A trusted world

Today we are witnessing a digital transformation that runs fast and is changing the face of the financial world. Customers are becoming more and more aware of security and trust is becoming a key element in building value relationships between companies and customers. Trust must be at the center of the digital transformation and must allow a new relationship that is creating new value toward the customers. Moreover, organizations did not examine fully the possible interactions that you may have between the financial contagion channels and the technological one. This is true even if the financial sector is at the forefront of information security and information sharing. Unfortunately, however, cyberattacks on financial institutions and their infrastructures are even more frequent and sophisticated, forcing organizations to invest in ever greater security with greater attention to mitigation and IT risk management. In parallel, the sector, together with national regulators and governments, have worked to improve and increase resilience and stability with the hope of preventing the recurrence of financial crises.

One of the aspects highlighted by regulators and governments is the loss of trust. Attacks generally affect consumer networks and do not always cause systemic impact; these phenomena, especially on a large scale, can lead to a loss of broad confidence such as to trigger, as a consequence, negative financial impacts. This is also linked to the issue of data integrity. Systemic impacts, resulting from computer intrusions that modify or influence data quality, can cause systems suspension until they are restored. Situation that has already been experienced by many organizations in the most recent cyberattacks such as WannaCry. Also in this case, a long-term restoration brings the theme of loss of confidence, increasing the systemic impact and increasing indirect economic damages. Share and further develop maps of critical financial structures, as well as financial processes additional relations, are important to better understand the overlay of cyber risk on the plumbing of financial institutions. Increasing exercises, at domestic level and cross-border, are even important, especially to create a bridge between senior-level executives from the financial institutions and cybersecurity communities. Stakeholders should be C-level executives from cybersecurity companies, regulators, banks, and central banks. The financial sector has always been a target and for mere criminal bank jobs or credit card theft, but far larger and more sophisticated attacks. It has never been so important to continue increasing resiliency and mitigate cyber risk guaranteeing financial stability and trust, where trust will be key in the customers relationships.

Enjoy the lecture…

Nicola Sotira
General Manager GCSEC

Cybersecurity (ENISA) and the Foundation for Hellas (FORTH) – The 6th Network and Information Security (NIS'19) Summer School is jointly organised by the European Union Agency for Cybersecurity (ENISA) and the Foundation for Research and Technology - Hellas (FORTH). The theme for this year is “Security Challenges of Emerging Technologies”.

IDM EUROPE 2019
Location: London, UK
Date: Sep 17, 2019
https://whitehallmedia.co.uk/idm europe sep 2019/

Businesses are under increasing pressure to protect their critical data assets, ensure regulatory compliance, and offer great user experiences in the digital domain for both employees and customers. To keep up with new and emerging risks – while also embracing the fullest potential of disruptive technologies like cloud, IoT, blockchain, AI and big data – enterprises are evolving to a different security paradigm, one that puts identify at the heart of their security model. IAM leaders are consequently faced with a new set of challenges which include aligning their IAM projects with business goals, identifying and responding to risks, and implementing successful next-generation identity architectures and technologies.

CYBERTECH EUROPE 2019
Location: Rome, Italy
Date: Sep 24-25, 2019
https://italy.cybertechconference.com/

An impactful event featuring thousands of representatives from across Europe, Italy, and around the world on the cyber world’s main stage! From lectures, to plenary sessions and VIP speakers, CyberTech Europe 2019 will feature an extensive exhibition […]
Cyber threats in financial markets, the continuous challenge as studied by SWIFT and BAE Systems
By Marco Fiore - GCSEC

Impacts of data theft on stock value
By Massimo Cappelli and Marika Mazza - GCSEC

Facing cyber threat is becoming a daily challenge for financial markets. This sector is increasingly becoming the focus of cybercriminals, from banking trojans affecting individual customers, through systemic threats posed to availability and integrity by ransomware,

to targeted attacks from Advanced Persistent Threat (APT). Attackers’ landscape is extending on a daily basis, and Financial Markets have to deal with this inevitable evolution.

The report, presented by SWIFT SCRL with BAE Systems, shows clearly the evolution of this threat and explains the main reasons why Financial Markets are one of the favorites hackers’ target to attacks.

A famous quote reads: “Follow the money and you will find “cyber criminals”.

As we could see the evolution in financial threats strictly follows the evolution of technology and interests. From initial banking Trojans

Golang Malware Targets Linux-Based Servers
A cryptominer campaign has been targeting Linux-based servers using a new Golang malware, according to research published by F5 Labs. Though not often seen in the threat landscape, the Golang malware was first identified in mid-2018 and has sustained throughout 2019. Researchers noted the latest operation, which has infected an estimated several thousand machines, began around June 10. The first exploit requests were identified around June 16. Using the cryptonight algorithm to mine XMR […]

"Agent Smith": The New Virus to Hit Mobile Devices
Check Point Researchers recently discovered a new variant of mobile malware that has quietly infected around 25 million devices, while the user remains completely unaware. Disguised as a Google related application, the core part of the malware exploits various known Android vulnerabilities and automatically replaces installed apps on the device with malicious versions without the user’s interaction.

So far, the primary victims are based in India though other Asian countries such as Pakistan and Bangladesh are also impacted, as are even a noticeable number of devices in UK […]

Popular Malware Families Using ‘Process Doppelgänging’ to Evade Detection
The fileless code injection technique called Process Doppelgänging is actively being used by not just one or two but a large number of malware families in the wild, a new report shared with The Hacker News revealed. Discovered in late 2017, Process Doppelgänging is a fileless variation of Process Injection technique that takes advantage of a built-in Windows function to evade detection and works on all modern versions of Microsoft Windows operating system […]

1 The Evolving Advanced Cyber Threat to Financial Markets


A famous quote reads: “Follow the money and you will find “cyber criminals”.

As we could see the evolution in financial threats strictly follows the evolution of technology and interests. From initial banking Trojans
attacks such as ZeuS, Dridex, Shylock, Carbanac APT\(^2\), or promoted by groups like the famous Hackers Lazarus Group\(^3\), the threat has moved to markets and participants. Referring to those two targets, the Report underlines four main different scenarios of analyzed market: FX Markets, Banking and Payments market, Trade Finance and Securities market. Each of these markets are composed by two main groups: “Market Infrastructures”, the environment and financial instruments, and “Participants” who make use of these infrastructures to execute transactions.

Although the first two sectors, FX Markets, Banking and Payments market, have strong regulation and standardization models; trade finance and securities are far more complex and have more non-standard and unstructured interactions.

1) FX Market: It is arguably the world’s largest (by volume) and most liquid financial market and is vital to global trade and money flow.

2) Banking and Payments market: it covers the fundamental movement of money between organizations and individuals and therefore underpins all other markets.

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

4) Securities: critical to the global economy, securities is maybe the most complex and diverse financial markets, and include many market areas such as trading equities, bonds and derivatives.

Analyzing the two main groups we could clearly understand that the main vulnerabilities could be found in “Participants” because of its intrinsic essence as a human factor.

According to experts there are 3 main reasons why actors are the real and main weak point:

**No safety in numbers:** Participants’ maturity but also the increasing interaction and complex processes between them, gives more opportunities for cyber threats to exploit.

**Less focus on cyber risk:** Participants can interact with multiple markets and multiple operations. This operational complexity does not allow a global view of the scenario so that “Participants” can’t focus everywhere and all of the time.

**Misplaced trust:** Manual and automated hybrid processes make more complex the financial environment. Automatized interaction sometime makes reliant people of the system and that trust view could provide plenty opportunities for APT groups to exploit.

As we can read in the Report in fact “people can be lulled into a false sense of security and trust the machine which cyber attackers will exploit”.

Another important factor impacting the system is the rise of FinTechs and other new entrants that are shaking up markets and are causing increased disruptions. Technological innovation and better competitiveness are a powerful trend but are contributing in increasing cyber risks as new factors and most of services and ways of working are immature and unable to withstand cyber threats.

The Report underlines clearly how a holistic approach is necessary. We have to consider Cyber Security not only a technical issue but also a must for all the company that involve all levels of an organization – from the board right through to operations and its markets.

**Building coordinated Teams:** In such direction all the “Participants” inside the Market have 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.

**Think like an attacker:** in reviewing policy, procedures, tools and process “Participants” should 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. Thinking like an attacker could be more predictive and could help people and organization to prevent cyberattacks.

**Approach and Objective of APT groups in Financial Markes**

Rather than analyzing the tactics, techniques and procedures that attackers may deploy, the Report examines what cybercriminals might attack, and why.

Taking for granted that APT groups are patient, structured and well-resourced, financial community should be always prepared to face up to cyber criminals’ attacks.

APT threats and attackers usually follow the same route: infiltrate the target, move laterally across the

---


\(^3\) Lazarus Group - https://attack.mitre.org/groups/G0032/
network deploying malware, learn how the organization work and how are set systems and procedures, eventually initiate the attack and duly cover their tracks.

SWIFT Report underlines the importance of the relationship between assets and target areas. In this article, for need of synthesis, we take into consideration the more critical areas that SWIFT AND BAE SYSTEMS have highlighted: FX market, Banking and Payments Market and Security Market.

The first sector analyzed is the **FX Market**. Foreign Exchange Market it is by far the largest market in the world (in terms of transactions). It includes exchanges between large banking institutions, central banks, currency speculators, multinational companies, governments, and other financial markets and institutions. 24hday (excepted weekends) the exchange activity that takes place in the global FX markets amounts to more than 4,000 billion dollars a day. The infrastructure level is settled on three different types of trading OTP (Over-the-Counter or Off-exchange) done directly between two parties, without the supervision of an official exchange and CLS (Continuous Linked Settlement) a settlement system for all multicurrency interbank payments which deals with 17 currencies and commonly used currency trading platforms.

In that case 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. Potential financial gains would be very high if Market Infrastructures such as settlement institutions, common trading platforms and infrastructure – including SWIFT – were compromised. In terms of simplicity it’s evident that cyber risk, due to the nature of the transactions, is much higher compared to FX Market Infrastructures. Attackers that manipulate individuals could gains lower margin trades, as well as smaller amounts available from each Participant.

Attacks against the small number of FX Market Infrastructures would take significant effort. Because of their importance is understood and there is greater awareness of cyber threat. On the other hand successful attacks would potentially yield high rewards due to the daily volume and value of FX transactions.

**Banking and Payments Market.** From a SWIFT perspective, “*payments messages are highest in terms of volumes of messages sent annually and there are more members sending payments messages than any other type*”. Banking and Payments Market infrastructure systems is split into two types the RTGS (Real Time Gross

---

Settlement) systems and the Retail Payment Systems (RPS). It’s true that Market Infrastructure elements in banking and payments are generally harder to penetrate due to segregation because of higher security resources and widespread awareness of threat but a successful attacks on SWIFT, RTGS, and RPS payment systems would yield high gains as the banking and payments infrastructure that controls the flow of money.

At the same level attacks on Participants can yield US$ millions for the attackers, as evidenced by the ongoing attacks on SWIFT members. Rewards are very high as shown by the Reported losses (into US$ millions) from the ongoing SWIFT payment attacks and in addition those attacks are harder to detect and are reliant on spotting ad hoc fraudulent payment messages and/or reconciliation processes in high volumes of transactions. The architecture of the infrastructure, driven by the trust of automating payment processes, leads Participants to do not check all payments if submitted via the correct process/system. Whilst there are general trends towards automation and digitization, there is still low maturity in IT and manual processes.

The third market analyzed by the Report is **Securities Market**. As anticipate before Security Markets are composed by the most complex and diverse financial market areas including equities, debt and derivatives. In terms of Market Infrastructures, it is composed by Central Counterparties (CPP), Electronic Trade Confirmation (ETC) and Central Securities Depositories (CSD). In this context, most operation of securities markets are well known from the pre and post trade life cycle for the functions of Market Infrastructure and their interactions with Participants. 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 for cyber attackers.

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.

The gains for criminals would be limited by the Participant’s holdings.

Securities markets are linked with interactions between multiple infrastructures and service providers. On the opposite these complexities, together with market opacity, provide greater opportunity for attacks to be hidden. This complexity is reflected also on the large number “Participant” in this Market and it includes investors, investment managers and broker dealers – with numbers of complex interactions and dependencies. From an attacker point of view, the huge market and its complexity means that they have necessarily to increase the effort in terms of “criminals” (physically operational people) and financial resources.

**Conclusion**

The question is: What we have to do if cyber risks are increasing day by day? The answer is well known but not always applied. Surely a continual improvement is the cornerstone of any security program and the Report suggests the following useful advices:

**Securities Participants**

Communication and 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.
In 2017, in the third issue of the Cybersecurity Trends Italian magazine, I wrote an article about the impact of misinformation on stock value. It was about the November 2016 US presidential election: "In mid-November 2016 was reported an interview of the CEO of a beverage company by a US conservatives blog. In that case the CEO stated (as an obliged condition) that Trump supporters should take their business elsewhere”.

The same day the news was reported and the rating of the company fell by about 35%. The share price on the same day fell by 3.75% and for the remaining part of the month fell by more than 5%. These two facts may be not associated but it was still a “use-case” discussed by brand reputation and communication analysts.

In addition, I also cited examples related to the "Pump & Dump" technique, i.e. pumping and “pass the buck”.

Disinformation becomes a very powerful and difficult instrument to stem with if we do not anticipate it with a pervasive and transparent communication strategy. From here, other considerations are born related to the share value impact, not only about disinformation but also about cyber-attacks against companies. The question was: "Does a cyber-attack, with consequent data theft, impact the share value of a company?"

Marika, a student of Economic Analysis at La Sapienza University of Rome, has studied the issue Efficient Market Hypothesis. During the internship at the GCSEC Foundation, she analyzed the phenomenon mentioned above based on her experience and on indications provided.

The analysis focused on identifying the effects of cyber-attacks on the performance of equities stocks. The attacks taken into consideration for the analysis come from external sources; in particular have been aggregated the following attacks: data destruction, data loss, data alteration, unauthorized data disclosure or process such as data access, data transmission, data retention or processes of personal data - (i.e.: data access or data acquisition by unauthorized third parties; inability to data access due to accidental causes or external attacks, viruses, malware, etc., personal data disclosure). The label associated to was: data breach. No distinction between attacks was needed because the impact was the same for all.

The results is based on 37 significant attacks from 2016-2019. Selected companies have been divided according to the listing exchange. The Aggregates are 3: New York Stock Exchange (18 companies), NASDAQ (11 companies) and Other (Tokyo, Oslo, London etc. 8 companies). The distinction on three major groups is related to the fact that North America States were the most attacked and for them information was most widely available. The 37 companies analyzed are: 27 Americans, 3 British, 2 Canadians, 2 Chinese, 2 German and one Norwegian.

The study is based on the financial literature of the Event Study, a methodology of analysis that studies the behavior of a time series at a given event. The most common Event Study approach generally involves three steps:

1. The estimate of the parameters in the chosen period;
2. The evaluation of the aggregate result for all the companies and, at the same time, the consideration of the average effect;
3. The estimate of the Abnormal Returns to isolate relevant characteristics of the title that influence the impact of the publication of the event.

Significance is related to the amount of data stolen, the selection parameter is “at least 5000 per type of data” (at least 5000 accounts, at least 5000 credit card profiles, at least $ 5000 in reference to losses), the selection criterion was useful to avoid considering too insignificant impacts whose detection would have generated outliers.
The abnormal Return of stocks, is obtained as the difference between the normal and expected performance in the absence of occurrence event and the current yield calculated during the event period. The market model is adopted in relation to the return on the market portfolio and in order to estimate the normal return of each company. The comparison is instead made with the corresponding market index or IXIC for Nasdaq, GPSC for New York Stock Exchange and a general index for the remaining markets.

The period for estimating the expected yield of shall be in the 120-day estimation window, which shall be interrupted 10 days prior to the event in order to obtain not-distorted values. It is stressed that Data Breach are almost never announced promptly. In the forecast analysis, to prevent effects from distorting the share value, the period prior to the announcement is not considered. The event window, instead, starts in the immediately in the following period (-10, +10) chosen for the actual analysis. It was also considered the short period and not the long one.

The event windows selected for the Cumulative Abnormal Returns estimate are centered on the 3-day report (event date) (-1, +1). It was then possible to calculate the average response in the entire sample (Cumulative Average Abnormal Return, CAAR) and results were subjected to statistical verification that has to be different from 0.

Below the results obtained from the analysis:

- **New York Stock Exchange (NYSE)** - On 18 companies attacked, the graph indicates the fluctuations of the Abnormal Returns. The impact of the announcement is different from zero, sometimes deviating slightly from it and sometimes even positive. The share value and the trading volume of the shares has changed on the trading day, but this does not differ from the expected normal return. The fluctuations, present within the graph, can represent events of different nature that in the estimate have been omitted, events probably related to the company and not to the market (the events related to the market have been incorporated in the estimate of normal returns through the 'index ^ JPIC). Through CAAR index, the investigation wanted to underline a general effect that could give a universal answer to the companies examined. The impact on the share value of the stock caused by the event is therefore -0.0226%, a negative and very small value, therefore it is really difficult for an investor to decide to change positions on a stock following such events, if it did, his choice to change would still be limited in the very short term, even a day-to-day choice.

- Even on NASDAQ the impact is minimal, greater than the NYSE, but still very moderate. Overall it is -0.0762%. The second picture shows the trend of daily abnormal returns and . The scheme is the same. In addition, settlements occur on the next day immediately to the announcement. The event does not propagate. When it is small, it is imperceptible on financial market.

- Other markets. In the remaining markets the impact is minimal as well. It seems to be sometimes zero and the value captured in this analysis is equal to -0.0086%.
Conclusions

It seems that cyber-attack, compared to other phenomena, determinates minimal impact on the stocks return of the business. This allows us to make some considerations.

The first one is that this type of attack is not useful to premediate an eventual climb to acquire more shares. Moreover, it highlights the fact that the loss of information is something that affects more compliance and consideration levels rather than the propensity to purchase stocks.

It is emphasized that such attacks, due to the sanctions related to them, are considered as a disputed announcement from markets point of view.

In the stock market, prices reflect the behavior of agents who are rational for economic theory, but for the new strands of finance this is not a sufficient hypothesis.

Agents do not move only based in risks and financial returns, in fact, the perception of the event is a pivot in decisions and if the disinformation spreads, the effects are sedated.

In the future, with the massive digitalization of services, something could change, but now the results of the analyzed cases had suggested to not deepening or expanding this analysis to understand impact effects.

Differently, disinformation may deserve an in-depth analysis.

Further relevant studies should be conducted on the impact of disinformation or on the expansion of the dissemination of news through bots, such as happened during the European campaigns, on investments or on companies’ stock in countries involved political elections.