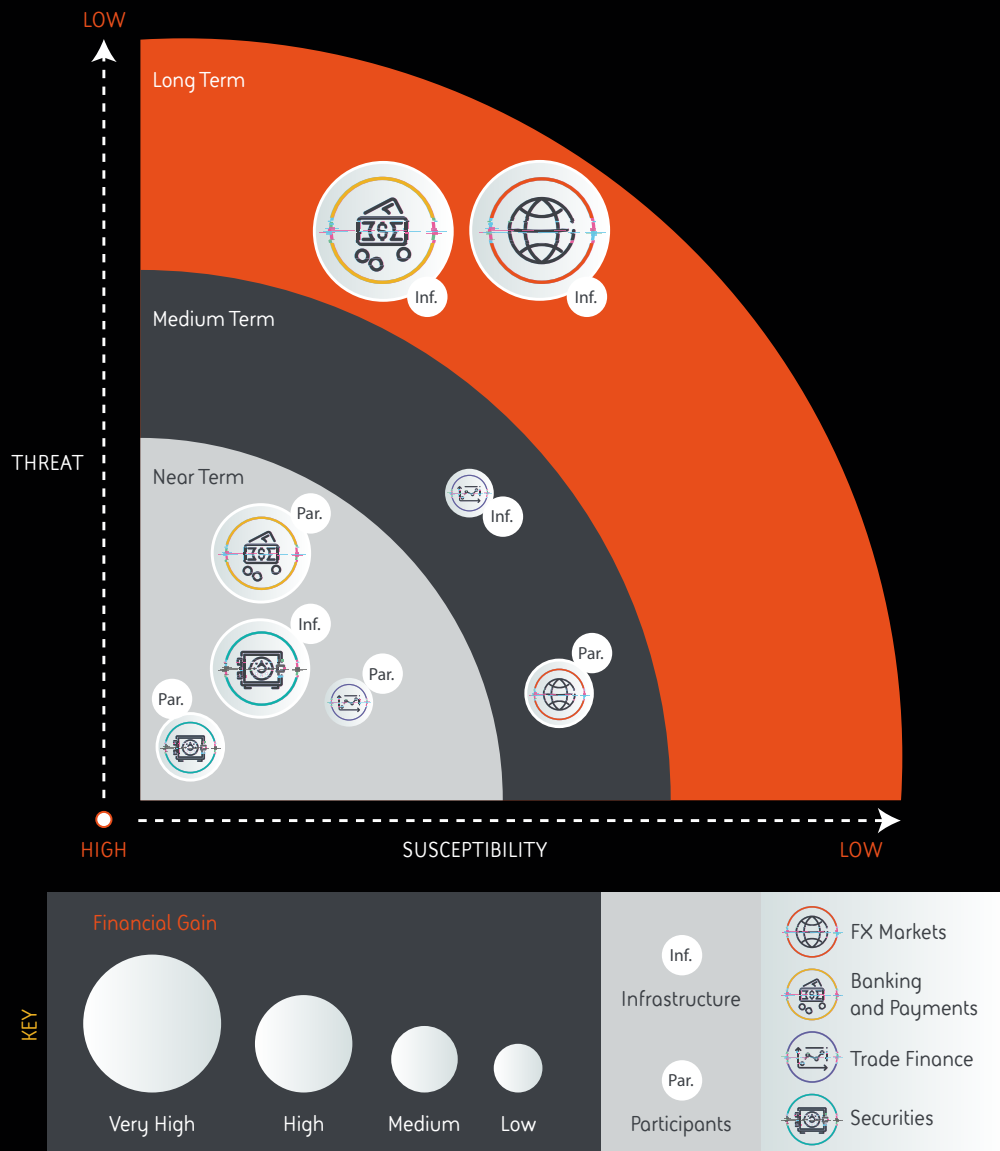
Disruption and increasing competition: The rise of FinTechs and other new entrants seeking to shake up markets is causing increased disruption. Whilst such change, innovation and competition is positive, it increases the cyber risk as new entrants and incumbents rapidly bring in new technologies, services and ways of working that are immature and unable to withstand the increasing cyber threat.

People can be lulled into a false sense of security and **trust the machine** which cyber attackers will exploit



The cyber threats facing your business

We believe that the cyber threat to Market Infrastructures and Participants can be illustrated as:



In the near term, we believe the cyber threat is highest in the securities markets, particularly to its Participants. This is due to the large numbers of Participants and infrastructures in that market, the complexities of their interactions, and inherent characteristics such as long chains of custody, unstructured communications and trusted practices – all of which combine to provide opportunities for APT groups to exploit.

The threat to Participants in the banking and payments market remains near term as it provides more direct cash out opportunities, but cyber risks are better understood in this area and SWIFT's CSP has also helped improve their defences. Trade finance participants, meanwhile, are subject to a near term cyber threat but less so than other near term targets due to the potential lower returns for the attacker.

FX Participants and trade finance Market Infrastructures are subject to a medium term threat as the cash out from attacking these targets is less direct than the near term targets. Attacks would also be more difficult due to having to manipulate more complex, individual transactions.

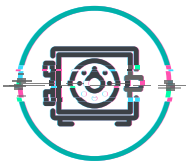
FX and banking and payments Market Infrastructures are subject to a longer term threat due to a variety of factors. Not only are these are known, systemically important infrastructures that are subject to oversight, they also have a higher awareness and state of readiness in response to the threat from APT groups.

What we recommend

Given the wide ranging cyber threat across Market Infrastructures and Participants, it is clear that a holistic approach is non-negotiable. It is not purely a technical issue as the threat takes advantage of weaknesses in market operations, people and processes. Security, therefore, needs embedding and co-ordinating across all levels an organisation – from the board right through to operations and its markets.

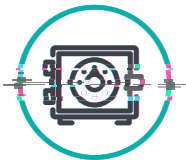
What you need to do now

Continual improvement is the cornerstone of any security programme. Those our assessment identifies as near term market targets of cyber attack may wish to take additional reviews and steps:



Securities Participants

Beware of fake news: Communications and data to support pre and post trade activities are critical to securities market operations but are vulnerable to fraudulent manipulation by cyber threats. Participants need to identify opportunities for such manipulation and ensure checks are in place throughout the trade lifecycle.



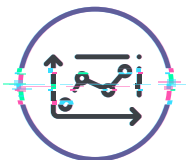
Securities Market Infrastructures

Crack down on inherent market practice risks: Securities Markets Infrastructures support common market operating practices which APT groups will seek to exploit. Market Infrastructure providers should seek to collaborate with Participants to identify risks in common practices to jointly defend market operations.



Banking and Payments Participants

Look beyond the payments system: Participants have strengthened security controls around their payments systems thanks to initiatives such as SWIFT's CSP and an increasing awareness of cyber attacks on payment systems. However, they also need to build on the work of the CSP to ensure protections are built in to upstream systems.



Trade Finance Participants

Trust but verify: Trade finance relies on trust and documentary evidence across a broad spectrum of sometimes anonymous participants. As a result, trade finance participants need to review and manage areas of inherent trust which are at risk of cyber exploitation.



All Market Infrastructures and Participants

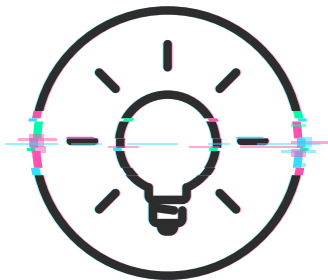
By their very nature, financial markets will always be attractive targets for APT groups. The potential gains on offer encourage sophisticated and planned attacks and this means that it is imperative for all Market Infrastructures and Participants to maintain a constant state of vigilance against the circling threat from APT groups. To do this, they can:

Team up to build up



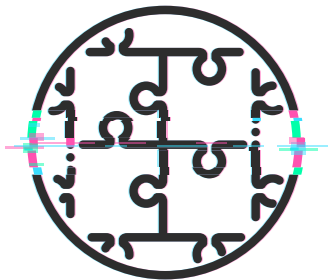
The different stakeholders in organisations, from board members to front office staff, need to collaborate and understand the markets they operate in, how they function and how they interact with each other in order to determine potential areas of cyber risk. They also need to co-ordinate with industry peers and regulators in order to share threat intelligence and defend market interests. This understanding can only come from collaboration across the stakeholders as each group has valuable insight. If cyber security professionals try and do this alone, they will potentially miss critical aspects of the way markets work and the way their organisations operate in those markets.

Think like an attacker



When reviewing market practices and the way the business is structured, apply a cyber threat lens and look for opportunities in the way data can be manipulated, trusted relationships can be abused, and automatic processing and execution can be subverted. The attacker will need to move assets and cash out – consider the steps they would take to do this in the organisation and do not assume existing checks and balances would prevent or detect such activities. For example, a business might use emails to confirm payment details. Such approaches may have been used for many years but they are inherently insecure from a cyber perspective.

Take a structured approach



Map out the people, processes, technology and dependencies that interact with markets in order to identify potential areas of cyber threat and provide a common frame of reference to focus efforts. The sheer scale and complexity of market operations may be daunting but a potentially helpful starting point would be to review and understand SWIFT message categories and types as these are derived from market practice. Participants would then identify areas of potential weakness that could be exploited by APT groups



■ Approach and Objectives

Introduction

This report considers the threat to financial markets from APT groups. Rather than analysing the tactics, techniques and procedures that attackers may deploy, we will instead be examining what they might attack, and why.

It is important to note that APT groups are well resourced teams who will patiently and rationally review and assess financial markets to determine where they should target next. The financial community needs to urgently understand its greatest cyber exposures in order to counter this threat.

We will provide the reader with overall analysis of the relative cyber threat facing financial markets and highlight areas of interest to help fulfil BAE Systems and SWIFT's shared mission to raise awareness and help the wider financial services community better defend itself.

Methodology

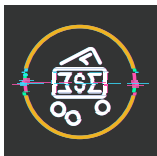
BAE Systems has almost 50 years' hands on experience in protecting some of the world's most sensitive data. In financial services our mission – to protect and enhance the connected world – manifests uniquely with solutions in both the cyber security and financial crime space. The insights and recommendations in this report are based on our extensive knowledge of both these domains and the cyber threats facing financial markets around the world. They have been tailored to address those experienced specifically by Market Infrastructures and their Participants.

Market Infrastructures are key components and systems of financial markets that enable the provision of services and are critical to the operation of the market. Participants are the various individuals or organisations involved in the market, making use of the Market Infrastructures to transact with each other and with the infrastructure itself.

We selected four financial markets to review and assess their vulnerability to APT groups:



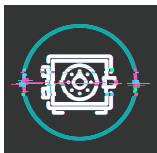
Foreign Exchange: The FX market is arguably the world's largest (by volume) and most liquid financial market and is vital to global trade and money flow.



Banking and Payments: The banking and payments market covers the fundamental movement of money between organisations and individuals and therefore underpins all other markets.



Trade Finance: Trade finance supports domestic and international trade transactions and as such is critical to facilitating global and domestic trade in goods.



Securities: Critical to the global economy, securities make up arguably the most complex and diverse financial markets, and include market areas such as trading equities, bonds and derivatives.

Each of these have been analysed against a set of threat and susceptibility factors:



Threat factors:

These are those which influence the APT group's assessment of whether to invest the time, effort and funding to develop and undertake attacks.



Susceptibility factors:

These are inherent characteristics of the market which determine how potentially vulnerable a market is to cyber threat.

For each market, the threat and susceptibility factors were assessed based on research and consultation with SWIFT and BAE Systems subject matter experts, as well as input from financial services peers. Factors were assessed as high, medium or low to provide a relative view of their significance and to allow for comparison between markets.

The potential financial impact of a cyber attack in each market target area was assessed from low financial gain to very high financial gain to provide a relative comparison between market target areas.

When assessing the threat and susceptibility factors, we took into consideration the method and approach of APT groups which we explored in our previous report, *The Evolving Cyber Threat to the Banking Community*¹. In summary, we considered the APT threat as being able to covertly infiltrate the target, move laterally across the network deploying malware and perform extensive reconnaissance on the use of target systems and processes to learn how they work, before eventually initiating the attack and covering their tracks.

Based on the threat and susceptibility factors, potential financial impact and understanding of each financial market target, an overall assessment of the potential cyber threat they are facing can be determined.



Threat Factors



Ease of Attack: The money, resources, knowledge and time required by APT groups to develop and deploy attacks against Market Infrastructures or Participants.



Reward per Attack: The financial return from each attack against a Market Infrastructure or Participant.



Ease of Cash Out: How complex it would be to obtain the stolen assets from an attack considering the number of steps and their complexity to successfully steal assets.



Repeatability: How repeatable the attacks are in the market.



Stealthiness: How likely the attack is to be discovered, taking into account factors such as the complexity of the market and the level of oversight.



Traceability: How difficult it is to link the stolen assets to the attacker.



Complexity: The range and number of operations and interactions within and between Market Infrastructures and Participants.



Standardisation: The maturity of manual and automated aspects of operations, whether interactions are structured or unstructured, and the standardisation of interactions.



Concentration: The reliance on key functions in the market and dependence on key suppliers.



Regulation Oversight: The maturity of regulation and oversight in the market.



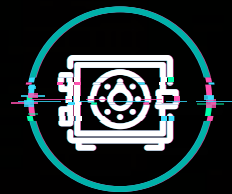
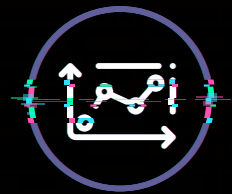
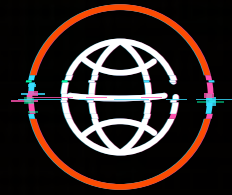
Transaction Speed: The speed of transactions in the market resulting in a transfer of assets.



Check and Balance: The level of trust and mutual checks, balances and reconciliation that occurs

Susceptibility Factors

Financial Markets: Cyber Threat Analysis 2018/19





Foreign Exchange Market Overview

The FX market is arguably the world's largest financial market (by volume) and operates at several different levels. At the top is the wholesale interbank FX market composed of major banks which trade large amounts of currencies. The retail level includes smaller banks, multinational corporates, hedge funds, retail market makers and investors – both professional and consumer.

At the interbank level, there are some common Market Infrastructures such as the use of Thomson Reuters dealing and Electronic Brokerage Services (EBS) as the main currency trading platforms, as well as the use of CLS (Continuous Linked Settlement) Bank, a US financial market institution which settles approximately 50% of daily FX trades globally for 18 major currencies. SWIFT provides common connectivity and messaging standards between CLS members and their third party customers.



Foreign Exchange Cyber Threat View

At Market Infrastructure level, FX is relatively simple as it is based on OTC trading with some concentrations in settlement infrastructures (such as CLS) and commonly used currency trading platforms. The interactions are more structured and standardised with these infrastructures receiving orders, performing netting and settlement, and currency trading platforms receiving and processing buy/sell orders.

The structure and standardisation of the interactions help identify anomalous activity, which makes it more difficult to disguise an attack. CLS is also recognised as a systemically important institution overseen by US regulators, and trading platforms, too, are known and watched over by local regulators. This is also broadly the case for other settlement infrastructures and is evidence of a greater awareness of risks to such infrastructures, including the threat from APT groups.

A successful attack on FX Market Infrastructure would potentially be highly lucrative due to its size and liquidity, but it would be more difficult to cash out and would require further breaches, potentially via Participants.

When considering the threat and susceptibility factors, the forecast cyber risk is therefore relatively low, and is longer term when compared to other markets.

Participants

At the FX Participant level, the story is different. Market operations are more complex due to many of them having differing cyber maturity, a multi-level market, multiple relationships, and fewer standard interactions. There is also greater hybrid IT and manual processing, little regulation and high volumes putting pressure on resources performing checks and balances. The cash out part of cyber-attacks is also more straightforward for FX Participants as attackers can establish direct relationships (such as setting up trading accounts) and influence FX transactions to their benefit.

Considering these and other threat and susceptibility factors, the forecast risk to FX participants is much higher when compared to FX Market Infrastructures. However, because it remains less than other Market Infrastructures and Participants, we view it as a medium term risk.

Market Impact

Target Areas: Market Infrastructures

Financial Gain: ● **Very High**

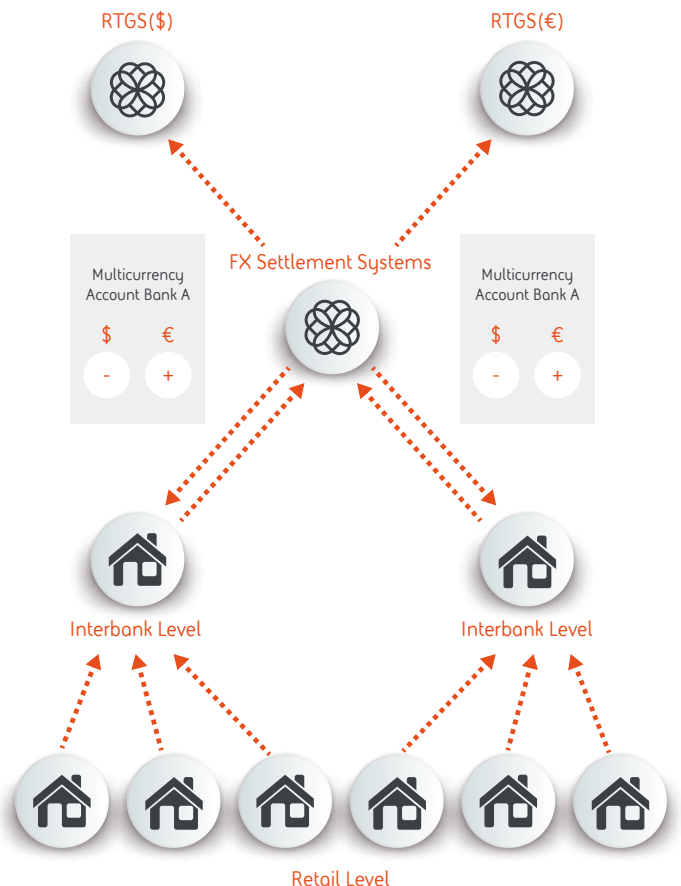
Rationale: FX is the largest and most liquid financial market by volume. This means that potential financial gains would be very high if Market Infrastructures such as settlement institutions, common trading platforms and infrastructure – including SWIFT – were compromised.

Target Areas: Participants

Financial Gain: ● **Medium**

Rationale: Compared to the potential financial gain from FX Market Infrastructures, the gain from Participants would be more limited. This is due to the largely bilateral, lower margin trades which an attacker would need to manipulate in their favour, as well as the smaller amounts available from each Participant.

Foreign Exchange Market Infrastructures and Participants Overview



FX Market Infrastructure Overview

FX Market Infrastructure Risk Scenarios

For FX Market Infrastructure, cyber risk scenarios would be focused on settlement infrastructures such as CLS and the interbank and retail level trading platforms. As the focal points in the FX market for transactions, the cyber risk would be to systems receiving and processing the FX orders and performing the netting calculations that determine the values of funds transferred. Malicious alterations to the orders and calculated values would affect the funds transferred and would be settled with finality.

For trading platforms, the cyber risk is where there would be malicious alterations to the FX instructions received, thereby affecting the value of funds transferred in a trade.

Threat Factors

Ease of Attack



Attacks against the small number of FX Market Infrastructures would take significant effort as their importance is understood and there is greater awareness of cyber threat.

Reward per Attack



Successful attacks would potentially yield high rewards due to the daily volume and value of FX transactions.

Ease of Cash Out



Direct cash outs are unlikely as they would be affecting clearing and settlement transaction details, and also require further breaches elsewhere to realise a gain.

Repeatability



As Market Infrastructures are independent of each other and implement functions differently, attacks would have low repeatability.

Stealthiness



The complexities and volumes of FX mean that subtle changes may be difficult to detect.

Traceability



Transactions are carefully recorded to support market operations so there would be an audit trail of FX transaction activity.

Susceptibility Factors

Complexity



FX Market Infrastructures include settlement infrastructures, interbank trading platforms, retail FX trading platforms and reference data sources. Their interactions are well established and relatively simple.

Standardisation



There is a high degree of standardised messaging and interactions between market infrastructures for settlements and with participants for electronic trading.

Concentration



CLS processes over 50% of global FX settlements and there are two main trading platforms at interbank, with SWIFT being the common network and messaging service provider.

Regulation Oversight



CLS is a US regulated institution and SWIFT has oversight from its governance members including central banks. Common trading platforms are also subject to regulatory oversight.

Transaction Speed



Settlement infrastructures generally have schedules for settlement during the day. FX trading platforms would transact at differing speeds and times depending on their settlement schemes.

Check & Balance



Settlement infrastructures settle with finality and instructions are processed on receipt and authenticated.

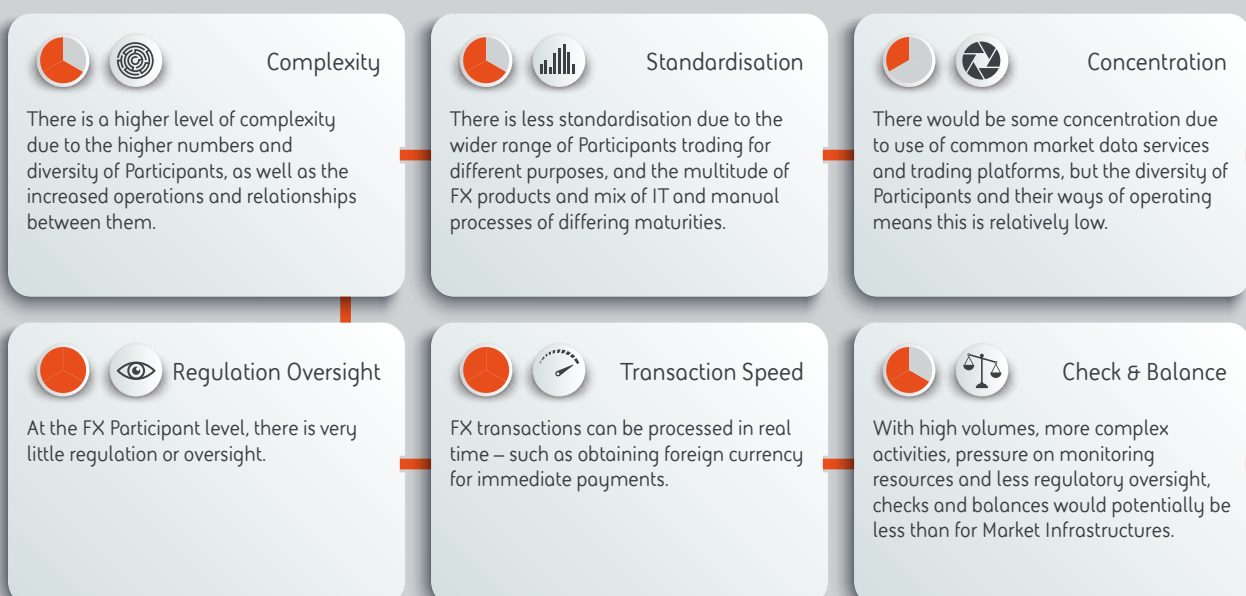
FX Participants Overview

FX Participants Risk Scenarios

For Participants, the anticipated cyber risk is higher due to their larger numbers in the retail FX market. And in addition, not only do they have varying cyber maturity, but there is also less regulation and oversight.

Participants are particularly vulnerable to attacks on their business processes. This is where unstructured communications and data – such as email and instant messaging – are used for orders and confirmations, and where key information covering payment details and amounts could be altered.

APT groups could also target systems used to generate the FX trade instructions to the market platforms to execute fraudulent transactions.





Banking and Payments Market Overview

The banking and payments market covers the fundamental movement of money between organisations and individuals and therefore underpins all other markets. From a SWIFT perspective, payments messages are highest² in terms of volumes of messages sent annually and there are more members sending payments messages than any other type.

Banking and payments Market Infrastructures payment systems are broadly split into two types – RTGS (Real Time Gross Settlement) systems and Retail Payment Systems (RPS).

SWIFT is the common network, messaging and service provider between RTGS and RPS although it is less prevalent within countries than between them. The Participants include banks, corporates, governments and individuals who interact with RTGS and RPS.

Banking and Payments Cyber Threat View

At the Market Infrastructure level, the operation and interactions are relatively simple and standardised. RTGS process low volumes of transactions and credit and debit accounts in core banking systems with finality. RPS, meanwhile, process high volumes in a netted way and settle with RTGS. Underpinning both systems are SWIFT network and messaging services.

These infrastructures are understood to be critical, are subject to regulatory oversight and the threat from APT groups is broadly understood and managed. Attacks on Market Infrastructures would be very lucrative as they would be attacking the direct movement of money, but cashing out the gain would be more difficult as further breaches elsewhere would be required.

Overall, considering the threat and susceptibility factors, the cyber risk to Market Infrastructures within banking and payments is relatively low and is considered a longer term risk.

Participants

For Participants such as banks, corporates, governments and individuals, there is a lower chance of detection when compared to the Market Infrastructure level. As noted by the FCA's Future Horizons Conference 2017 Cyber Crime Paper³, the increased investment from larger financial institutions on cyber security is displacing attacks and attackers "to target new geographies, individual and enterprises who do not have similar levels of protection".

Therefore, the overall cyber risk to Participants, particularly for those with less investment and maturity in cyber security, is considerably higher and more near term than for the Market Infrastructure.

Market Impact

Target Areas: Market Infrastructures

Financial Gain: ● **Very High**

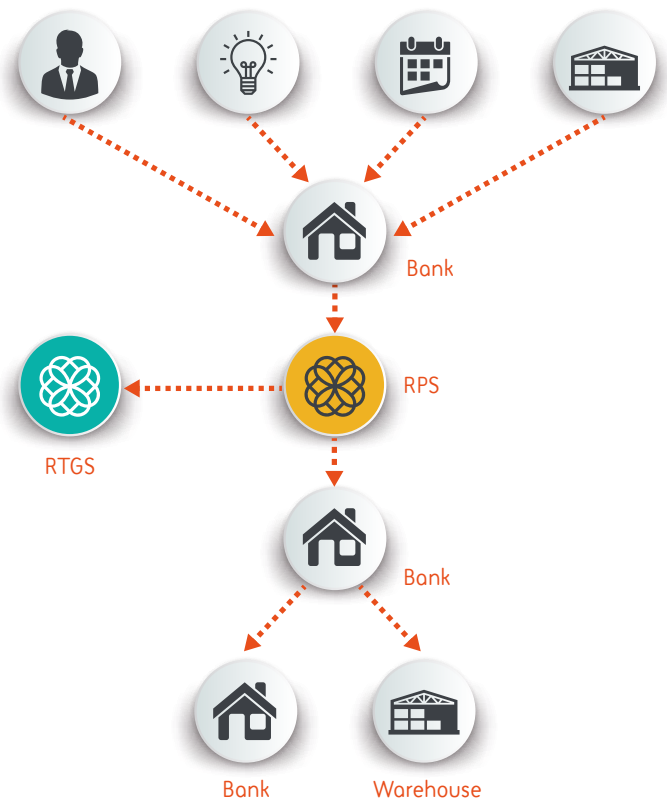
Rationale: Successful attacks on SWIFT, RTGS, and RPS payment systems would yield high gains as they control the flow of money.

Target Areas: Participants

Financial Gain: ● **High**

Rationale: Attacks on Participants can yield US\$ millions for the attackers, as evidenced by the ongoing attacks on SWIFT members.

Banking and Payments Market Infrastructures and Participants Overview



Banking and Payments Infrastructure

Banking and Payments Market Infrastructure Risk Scenarios

For RTGS, the threat from APT groups is primarily focused on altering the ledger of settlement accounts maintained for RTGS Participants. To successfully cash out, the attackers would need to have further compromised the RTGS Participants affected, or impersonated another legitimate RTGS account.

For RPS, the cyber risk could target modification or falsification of individual payment instructions or the netting or authorisation mechanisms for payments to benefit the attacker. This would be a more direct cash out as attackers would receive funds to bank accounts that could then be extracted.

Overall, the risk scenarios for Market Infrastructures would be more complex than those affecting Participants.

Threat Factors

Ease of Attack



Market Infrastructure elements in banking and payments are generally harder to penetrate due to segregation, higher security resources and awareness of threat.

Reward per Attack



At the infrastructure level, rewards would be very high as the banking and payments infrastructure controls the flow of money.

Ease of Cash Out



Substantial effort would be needed to cash out – attacking elements such as RTGS, RPS and SWIFT is not the same as accessing a payment mechanism – and would require support further down the banking and payment ecosystem.

Repeatability



Once one attack had succeeded, the other operators would respond as it is a smaller group who are more aware of the threat. This makes attacks on Market Infrastructure less repeatable.

Stealthiness



There is generally greater capability to detect attacks with more investment in monitoring and fewer, more structured interactions that allow for more focused monitoring.

Traceability



Movement of funds between banks is traceable as there is structured, standardised communication with SWIFT providing an audit trail of movements.

Susceptibility Factors

Complexity



It is relatively simple with each nation's RTGS linked to one or more RPS with known standard interactions with SWIFT providing common messaging services.

Standardisation



At the infrastructure level, RTGS, RPS and SWIFT use structured messages and interactions.

Concentration



At the infrastructure level, there is generally high concentration of function in RTGS and RPS.

Regulation Oversight



At the Market Infrastructure level, RTGS, RPS and SWIFT are subject to significant oversight and regulation.

Transaction Speed



At the infrastructure level, RTGS is real time and some RPS (such as Faster Payments in the UK) settle several times per day.

Check & Balance



Links between RTGS and RPS are secured and messages authenticated. There would be checks during the day before period closes but handling large volumes would make checks difficult.

Banking and Payments Overview

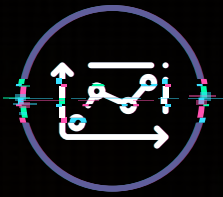
Banking and Payments Participants Risk Scenarios

There are a large number of Participants across many industries with varying levels of cyber maturity and complex, non-standardised processes and interactions with payments systems.

Payments systems are a supporting part of Participants' business and are not usually considered core to their operations. For example, the core business of a manufacturing company will tend to be the development and production of its product, with payments seen as part of its supporting function. This means there is potentially less focus and attention on payments systems and associated processes – which might well open the door to APT groups.

In addition to the vulnerability of their business systems to fraudulent payment instructions, Participants should also be aware of the risk of false communications and instructions being created. Such data – in the form of emails and spreadsheets – are often relied on without checks and, as a result, are ripe for exploitation by APT groups.





Trade Finance Market Overview

Trade finance supports domestic and international trade transactions and is decentralised with few Market Infrastructures. From a SWIFT perspective, trade finance messages may represent the lowest proportion of market messages sent⁴, but trade finance is a value, rather than volume business.

The trade finance market attracts a large number of diverse Participants including correspondent banks, importers and exporters, insurers, credit agencies, transport and logistics agents, and customs agents. There are also low levels of standardisation leading to poor quality data, complicated interactions and a continued reliance on paper documentation. Although there is a trend towards digitisation, this is acknowledged to be slow and is inconsistent amongst trade finance institutions due to the decentralisation.

Trade Finance Cyber Threat View

Trade finance Market Infrastructures are limited and could be seen as the banks providing trade finance services and developing infrastructures such as SWIFT's Trade Services Utility (TSU). More recently, the emergence of Blockchain is arguably the most significant technology trend in trade finance as it can potentially quicken transaction times and deliver self-executing "smart" contracts which will increase efficiency, reduce risk and enable greater participation and value generation in global trade.

An area that APT groups would potentially target is documentary collection and documentary credit – in both Market Infrastructures and Participants. These are trade finance methods that are the most complex in terms of the number and variety of Participants.

They also rely on documents, often physical papers, being the evidence to release goods or funds, and complex interactions – such as those between importers, exporters, their respective banks, customs and transport agents – are common. There are also uncertain timescales in the transaction – it can take days to clear customs and obtain the right paperwork. And there are also the non-standard terms and documents being relied upon and inherent trust in the process and between Participants.



All these characteristics provide APT groups with opportunities to influence and subvert documentary collections and credit. The combination of little standardisation and the widespread use of emails, spreadsheets and word processors, means that it is relatively simple for APT groups to gain access either to Participants or trade finance provider IT infrastructures and modify these documents.

Trade finance Blockchain platforms could potentially remove inefficiencies and reduce the risk of fraud. However, multiple competing Blockchain players in different stages of pilot and production, a differing set of approaches and uneven levels of technology and operational maturity all add up to an increased cyber risk, one that APT groups will seek to exploit by targeting automated matching and self-executing aspects such as smart contracts.

A potentially higher reward is on offer from attacks on Market Infrastructure as they would be handling multiple trade finance transactions for multiple Participants. However, such attacks and cash outs are more complex than those on Participants.

This means that the cyber risk to trade finance Market Infrastructure is considered to be medium term.

Participants

The same documentary collection and credit characteristics affecting Market Infrastructures also affect Participants. At this level, attacks would potentially be limited to particular trade transaction deals or agreed credit lines and loan amounts – so the rewards would be less when compared to Market Infrastructure.

However, Participants would also potentially be easier to attack due to higher numbers of Participants, a greater diversity of cyber maturity and less standardisation – all of which provide greater opportunities for the attacker.

This means that Participants are at a higher risk of cyber attack in the near term.

Market Impact

Target Areas: Market Infrastructures

Financial Gain: ● Low

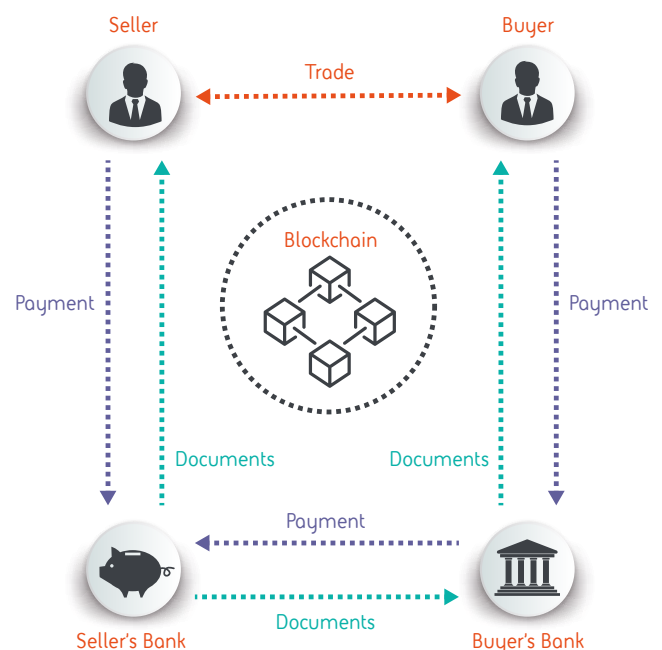
Rationale: There is relatively low financial gain as attacks would be targeting the bank side of specific trade finance deals.

Target Areas: Participants

Financial Gain: ● Low

Rationale: There is relatively low financial gain as attacks would be targeting specific trade finance deals.

Trade Finance Market Infrastructures and Participants Overview



Trade Finance Market Infrastructure Overview

Trade Finance Market Infrastructure Risk Scenarios

Given that Blockchain will likely become the de facto standard, multiple competing providers are racing to become the leading market provider. However, this accelerated process will perhaps lead to security flaws in the software that forms the Blockchain platforms or in the design and operation of interactions between the platforms and Participants. This will allow attackers to steal assets including by:

- Manipulating key information on the Blockchain, such as payment beneficiary details and confirmations, and then simply waiting for the automated self-executing aspects to deliver the assets to the attacker.
- Subverting or creating false nodes to manipulate the consensus decision process that underpins the Blockchain – thereby enabling the attacker to determine the outcome, such as approving payments, confirming conditions met or releasing of assets.

Threat Factors

Ease of Attack



Although SWIFT provides a TSU, trade finance is decentralised with little concentration of function. There is much diversity in the way trade finance services are provided between banks, and generally a higher cyber awareness compared to Participants.

Reward per Attack



There would potentially be higher reward in attacks on infrastructures as such systems would be handling multiple trade finance transactions for multiple Participants.

Ease of Cash Out



Attacks would need to influence the trade finance product to the benefit of the attacker – such as changing beneficiary details or confirming trade terms were met. Attacks would also potentially need to affect buyer and seller side banks.

Repeatability



Parts of attacks may be repeatable as there is some consistency in the way the market operates, but there is little standardisation in either Market Infrastructure providers or Participants.

Stealthiness



A range of interactions in unstructured formats such as emails and faxes, with complex documentary requirements and payment methods, make it potentially difficult to detect attacks.

Traceability



Banks and services such as TSU and Blockchain platforms would have records for trade finance transactions and products/services as these would be customer facing and require tracking.

Susceptibility Factors

Complexity



Trade finance is decentralised and based around corresponding banking relationships. There is little common infrastructure although some is emerging. Banks can provide various products but these can require multiple steps and lead times.

Standardisation



Trade finance is heavily dependent on physical documentation. There is some use of SWIFT messaging and emergence of TSU and Blockchain platforms, but these are minor aspects of the current market.

Concentration



There is low concentration of function – SWIFT messaging is used and Blockchain platforms will lead to more concentration but unstructured physical documentation is still prevalent.

Regulation Oversight



There are high level regulations such as Basel standards that regulate bank activities but this is mostly focused on capital/debt ratios and stability of the financial system.

Transaction Speed



Trade finance activities range from letters of credit paying out at 90 days to documentary collection checking which can take months. Blockchain platforms aim to increase transaction speeds but these are in early stages.

Check & Balance



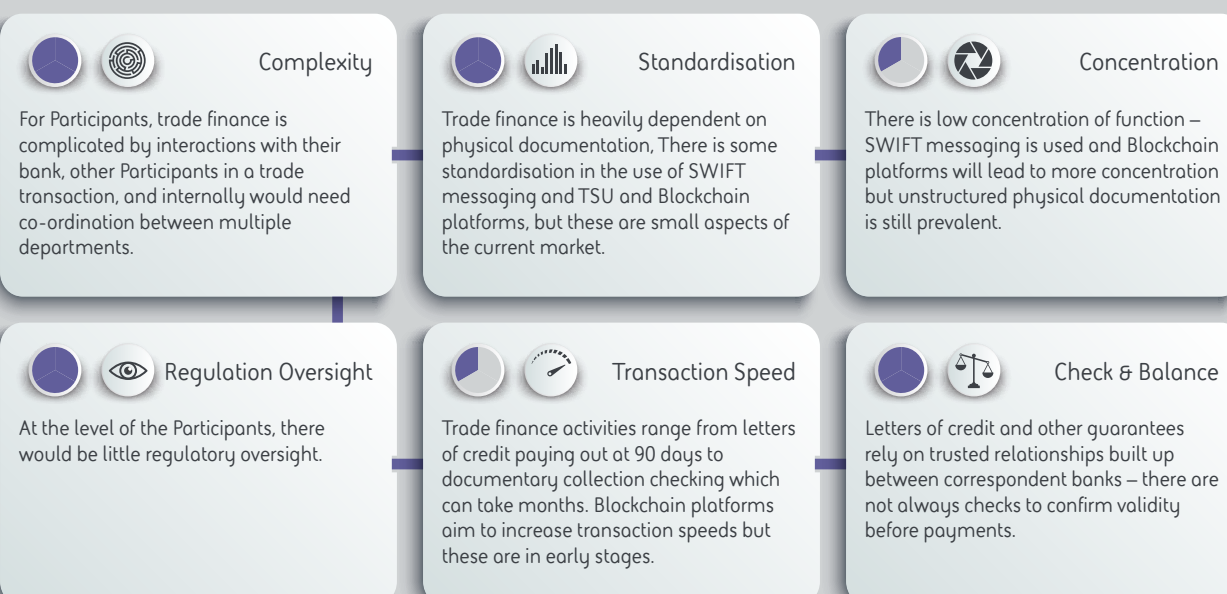
Letters of credit and other guarantees rely on trusted relationships built up between correspondent banks – there are not always checks to confirm validity before payments.

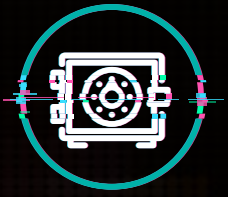
Trade Finance Participants Overview

Trade Finance Participants Risk Scenarios

At the Participant level, the inherent lack of standardisation and structure in processes and documentation and the reliance on unstructured and unverified communications combined with the higher numbers of Participants of differing cyber maturity levels, provides a wide field of opportunities for APT groups to take advantage of.

The exploitation of unstructured data – such as word processing documents and spreadsheets and modifying critical information such as payment details and terms to benefit the attacker – is a particularly important area of weakness.





Securities Market Overview

Securities make up arguably the most complex and diverse financial market areas including equities, debt and derivatives. It also involves a multitude of Market Infrastructures and Participants.

The focus of this paper is the secondary market (Over the Counter and Exchange trading of issued securities) rather than primary market (where new securities are issued) as there is more activity, infrastructure and Participants involved in the secondary market. From a SWIFT perspective, securities messages are amongst the most prevalent type representing around 46% of message traffic annually⁵.



Securities Cyber Threat View

In terms of Market Infrastructures, Central Counterparties (CPP), Electronic Trade Confirmation (ETC) and Central Securities Depositories (CSD), would potentially yield significant rewards. However, such attacks would require substantial effort because these are systemically important infrastructures and would be reasonably aware of the threat from APT groups, particularly when compared to Participants. They are also designed with known interactions allowing for more precise checks and balances. For example, exchange trading systems are intended to fulfil specific functions with specific allowed interactions with users.

The attacker would also potentially need to further compromise elsewhere in the trade lifecycle to cash out. So if a CSD was compromised and ownership of securities was changed, they would then need to be sold to cash out. This would require establishing an account with a broker dealer and a potential compromise at the broker dealer, clearing member and settlement agent.

However, the operation of securities markets is well known from the pre and post trade life cycle and the functions of Market Infrastructure and their interactions with Participants which the cyber threat will exploit. The interactions can be complex, non-standardised and unstructured and there are varying levels of automation, processing and manual handling which provide the attacker with a wide range of opportunities to target and exploit. The higher numbers of securities Market Infrastructure compared to other markets (there are some 60 major stock exchanges globally) means greater numbers of targets and hence more opportunities.

In summary, though less at risk than securities Participants, there is still a near term cyber risk to Securities Market Infrastructure which is higher than the other markets we have examined in this paper.

Participants

A fertile area for potential exploitation lies in the interactions between Participants and between Participants and Market Infrastructures. This involves taking advantage of the higher number of Participants with varying levels of cyber maturity, the non-standard, unstructured processes internally and between Participants – particularly their use of faxes and emails for communication, or managing critical trade data in spreadsheets.

Operations and practices in securities markets can sometimes be opaque, which has the effect of making it difficult to link actions, assets and owners/beneficiaries. This can be seen in anonymous trading where the identities of buyers are not readily revealed. There are legitimate reasons for anonymous trading (such as to prevent other Participants buying for arbitrage) but this anonymising can also benefit cyber attackers as it adds another layer of obfuscation to their actions.

Another example is the use of Omnibus accounts which aggregates securities into accounts under the control of the broker dealers and hiding the identity of investors from the market.

The cyber risk is therefore higher to Participants than to Market Infrastructures. And given the complexities in interactions, lack of standardisation of processes and interactions, and the sheer number and variety of Participants, their near term cyber risk must be classed as amongst the highest across all the markets reviewed.

Market Impact

Target Areas: Market Infrastructures

Financial Gain: ● High

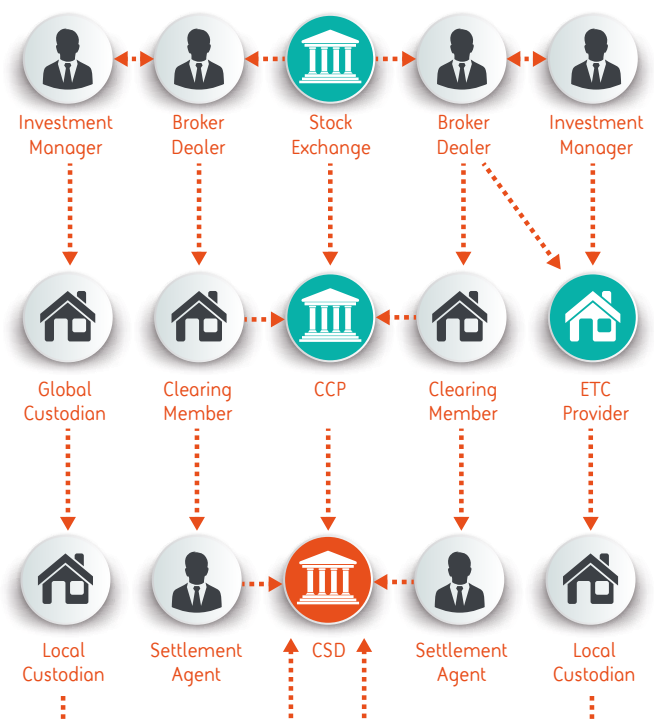
Rationale: Compromising securities market infrastructures would yield high gains. However, there are large numbers of Market Infrastructures globally so the gain would be dependent on the specific infrastructure and its controls and limits, such as its amount of collateral and securities.

Target Areas: Participants

Financial Gain: ● Medium

Rationale: The gains would be limited by the Participant's holdings and the attacker's investment if trading against Participant. For example, if shorting shares based on inside information, the attacker would still require investment to obtain the shares to short.

Securities Market Infrastructures and Participants Overview



Securities Market Infrastructure Overview

Securities Market Infrastructure Risk Scenarios

Market Infrastructures such as Exchanges, CSD, CCP and ETC all face significant risk scenarios. These include:

- Manipulating data held in the infrastructure itself, such as securities ownership in CSD and values, beneficiaries of trade transactions in CCPs and ETCs.
- Manipulating market and reference data such as Standing Settlement Instructions (SSIs) and pricing in information service providers that are relied on to enable fraudulent payments, relaying incorrect material financial information to influence share pricing or exploiting algorithmic trading through fake orders (market manipulation).
- Attacking the mechanisms which match trades and calculate settlement values to fraudulently increase the gain on trades to the attackers benefit.

Threat Factors

Ease of Attack



In the securities secondary market, there are many different securities markets and associated Market Infrastructures. These are also operated differently and so substantial effort would be needed to develop successful attacks.

Reward per Attack



For Market Infrastructures, there is a potentially very high reward if large values of securities were stolen by attackers.

Ease of Cash Out



The attack would need to move securities to the attackers' control. They would then need to sell to cash out without triggering scrutiny by Market Infrastructure operators.

Repeatability



Some elements of attacks may be re-usable but different markets may have different implementations of similar infrastructures – making repeatability harder.

Stealthiness



Securities markets are interwoven with interactions between multiple infrastructures and service providers. These complexities, together with market opacity, provide greater opportunity for attacks to be hidden.

Traceability



The use of Omnibus accounts, hiding of buyers, seller, beneficiaries and other complex finance and market practices potentially make it difficult to trace the ultimate beneficiaries.

Susceptibility Factors

Complexity



Securities has a complex set of Market Infrastructures with multiple interactions between them, as well as complex securities products and opacity in ownership due to market and financial practices.

Standardisation



The main phases of the securities trade lifecycle are broadly standardised with varying degrees of automation maturity.

Concentration



In securities markets, there is generally a high degree of concentration in Market Infrastructures.

Regulation Oversight



Different areas are regulated differently. For example, trading on exchanges is regulated and monitored but FinTech, is self-regulated and adopting technology faster so is potentially less prepared for the cyber threat.

Transaction Speed



Transactions speeds are increasing – recent years have seen high frequency trading in some securities markets with very fast transaction times.

Check & Balance



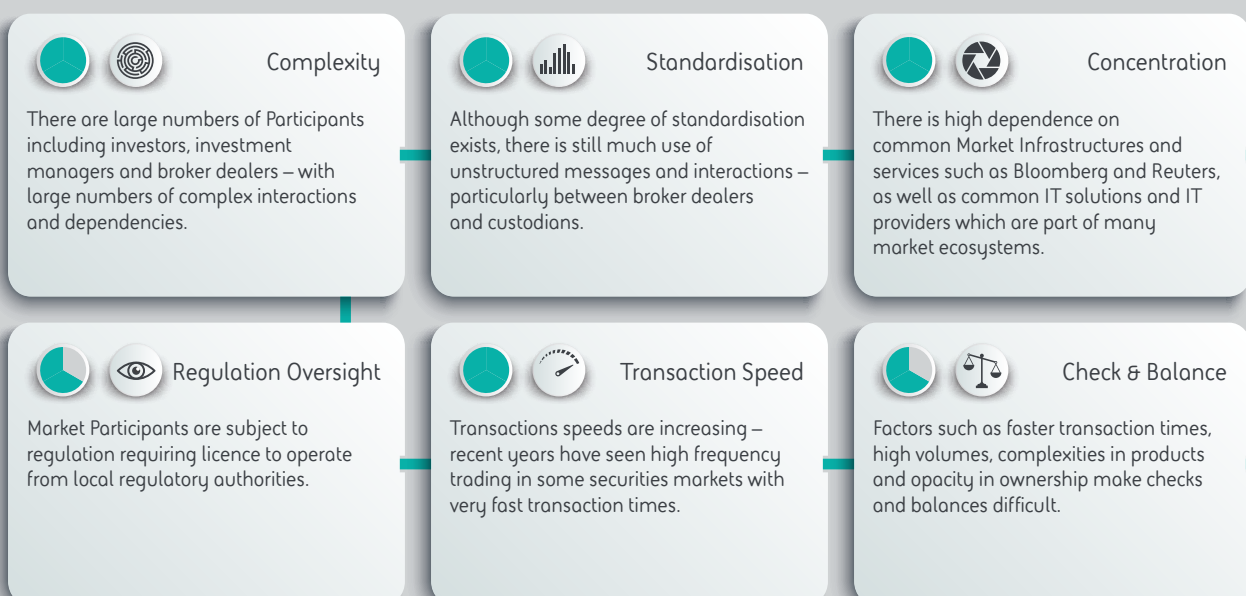
Practices such as Omnibus accounting, complex instruments, and long opaque chains of custody combine to make it difficult to perform checks and balances at Market Infrastructure level.

Securities Participants Overview

Securities Participants Risk Scenarios

For Participants, there are potentially more risk scenarios around falsification of information and communications relying on the complex, unstructured processes Participants use. For example:

- Falsifying trade orders and exploiting unstructured communications and data such as email and faxes used for orders, changes and confirmations.
- Exploiting market practices, including “delivery free of payment” to steal securities.
- Falsifying instructions to Market Infrastructures such as CSD, requiring changes in securities ownership or changing SSIs at reference data providers.





Threat Factors Scoring



Ease of Attack

1. High effort
2. Medium effort
3. Low effort



Reward per Attack

1. Low return
2. Medium return
3. Very high return



Ease of Cash Out

1. Hard to cash out
2. Some effort needed
3. Simple to cash out stolen assets



Repeatability

1. Attacks would be custom one off
2. Parts of the attack are repeatable
3. Attacks are repeatable



Stealthiness

1. Attacks would likely be detected
2. Attacks may be detected due to some aspect of the target
3. Attacks are covert and hard to detect



Traceability

1. Traceable
2. Potentially traceable
3. Untraceable

Susceptibility Factors Scoring



Complexity

1. Low complexity
2. Medium complexity
3. High complexity



Standardisation

1. High standardisation
2. Medium standardisation
3. Low standardisation



Concentration

1. High concentration
2. Medium concentration
3. Low concentration



Regulation Oversight

1. Highly regulated
2. Lightly regulated
3. Little to no regulation



Transaction Speed

1. Slow transactions – greater than 2 days
2. Medium speed – 2 days or under
3. Fast transactions – up to real time



Check and Balance

1. Extensive checks and low inherent trust
2. Some checks and balances,
3. Low levels of checks with implicit trust

Stay compliant in
the **fight against**
financial crime
with BAE Systems
and SWIFT

SWIFT
BAE

Appendix

¹ The Evolving Cyber Threat to the Banking Community, BAE Systems & SWIFT, November 2017

^{2, 4, 5} <https://www.swift.com/about-us/financials>
2017 SWIFT Annual Review

³ <https://www.fca.org.uk/events/future-horizons-conference>

About SWIFT


SWIFT is a global member-owned cooperative and the world's leading provider of secure financial messaging services.


Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories, enabling them to communicate securely and exchange standardised financial messages in a reliable way. SWIFT's Customer Security Programme, which launched in June 2016, is a dedicated initiative designed to reinforce and evolve the security of global banking, consolidating and building upon existing SWIFT and industry efforts. Within the Programme, SWIFT has established an information sharing initiative and created a dedicated Customer Security Intelligence team, bringing together a strong group of IT and cyber experts.

The team undertakes forensic investigations on security incidents within customer premises related to SWIFT products and services; the related intelligence is published in a readily readable and searchable format in the 'SWIFT Information Sharing and Analysis Centre' (SWIFT ISAC) a global portal which is available to the SWIFT community. By feeding back this intelligence in anonymised form to the wider community, SWIFT aims to help prevent future frauds in customer environments.

SWIFT, Avenue Adèle 1,
B-1310 La Hulpe, Belgium

W: swift.com

 [linkedin.com/company/swift](https://www.linkedin.com/company/swift)

 twitter.com/swiftcommunity

About BAE Systems


BAE Systems help nations, governments and businesses around the world defend themselves against cyber crime, reduce their risk in the connected world, comply with regulation, and transform their operations.


We do this using our unique set of solutions, systems, experience and processes - often collecting and analysing huge volumes of data. These, combined with our cyber special forces - some of the most skilled people in the world, enable us to defend against cyber attacks, fraud and financial crime, enable intelligence-led policing and solve complex data problems.

We employ over 4,000 people across 18 countries in the Americas, APAC, UK and EMEA.

BAE Systems, Surrey Research Park, Guildford
Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/swift

 [linkedin.com/company/baesystemsai](https://www.linkedin.com/company/baesystemsai)

 twitter.com/baesystems_ai

Copyright © S.W.I.F.T. SCRL ("SWIFT") 2018. All rights reserved.

Copyright © BAE Systems plc 2018. All rights reserved.

SWIFT and BAE Systems supply this publication for information purposes only.

While every effort is made to report accurate and truthful information, SWIFT and BAE Systems make no representations about (and are not liable for) the accuracy, completeness, reliability, suitability or availability of the data and information included in this publication.

This document may include general guidelines or recommendations or interpretation of data.

The recipient is solely and exclusively responsible for deciding any particular course of action or omission and for implementing any actions or taking any decision based on the information in this publication.

SWIFT and BAE Systems disclaim all liability with regards to such actions or decisions and their consequences. Nothing in this document shall be interpreted or construed as constituting any obligation, representation or warranty on the part of SWIFT or BAE Systems.

The following are registered trademarks of SWIFT SCRL: SWIFT, the SWIFT logo, MyStandards, 3SKey, Innotribe, Sibos, SWIFTNet, SWIFT Institute and the Standards Forum logo. Other product, service, or company names in this publication are trade names, trademarks, or registered trademarks of their respective owners.