Mitigating cybersecurity challenges in the financial sector with Artificial Intelligence

CENTRE FOR FINANCIAL REGULATION AND INNOVATION

White Paper

Mitigating Cybersecurity challenges in the Financial Sector with Artificial Intelligence

Chenle Jiang[1†] | **Daniel Broby**[1*]

[1]Strathclyde Business School, Glasgow, Scotland

Correspondence
Daniel Broby, Department of Accounting and Finance, Stenhouse Wing, 199 Cathedral Street, Glasgow G4 0QU
Email: daniel.broby@strath.ac.uk

Funding information
Department of Accounting and Finance.

This paper investigates the evolving cyber threats landscape. This includes the phenomena of ransomware and the risks that such threats have to financial corporations. Cutting-edge technologies, such as Artificial Intelligence, could potentially have an influential impact on detecting cyber intrusions and protecting sensitive and critical business information, as well as ensure privacy. We comment on a framework that explains the causes of reported cyber incidents and the consequences of IT systems breakdown. This is done using fault tree and event tree risk analysis models. The results show that applying Artificial Intelligence techniques can increase the probability of the monitoring systems detecting anomalies and reducing threats. Although the cost benefit of implementing such techniques is still uncertain, they appear to be related to company characteristics such as size and maturity level. We therefore recommend that companies adopt such measures as part of their IT security protocols.

KEYWORDS
Fintech, Cybersecurity, Artificial Intelligence, network security.

Abbreviations: FTA - Fault Tree Model; ETA - Event Tree Model; AI - Artificial Intelligence; IT - Information Technology.

* Director, Centre for Financial Regulation and Innovation
† MSc Fintech

1 | INTRODUCTION

We investigate the defensive mechanisms used by financial companies to protect their cyberspace and mitigate the inherent security risks. We define cyber crime as "crime committed in a computer enabled fashion". We observe that the world is experiencing a dramatic digital transformation. As a result of the internet, it has moved to an intelligent paradigm. Corporations now embrace digital and networked computing. Economies and societies are more closely interrelated. Without the boundary of borders or industries, they share a common cyberspace that facilitates their interaction. Indeed, the convenience and advantage this facilitates makes corporations more vulnerable to cyber attacks from outside their firewalls. It also makes them vulnerable to intrusion from insiders. The interconnected and shared characteristics of digital enterprises increases the threat from such attacks. We therefore suggest that Artificial Intelligence and quantitative risk analysis can be used to assess and mitigate this threat.

The science of cybersecurity is multidisciplinary. It encompasses adversarial engagement, attack, defence and mitigation. Cyber security can be divided into three key arenas of threats, (1) vulnerability, (2) response and (3) legal redress. These threats and incidents are changing in scale and magnitude. Mitigation of these is either done in a defensive or offensive way. To have a proper picture one has to understand the threat actors. These can be state, criminal and other malicious stakeholders. There is proliferation of technique by all of these but clearly a different magnitude in terms of resources available to them. This impacts their tactics techniques and procedures (TCP's).

State military grade cyber tools have developed dramatically, particularly in the last few years. That said, large-scale state attacks are a rarity. The only time a critical infrastructure attack that has been documented was a cyber attack on Ukraine. This does not mean, however, that the capability is not there. That said, State resources have been deployed against companies and organizations. For example, in 2020, the World Health Organization was allegedly attacked by a Vietnamese source. On the whole, however, state attacks are mostly targeted at intellectual property. As such, the threat from state threat actors is real and heightened.

Investigation of risk mitigation is important because the Internet is becoming more susceptible to diverse and sophisticated cyber crimes. The financial sector is the main target, largely because of the ease of transferring money digitally. According to the World Bank (2018), customers of financial services suffer 65 per cent more cyber attacks than those in any other industry. The majority category of attackers for financial breaches is quite different from those for espionage breaches. Likewise, the detection methods vary accordingly. Within finance, there is great emphasis on automating threat detection.

The enhancement of cybersecurity protection has become a priority in many financial institutions. Various monitoring and detection systems have been developed to identify cyber attacks. However, in the constantly evolving threat landscape, it is critical to equip such corporations with advanced and innovative tools to take control of the threat. We suggest these can be supplemented by Artificial Intelligence techniques which can enhance and improve such approaches. This paper therefore identifies these and where they can be deployed to best effect.

With cybersecurity concerns in mind, we provide a framework of the potential application of Artificial Intelligence techniques. This can help detect cyber attacks and mitigate the cybersecurity challenges in the finance industry. We begin with a discussion of industrial and academic research into both cybersecurity and Artificial Intelligence techniques. We suggest an infrastructure for measurement of cyber risk and its impact with fault tree and event tree models. Using these, we are able to classify the complex cybersecurity environment and any resulting system issues.

2 | THE STATE OF CYBERSECURITY IN THE FINANCIAL SECTOR

The definition of cybersecurity is varied because it is an interdisciplinary concept. Kizza (2014) describes it as operating in multi dimensional space where information moves between computer and computer clusters. There is a lack of consensus on its fundamental aspects, such as the access to information and its secured sharing properties (Thakur et al, 2015). We suggest it is not necessarily only the protection of cyberspace that needs attention (Solms and Niekerk, 2013) but also the entities that function in cyberspace, and the assets that can be reached from it. Amoroso, (2006) believes it is best conceptualized by "the tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications"

Recently, academics have begun to interpret cybersecurity from an economic and psychological approach, rather than technological one. They argue that essentially cyber crimes are driven by rational cost-benefit calculations and that intangible perceptions such as feelings of fear and insecurity of the virtual world, and a lack of awareness, have significant influence on cybersecurity (Lagazio et al, 2014). This highlights that the threats from external hackers, espionage, terrorism attacks, internal data leakage, malicious revenge and cyber bullying, cover a wide scope and multiple classifications.

The increasing volume of cyber threats and the more sophisticated and diverse means of conducting such crimes are well documented. Emerging and innovative technologies are in the hands of cyber villains, who are making illegal gains rather than benefiting society. Organizations are increasingly fearful about the vulnerabilities resulting from new tools and channels. According to the Global Information Security Survey done by EY (2018), 77 per cent of respondents are concerned about the lack of user awareness and behaviour exposing them to the risks through mobile devices. The survey vulnerabilities are shown in Figure 1. Some 50 per cent of respondents are worried about the loss of such devices and the further loss of information and identity they may contain. Careless (or unaware) employees are among the top risk exposures.

Organizations have to be prepared for sunburst attacks. This is where threat actors that address the supply chain. Such attacks have become more common since code was injected into Micorsfot and Solarwinds software in September 2019. The attack was attributed to Russian government, however they deny any involvement. This type of attach results in malicious code being transmitted to customers who update to the latest piece of software. This in turn gives attackers remote access to the third parties. White hat hackers - malicious activity for so called ethical motivation - are just as dangerous. This is because the issue is vulnerability. There is a weak correlation between cyber security spend and robust defence of networks.

Dwell time is how long the average hostile intruder is inside a network. Hang and Dong (2019) suggest minimizing the average dwell time is important. In Europe, this figure is averaging one hundred days. The threat, comes from within the organization as well as from outside. Very few teams have the technical ability to deal with an enterprise wide attack. Where ransomware is used, it makes sense to have a policy on how to handle the threat and operational consequences before hand.

In Financial Services in the UK. The Financial Conduct Authority (FCA) has provided significant guidance on cyber risk. The FCA expects firms to have adequate systems and controls to be able to recover from cyber attacks. This is matched across into the Prudential Regulation Authority (PRA) that requires procedures in place for the protection and response to breaches. Typically, the requirement to report an attack to these bodies is 72 hours, including to the information commissioners office. The FCA is also concerned about the practice of spoofing in high frequency trading. Broby et al (2019) propose the precision times-tamping of orders and regrouping trades as a way to mitigate this practice.

The current regulatory focus is to acknowledge "you are as week as your weakest link". As such, the FCA is focusing

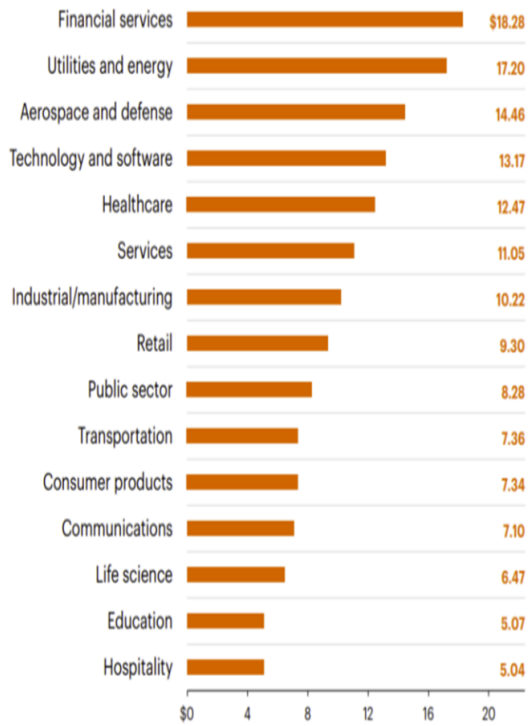

FIGURE 1 Vulnerabilities and threats perceived to have most increased the risk exposure. Average annual cost per sector in USDm. Source: 20th Global Information Security Survey 2017-2018, EY.

on outsourcing and resilience. The Network and Information Systems Regulations (2018) and the Global Data Protection Regulations (2018) apply. There has been a clear regulatory shift from sympathy to a compensation culture. At the same time, there is an ongoing debate with the insurance industry over coverage and exclusions. There is also a stronger focus on third party supply chain risk. Attacks on hardware can control a system within three to four minutes. As such, the problem isn't just a software one. States and well organised criminals have the ability to target both hardware and software simultaneously. Indeed, a high level attack like this can be done without much of a fingerprint.

There are a number of issues that make cyber threat worse. There is a lack of dependable vendor remote access management. Out of date infrastructure adds to vulnerabilities. There is also a lack of cyber awareness at board and management level. The advent of Covid 19 has made the problem worse, because home working is being done on less secure computing. There is a marked rise in man in the middle attacks, where a legitimate email is compromised and account data changed.

The severe and growing cybersecurity threat is identified by several reports and studies. The cost of cyber crime study (Ponemon and Accenture, 2018) revealed that the average number of successful breaches per company has grown 27.4 percent to 130 percent in a single year. Malware accounts for a large proportion of cyber attacks. Overall malware variants growing percentage of 88 per cent. Malware and phishing are the top two attacks that increase risk exposure to an organization. In 2017, there were about 670 million new variants that emerged and the growth was largely owning to the Kotver Trojan which consisted of 78 per cent of new variants (Symantec, 2018).

The rise in cryptocurrency adds another dimension. This phenomena has resulted in an 8,500 percent increase in detections of crypto minors on endpoint computers since 2007 (Symantec, 2018). The widespread use of cloud services and the expanding usage of Internet of Things (IoT) both accelerate the pace of cyber attacks and allow massive cyber attacks in a larger scale become more possible. Distributed denial of service (DDoS) is one of such tools. It is an approach that uses multiple computers to generate excessive amount of network traffic towards an internet-facing target. The frequency of attach exploiting 100 gigabits per second to attack the root DNS services of a network has jumped by 140 per cent in 2016 alone (Akamai, 2016). In thinking about designing a ransomware attack policy, the starting point should be what the worst outcome can be, then it should cover the appointment of external assistance and whether there is a negotiation policy. The frame is therefore to know what the response should be and what a corporations attitudes are to paying up to blackmail.

The financial costs of cyber crimes are also on the rise. During the past year and the annual cost of cyber attacks came in at £11.7 million per company. This is expected to grow substantially over the next five years (Juniper Research, 2017). The largest impact cyber crimes are currently related to ransomware, a growing type of malware that encrypts targets confidential data and demands a ransom for the company to recover access. One of the biggest and most influential ransomware attacks was in 2017, namely *WannaCry*. On May 12th of that year it exploited the *EternalBlue* vulnerability in the Windows operating system which is used to encrypt critical business files. The malware demanded payment in Bitcoin ranging from USD 300 to USD 600. It used a security loophole that allowed the phishing scheme to grant access to malicious code through shared files within organizations, without the permission of users. This destructive incident was reported to have infected more than 200,000 devices across industries and 150 countries. It caused huge corporate losses as detailed in Jones (2017). In fact, Microsoft had released an important patch for EternalBlue on March 14, earlier than the ransomware outbreak. The malware sent a wake-up call to those who had turned a blind eye to such threats and risks but was not adopted rapidly enough by industry.

Among all industries, the cybersecurity challenge within financial sector is unprecedented compared with others, not only in respect of the number of breaches but also in terms of the financial cost of incidents. The reason is that financial products and services, such as payments and transactions, savings and borrowing are major targets for cyber criminals. Moreover, the increased number of processes and use of robotics for automatic trading, outsourcing to

third parties all pay a part. Transactions across borders and the interaction with customers through multiple channels and devices possibly exacerbate cybersecurity challenges. As a result, financially motivated hackers, international intruders and manipulation, online fraud and phishing activities could potentially cause financial institutions to lose millions of values of assets. Besides, a single meltdown of system. Even a small glitch caused by negligence could put a company's reputation at risk and thus bring about further revenue loss and brand damage. According to the Ponemon and Accenture (2018) report, the average annualized cost of cyber crime for companies in financial services is USD 18.28 million, among the highest in total 15 industries.

The cyber security challenge is magnified by the incredible expanding and evolving threat landscape which is harnessing cutting-edge technology and intercorrelated global systems. This is happening across all countries and industries. There are concerns that their could be shortages of cyber specialists to deal with the number of attacks. The imbalance is likely to be much worse in the future. Humans are less competent in coping with such complex systematic risks characterised by opaque cause-and-effect relationships alone, thus we could use a little help from intelligent machines.

3 | ARTIFICIAL INTELLIGENCE

In its broadest sense AI indicates that a machine simulates and performs action that is a reflection of human thoughts. As early as 1950s, McCarthy et al (1995) stated that AI is "the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it". Barr and Feigenbaum (1981) mentioned that AI is a part of computer science concerned with designing intelligent computer systems that exhibit the characteristics associated with human intelligence behaviour – understanding language, reasoning, solving problems and so on.

Automation is great at large volume reduction. It can take threat intelligence information and sort it for the analysts to understand the threat. This is because visibility is key. If you have a lot of devices, they produce data and logs. It is the managing of these data-points that successful identifies intrusion. Artificial Intelligence, however, is simply means to help, not the solution. It helps reduce the sphere of the possible for the team defending the organization. It has been used in a number of finance applications. Swankie and Broby (2019) demonstrate how to utilise Artificial Intelligence to evaluate of banking risk.

The majority of AI studies have focused on narrow and specific questions and goals. Recently attempts are being made to develop and demonstrate systems that exhibit the broad range of general intelligence, which is referred to as Artificial General Intelligence (AGI). This shows promise as a cyber deterant. Various narrow AI branches appeared during its evolving path such as artificial neural network (ANN), machine learning (ML), genetic algorithms, fuzzy logic, natural language processing (NLP) and robotics. One of the classic examples of narrow AI approach is IBM Deep Blue (which beat the world chess champion after a six-game match in 1997). The architecture used in Deep Blue was applied to financial modelling including market trends and risk analysis, data mining which uncovered patterns and relationships in large databases and molecular dynamics. AI has been used to discover and develop new drugs (IBM, 2011). In 2011, a new IBM machine Watson defeated two of the most successful human players of a game Jeopardy. As more advanced software is developed with natural language, the door is opening to the new generation of human-machine interactions.

In terms of detecting cyber attacks and bolstering cybersecurity, AI certainly has a role to perform. There are various reports and substantial academic research that illustrates different approaches. AI can be used in detecting cyber attacks and mitigating security risks.

A survey based on 412 IT and information security professionals from medium to large organizations shows that

12 per cent of respondents said that they have extensively employed machine learning techniques for cybersecurity analysis and operations, while 27 per cent said that they implemented them on a limited basis (ESG, 2017). Machine learning is essentially a hybrid of data analysis and automation, providing predictions and detections by identifying patterns from large amount of data inputs. It also investigated the reasons for organizations to consider deploying ML techniques. Figure 1.3 shows that 29per cent of cyber experts intend to accelerate incident detection with ML techniques and 27per cent want to accelerate incident response.

4 | REASONS FOR DEPLOYMENT

The perspective of academia is given by Soska and Christin (2014) who provided an approach to design, implement and evaluate a novel classification system that predicts vulnerable websites before they turn malicious. They adapted several techniques from data mining to machine learning and built the system which would automatically learn from the data it acquired and parse and filter websites to extract features to be able to detect new attack trends quickly and efficiently. Choudhary and Vidyarthi (2015) suggested a dynamic analysis approach to understand and execute the behaviour of metamorphic malware and designed a classifier to quantify the behaviour of Portable Executable to make decisions of whether being malicious using machine learning methods.

Bitter et al (2010) focused on making use of artificial neural networks and variations on either host-based or network-based intrusion detection systems, trying to separate suspicious and potentially malicious traffic from ordinary traffic. They attempted to use ANN to resolve specific intrusions such as DoS, worm and spam and they pointed out that the key to a successful model is the choice of appropriate data reflecting implicit domain knowledge. Jongsuebsuk et al (2013) considered to use genetic algorithm to help find appropriate fuzzy rule and work out the optimal solution for detecting network intrusion and they managed the detection rate of the algorithm in the experiment to be over 97.5per cent.

Mainly academic studies are concentrated on the detection of external cyber intrusion and anomalies with the utilization of diverse AI methodologies and techniques. that said, industry should not neglect the important potential benefits of AI preventing internal threats. Companies are not only creating infinite amount of data externally through customers and suppliers but also internally through their own systems and platforms, which leaves insider breakers opportunities to conduct breaches. Besides, according to PwC Global State of Information Security Survey (2018), current employees remain the top source of security incidents and they are responsible for 27 percent of all cybersecurity issues. Detecting internal information breach is never an easy task as employees, no matter a disgruntled or careless staff or a staff on the leave, have access to the endpoint and cloud services within company and that will be convenient for them to copy or bring confidential data out of the company.

User and entity behaviour analytics (UEBA) can be used in combination with machine learning techniques. These can be deployed to catch up the subtle insider threats. UEBA is defined by Gartner Inc as using analytics to build the standard profiles and behaviours of users and entities across time and peer group horizons. Activities that are anomalous to the standard baselines are reported as suspicious and packaged analytics applied on these anomalies help discover threats and potential incidents. The 2017 Cost of Cyber Crime Study (Ponemon and Accenture, 2018) reported that these two technologies ranked lowest for enterprise deployment, 32 and 28 percent respectively but they prove to be the third and fourth highest cost saving innovations for cybersecurity protection.

There are not many academics researches that have investigated the application of UEBA in detecting insider threats. The focus has been more about the industry implementation and researching. A UEBA approach together with machine learning doesn't require human to create inputs and data for the purpose of identifying a certain pattern; it

learns from its own statistical models which are generated from employee daily activities to deduce and reason potential anomalies. It saves large amount of time for creating files and rules and help provide more accurate and efficient results than conventional detection solutions.

4.1 | Augmented Intelligence

A different but interrelated research direction is Augmented Intelligence. This requires more interaction between human and machine, allowing computer to supplement and support human thinking, analysing and reasoning. Khisamova ets al (2019) were the first to actively use scenario analysis to model risk-related cyber attacks. Instead of building a machine to reproduce human cognition and function automatically such as robo-advisor and AlphaGo, it is more efficient to construct a hybrid system in combination of human intelligence when it comes to behaviour change or intuitive intentions.

Augmented Intelligence is also referred to as Human Computer Interaction (HCI). In essence, it is more similar to the concept of Artificial General Intelligence which towards to the path that those AI pioneers would like to enter. Human computer users are viewed as the "weakest link in the security chain". In that respect, Treat Avoidance Theory is relevant. This claims avoidance of a malicious threat is not similar to the acceptance of a safeguarding measure.

5 | AN INFRASTRUCTURE OF CYBER RISK AND ITS IMPACT USING FAULT TREE AND EVENT TREE MODELS

This section considers Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) as methods to build a robust infrastructure for cyber risk evaluation. It reviews its impact based on previous studies and considers how to apply AI techniques that can significantly increase the chance of detecting anomalies, and lower the cost of consequences of being attacked.

In order to have a clear view of cybersecurity system and risk impact, it is vital to predetermine the classification of various cyber crimes and the systemic detection and influence mechanism. A few researches have concentrated on the taxonomy of cyber risks and the impact on both financial sectors and other industries, trying to build theoretical or empirical models to examine cybersecurity architecture, measurement and the cost. Some of them enlightened the construction of FT and ET models, which are detailed below.

Elnagdy et al (2016) addressed a Semantic Cyber Incident Classification (SCIC) model which used ontology-based knowledge representation deriving from semantic techniques to present risk classification and operate cybersecurity insurance. The model includes three phases.

Phase I consists of three vital activities which are defining cyber incidents, identifying features and constraints of each incident and understanding regulations and technique rules.

Phase II is mainly about defining ontologies which use the inputs generated from phase I.

Phase III is knowledge representation of the outcomes that link all ontologies. This is based on semantic web techniques.

The developed model could be evaluated in a practical operating environment. Ten et al (2010) proposed a supervisory control and data acquisition (SCADA) framework for the cybersecurity of an electric power infrastructure. As is shown in Appendix C, it includes four major components – real-time monitoring, anomaly detection, impact analysis and mitigation strategies. Besides, attack-tree methodology is what they used to analyse impact of a computer network system by identifying adversary objectives and a cybersecurity vulnerability index is what they used to measure the likelihood that an attack tree or attack leaf will be compromised by hackers.

The procedure works by identifying attack conditions to evaluating vulnerability indices and making relevant decisions. Lagazio et al (2014) put forward a multi-level model based on system dynamics (SD) methodology to capture the impact of cyber crimes on the financial sector. They found out that both tangible and intangible factors such as shifts of company strategic priorities, customer trust and loyalty, in together with market positioning and competitors are crucial to determine the cost of cyber crimes. For example as is illustrated in Appendix E, the reinforcing loop R1 indicates that as a major consequence of cyber attacks, the loss of customer trust and/or loyalty leads to lower growth for companies.

These studies all have their own methodologies and models built, either considering the framework and classification of cyber crimes or only the impact it may cost. However, there is a lack of integration to combine those two parts together to provide a broader perspective of mitigating the risk and reduce adverse consequences. Therefore, based on previous work, an integrated cyber risk infrastructure and the consequence it would cause can be constructed with a systemic quantitative risk analysis approach which is specifically FTA and ETA.

5.1 | Risk modeling

Risk modelling is one of the best ways to indicate threat priorities. FTA and ETA are two distinct methods for quantitative risk analysis that determine the Boolean logic relationship of events leading to an incident and estimate the risk associated with the incident (Ferdous et al, 2011). FTA refers to the basic causes of an unwanted event and predictions of the probability of occurrence.

Fault tree models follow a deductive logic that a top undesirable event is defined and various tree branches are constructed to model the failure. By moving downward, the first level of the tree branches represent general conditions that lead to the top event, independently or interactively. There are two main symbols standing for the relationship between each condition – "AND" and "OR" gate, which means each condition have a joint correlation leading to the top event or they could cause failure by their own. ETA is used to describe the consequences of the unwanted event and estimate the likelihood of possible outcomes regarding to the event.

In an event tree, the unwanted incident is called the initiating event and there are also tree branches that lead to the consequences using inductive logic. As is exactly the opposite logic from FTA, by moving forward, possible outcomes are determined from a series of safety barrier events and finally the frequency of consequences will be calculated for risk assessment purpose. Within each safety barrier event, there are two conditions, "success" and "failure" and their possibilities sum to 1. If there is only one possibility then the condition will be shown as "Null", which means the probability is one.

There are certain limitations to the fault tree and event tree modelling approaches. Both FTA and ETA require probabilities of the occurrence of events as inputs to conduct quantitative risk analysis, however, a process might combine hundreds of components and influences, which adds much more difficulty to the acquisition of each probability. Under this circumstance, expert knowledge and judgement can be used as alternative method for data collection and this will need to be evaluated and assessed.

In addition, the interdependency between each event and condition is often unknown and assumed to be independent in FTA and ETA for the purpose of simplicity. The limitations could cause inaccuracy and variations for risk modelling of complex system in the practical environment, thus a few improved approaches emerged to address these deficiencies such as fuzzy set methodology (Suresh et al, 1996), binary decision diagram (Andrews and Dunnett, 2000). Nevertheless, in this project, simplified fault tree and event tree models are created to describe complex cyber attack system.

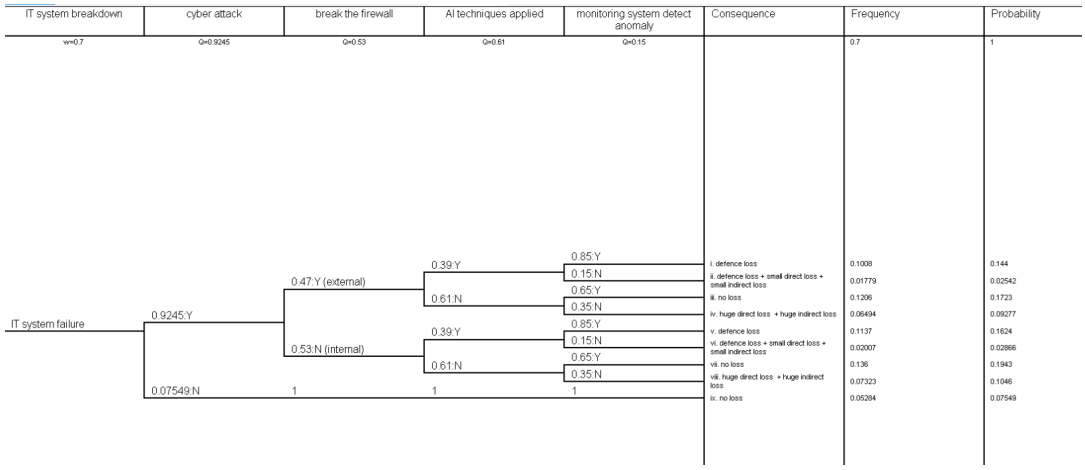

FIGURE 2 Fault tree model of occurrence of cyber incident

5.2 | Fault tree model

In a fault tree, the top unwanted event is a "cyber incident". In this respect, there are two channels of getting attacked, externally and internally. Thus, either "external attacks" or "internal attacks" contribute to a cyber incident being recorded. This is listed as a first level of cause, connected by an "OR" gate. Under "external attacks" branch, according to the taxonomy of financial cyber crime developed by Lagazio et al (2014), "web-based attacks", "phishing emails", "ransomware", "Denial of Service (DoS)" and "vulnerability exploit" are the major issues. Under "internal attacks" branch, mainly "employee behaviour" and "third parties" are related to the endpoint and cloud data breach within a company. All the second level events are considered to be connected with "OR" gates as these events can happen independently on their own.

In order to acquire the relevant probabilities of each event occurrence, reliable reports and researches published by acknowledged organizations need to be used for reference. Lagazio et al (2014) collected data for the period spanning 2017 and are updated unless specifically notified. These are detailed below:

- Phishing emails: 1 in 2995, so the fixed rate is 0.00033389 (Symantec,2018)
- Ransomware: 27per cent, so the frequency is 0.27 (Ponemon and Accenture, 2018)
- Denial of Service (DoS): 53per cent, so the frequency is 0.53 (Ponemon and Accenture, 2018)
- Web-based attacks: 1 in 13, so the fixed rate is 0.0769231 (Symantec,2018)
- Vulnerability exploit: 56 percent, so the frequency is 0.56 (Symantec,2018)
- Employee behaviour: 27 percent, so the frequency is 0.27 (PwC, 2018)
- Third parties: 26 percent, this was derived from 53per cent-27per cent, as 53per cent of companies experienced insider attacks in the past year, so the frequency is 0.26 (CA technology, 2018)

5.3 | Event tree model

An event tree model aims to define all the consequences of a cyber attack, both economically and socially. As suggested by Anderson et al (2012), the cost of cyber attack can be split into three categories, direct loss which refers to the monetary loss, indirect loss which represents intangible cost such as damaged reputation and decreasing customer trust/loyalty, defence loss which means the implementation of cybersecurity measures and training of employees. Therefore, the model is initiated by "IT system breakdown" and contains four safety barriers, which are "cyber attack", "break the firewall", "AI techniques applied", " monitoring system detect anomaly".

The difference between Event Tree and applying AI techniques lies in the monitoring systems. With the latter, these have a higher probability of detecting anomalous activities, resulting in less direct and indirect loss, however the defence loss would be higher when AI techniques are utilized. Besides, whether breaking the firewall differentiates external intrusion and internal breach because employees can access confidential information within the IT system.

Last but not least, there is an assumption that when monitoring system detects an anomaly, either there will be appropriate patches available to be installed in time or relevant IT staff will be alerted to take action immediately, thus there will not be any further loss caused to the company. With the same data collection method as fault tree model, the probabilities of each event are summarized below.

- IT system breakdown: 70per cent, with a frequency 0.7 (KPMG New Zealand, 2017)
- Cyber attack accident: yes 0.9245, no 0.07549 This is derived from the top event TP1 of fault tree model
- Break the firewall: yes 47per cent, no 53per cent. Successfully breaking the firewall is recognized as external attack, thus possibility of success is 100per cent-53per cent (CA technology, 2018)
- AI techniques applied: yes 39per cent, no 61per cent (ESG, September 2017)
- Monitoring system detect anomaly: when AI techniques applied, yes 85per cent no 15per cent; when no AI techniques applied, yes 65per cent no 35per cent (MIT, 2016)

The potential consequences resulting from the series of initiating event and safety barrier events can be seen in the column "Consequence" and are briefly explained below in figure 3.

FIGURE 3 Event tree model initiated by an IT system breakdown:

1. defence loss: Utilizing AI techniques causes defence loss but monitoring system detect the cyber attack so there is no other direct and indirect loss.
2. defence loss + small direct loss + small indirect loss: Even if monitoring system doesn't detect anomalous attack, AI techniques would help relevant IT department staff discover abnormal activities faster and more efficient than the circumstance where no such technology is applied, thus small direct and indirect loss will be imposed.
3. no loss: Even if AI techniques are not applied, monitoring system is able to detect anomaly so it is assumed to be fixed in time.
4. huge direct loss + huge indirect loss: No AI techniques and not detecting attacks put company at stake, resulting huge direct and indirect suffering.
5. defence loss: Same with consequence i but insider attack instead of outside threat.
6. defence loss + small direct loss + small indirect loss: Same with consequence ii, insider attack instead.
7. no loss: Same with consequence iii, insider attack instead.
8. huge direct loss +huge indirect loss: Same with consequence iv, insider attack instead.

9. no loss: IT system breakdown not because of cyber attack accident so it is assumed to be fixed in time, thus there is no loss suffered.

From fault tree model results, it can be show that top event, *cyber incident*, has a 92.45per cent probability of occurring, which is relatively high within a company. This indicates the conclusion that cybersecurity challenge should be on the priority of an organization's agenda and measures should be taken to mitigate cyber risks.

Event tree model results shown in figure 4 there is a lower frequency and probability of the occurrence of initiating event and causing corresponding losses when applying AI techniques, 0.1008, 0.1206 respectively for frequency and 0.144, 0.1723 respectively for probability. Comparing with consequence i. and ii., both under the circumstance of applying AI techniques, there is a higher frequency and probability of monitoring system detecting anomalies thus causing fewer losses, 0.1008, 0.01779 respectively for frequency and 0.144, 0.02542 respectively for probability.

The same approach can be used to analyse the consequence of internal cyber attacks, more specifically, to compare consequence v. and vii.; vi. and viii.; v. and vi.; vii. and viii. The results all indicate that applying AI techniques will improve of the chance of monitoring system detecting anomalous activities and have lower probability of IT system breakdown occurrence as well as causing fewer losses.

FIGURE 4. The frequency and probability of all consequences (Consequence, Frequency and Probability)

1. defence loss 0.1008 0.144
2. defence loss + small direct loss + small indirect loss 0.01779 0.02542
3. no loss 0.1206 0.1723
4. huge direct loss + huge indirect loss 0.06494 0.09277
5. defence loss 0.1137 0.1624
6. defence loss + small direct loss + small indirect loss 0.02007 0.02666
7. no loss 0.136 0.1943
8. huge direct loss +huge indirect loss 0.07323 0.1046
9. no loss 0.05284 0.07549

FT and ET models can potentially be implemented to elaborate the mechanism of occurrence and consequences of cyber risk as well as the quantitative analysis of the loss due to cyber incident. They could help companies better define the vulnerabilities of their cybersecurity infrastructure and measure the risk exposure and cost, allowing them to make appropriate strategic decisions to improve and protect their cyber space. However, the models need to be evaluated in practical environment and apply real or estimated data to examine the accuracy and effectiveness. For example, how efficiency is it to apply AI techniques to detect anomalies (what is the probability of correct detection) and how to measure the intangible loss, which are apparently dependent to company characteristics.

In addition, although there is less probability of causing losses when applying AI techniques, the implementation of such complicated technology would generate installing fees, maintenance fees and the opportunity cost of staff training and recruiting. As a result, the aggregated result of cost benefit is unknown and related to company specific status. Lastly, as it is a simplified model with its specific assumptions, the real model will be more complex and have more safety barrier events followed by the initiating event.

6 | REGULATORY ISSUES

When operating in the real world, it is important for a company to comply with the broader regulatory requirements regarding cybersecurity and data protection. Within the scope of law and regulation, the most significantly influential rule up to date is the EU General Data Protection Regulation (GDPR) which was set into place in April 2016 and came into force in May 2018. It repeals the former Directive 95/46/EC and brings a single standard regulation to all EU member states, allowing people to have more control over their personal data and businesses to benefit from a transparent and equal playing field.

The GDPR landscape applies to all citizens and companies processing data in the EU, regardless of the locations of entities, which means it is also applicable if controllers and processors established outside EU process data to EU member states, for example providing services and offering commodities to EU citizens. In addition, it applies when monitoring behaviour takes place in the EU.

Within the world of data, there are available sanctions for cyber misbehaviour. This is why the regulations such as GDPR focus on whether defences are in line with peers and whether the measure of defence are appropriate. GDPR regulates that "as soon as the controller becomes aware of the personal data breach, the controller should notify supervisory authority without undue delay and, where feasible, no later than 72 hours after having become aware of it, unless the controller is able to demonstrate that the data breach is unlikely to result in a risk to the rights and freedoms of natural persons" (European Union, 2016).

"A data subject should have the right to erase and rectify his or her personal data where they are no longer necessary in relation to the purpose for which they are collected or otherwise processed. It should also be extended in such a way that controllers who have made the personal data public should be obliged to inform the third parties which are processing data to erase any link, copy or replication of those personal data" (European Union, 2016).

7 | CONCLUSION

We have provided a comprehensive review of the current cybersecurity threats landscape, especially from the perspective of the financial sector. We highlighted industrial and academic reports and research into the field. We reveal that cyber attack challenges are becoming increasingly severe and complicated and more advanced technical tools are being used by cyber criminals to conduct massive cyber crimes. This situation urges organizations and companies to put cybersecurity protection on the priority. Therefore, an integrated infrastructure of the causes of cyber incidents and the consequences resulting from the IT system breakdown is described.

We illustrated fault tree and event tree models. These show it is possible analyse the risk exposure and have a clear view of the cost and benefit. The results show that applying AI techniques could potentially increase the probability of detecting anomalous activities and causing fewer losses including direct and indirect losses.

Implementing such AI system will require training and maintenance of systems. The net result of risk analysis is therefore related to company size and maturity. We suggest future work should be focused on seeking more information and the investigation of specific business instances to examine the models we suggest in a practical environment. We further illustrated how an organization can use machine learning and UEBA techniques to detect malicious internal behaviours and protect important business information. In terms of creating future intelligent machines and harnessing this technology, there are voices calling for robust AI to avoid any adverse outcomes related to economic, ethical and social issues.

REFERENCES

Akamai Technologies Inc, (2017) "Q2 2017 State of the Internet.

Amoroso, E. 2006. Cyber Security. New Jersey: Silicon Press.

Anderson, R., Barton, C., Bohme, R., Clayton, R., et al, (2012) "Measuring the Cost of Cyber Crime", In: Workshop on the Economics of Information Security, Berlin, Germany.

Andrews, J.D., Dunnett, S.J., (2000) "Event-tree analysis using binary decision diagrams", IEEE Transactions on Reliability, Volume 49, Issue 2, pp. 230-238.

Barr, A. and Feigenbaum, E.A., (1981) "The Handbook of Artificial Intelligence", Kaufmann, William Inc, 1st Edition.

Bitter, C., Elizondo, D.A., Watson, T., (2010) "Application of Artificial Neural Networks and Related Techniques to Intrusion Detection", IEEE World Congress on Computational Intelligence (WCCI 2010), pp. 949-954.

Broby, D., Basu, D. and Arulselvan, A., 2019. The role of precision timing in stock market price discovery when trading through distributed ledgers. Journal of Business Thought, 10(1).

Choudhary, S.P., Vidyarthi, D., (2015) "A Simple Method for Detection of Metamorphic Malware using Dynamic Analysis and Text Mining", Procedia Computer Science, Volume 54, pp. 265-270.

Elnagdy, S., Qiu, M., Gai, K., (2016) "Cyber Incident Classifications Using Ontology-based Knowledge Representation for Cybersecurity Insurance in Financial Industry", 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing, pp.301-306.

European Union, (2016) "General Data Protection Regulation".

Ferdous, R., Khan, F., Sadiq, R., Amyotte, P., Veitch, B., (2011) "Fault and Event Tree Analyses for Process Systems Risk Analysis: Uncertainty Handling Formulations", Risk Analysis, Vol.31, No.1, pp.86-107.

Huang, X. and Dong, J., 2019. On modeling and secure control of cyber-physical systems with attacks/faults changing system dynamics: An average dwell-time approach. International Journal of Robust and Nonlinear Control, 29(16), pp.5481-5498.

IBM, (2011) "Deep Blue".

Jones, S., (2017) "Timeline: How the WannaCry cyber attack spread", Financial Times.

Jongsuebsuk, P., Wattanapongsakorn, N., Charnsripinyo, C., (2013) "Real-time intrusion detection with fuzzy genetic algorithm," 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), pp.1-6.

Juniper Research, (2017) "The Future of Cybercrime and Security: Enterprise Threats and Mitigation", Proofpoint 2017 Quarterly Threat Report Q3 2017.

Khisamova, Z.I., Begishev, I.R. and Sidorenko, E.L., 2019. Artificial Intelligence and Problems of Ensuring Cyber Security. International Journal of Cyber Criminology, 13(2), pp.564-577.

Kizza, J.M., 2014. Computer network security and cyber ethics. McFarland.

Lagazio, M., Sherif, N., Cushman, M., (2014) "A multi-level approach to understanding the impact of cyber crime on the financial sector", Computers and Security, pp.58-74.

Livadas, C., Walsh, R., Lapsley, D., Strayer, W.T., (2006) "Using Machine Learning Techniques to Identify Botnet Traffic", Proceedings. 2006 31st IEEE Conference on Local Computer Networks, pp. 967-974.

McCarthy, J., Minsky, M., Rochester, N., and Shannon, C. E., (1955) "A proposal for the Dartmouth summer research project on artificial intelligence".

Oltsik, J. and Poller, J., (2017) "Automation and Analytics versus the Chaos of Cybersecurity Operations", ESG and McAfee.

Ponemon Institute LLC and Accenture, (2018) "2017 Cost of Cyber Crime Study"

PwC, (2018) “Global State of Information Security® Survey”
Solms, R., Niekerk, J., (2013) “From information security to cyber security”, Computers and Security, volume 38, pp. 97-102.
Soska, K., Christin N., (2014) “Automatically Detecting Vulnerable Websites Before They Turn Malicious”, included in the Proceedings of the 23rd USENIX Security Symposium, San Diego, CA.
Suresh, P.V., Babar, A.K., Raj, V.V., (1996) “Uncertainty in fault tree analysis: A fuzzy approach”, Fuzzy Sets and Systems, volume 83, Issue 2, pp. 135-141.
Swankie, G.D.B. and Broby, D., 2019. Examining the Impact of Artificial Intelligence on the Evaluation of Banking Risk.
Symantec Corporation, (2018) “2018 Internet Security Threat Report”, volume 23.
Ten, C.-W., Manimaran, G., Liu, C.-C., (2010) “Cybersecurity for Critical Infrastructures: Attack and Defense Modeling”, IEEE Transactions on Systems, Man and Cybernetics – Part A: Systems and Humans, vol 40, No.4, pp.853-865.
Thakur, K., Qiu, M.K., Gai, K.K., Ali, M.L., (2015) “An Investigation on Cyber Security Threats and Security Models”, 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, pp.307-311.
World Bank, (2018) “Cybersecurity, Cyber Risk and Financial Sector Regulation and Supervision”