**International Journal of Research in Economics and Social Sciences(IJRESS)**
Available online at: http://euroasiapub.org
Vol. 13 Issue 8, August- 2023
ISSN(o): 2249-7382 | Impact Factor: 8.018
**(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)**

# EFFECTIVENESS OF CYBER SECURITY IN PENSION PAYMENTS TO AVOID THE FRAUDS AND EMBEZZLEMENTS IN USA

**Dr Robin Malik**

**robinmalik511@gmail.com**

## Abstract

*Although the ramifications of this may be comparable to those of cyber data theft, the focus of this work is on intentional acts rather than the unintentional loss of data, such as via the loss of data files1; despite the fact that the implications of the former may be similar to those of the latter, this document does not address other accidental violations of data protection regulations. the most significant dangers posed by cyber attacks to pension plans; who is accountable for mitigating these dangers; even while pension plans often delegate day-to-day operations to third parties, the trustees or the employer are ultimately responsible for the plan's security. It is more necessary than ever before to have a solid understanding of the extent of cybersecurity risk that your organisation is exposed to as well as the possible consequences of an event. In spite of the significance, many organisations have a poor knowledge of the amount of risk that they currently face and are under the impression that acquiring any of this information is a procedure that is both time-consuming and expensive. The answer can be found in pondering. The approach that we use to assess risk gives you a fast and simple method for determining the levels of risk you now face as well as the likelihood of an event occurring.*

***Keywords:*** *Cyber Security, Pension, Fraud*

**International Journal of Research in Economics and Social Sciences(IJRESS)**
Available online at: http://euroasiapub.org
Vol. 13 Issue 8, August- 2023
ISSN(o): 2249-7382 | Impact Factor: 8.018
**(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)**

## INTRODUCTION

Because pension plans store significant quantities of personal data and assets, fraudsters and criminals may target them as a potential source of income for themselves. As trustees and managers of the scheme, it is your responsibility to take the necessary precautions to protect your members and assets, and this includes protecting them from the so-called "cyber risk." This is a matter that every trustee and scheme management, regardless of the size or structure of their scheme, should be aware of and vigilant about.

Cyber risk may be loosely described as the risk of loss, interruption, or harm to a scheme or its members as a result of the failure of the scheme's information technology systems and procedures. This definition is wide enough to encompass a variety of potential outcomes. It encompasses threats to both information (data security) and assets, as well as both internal threats (such as those posed by workers) and external threats (such as those posed by hackers).

You need to take measures to enhance your cyber resilience, which is your capacity to not only identify and decrease the danger of a cyber event occurring, but also to recover once one has occurred. You should design your strategy for controlling this risk in collaboration with all relevant stakeholders, including employers, in-house departments, and third-party service providers. This book outlines best practises for pension plans, all of which may be implemented into your scheme in a manner that is suitable to its profile. At the very end of this tutorial, you will find a glossary that defines a variety of essential terminology.

### What are the key risks faced by pension scheme?

It is crucial to understand what assets might be at danger from cyber thieves in order to correctly identify the most significant threats. Pension plans not only contain billions of pounds worth of assets, with millions of pounds travelling around constantly from member bank accounts to scheme bank accounts, employers, and fund managers, but they also have an abundance of member data, which are equally desirable assets for a criminal. There is an additional risk of reputational harm for pension plan sponsors if their pension scheme is affected by a cyber-attack, which might also result in an increase in scheme deficits. This risk is compounded when the scheme in question is a pension scheme.

### Ransomware attacks

In these attacks, the target's data is encrypted, and the perpetrators demand a ransom in order to decrypt it. They might accomplish this by luring members of staff working for third party administrators (TPA) to download malware as part of an email. Nevertheless, the WannaCry

**International Journal of Research in Economics and Social Sciences(IJRESS)**
Available online at: http://euroasiapub.org
Vol. 13 Issue 8, August- 2023
ISSN(o): 2249-7382 | Impact Factor: 8.018
**(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)**

ransomware assault that occurred in 2017 used vulnerabilities in Microsoft Windows operating systems that were either outdated or not updated for security updates. This allowed the ransomware to infect machines automatically and without the input of users. There is anecdotal information to suggest that a ransomware assault has already been successful against at least one TPA. For many, it is feasible that data can be recreated from backups, but even if this were possible, it would cause some interruption in the functioning of the scheme and result in additional expenses since transactions would have to be reprocessed starting from the date of the backup.

If the attack was successful because to shortcomings on the side of the scheme or the service providers, such as neglecting to deploy software updates or using unsupported software2, there is also the possibility of incurring sanctions in accordance with data protection regulations. Due to the unfortunate fact that ransomware attacks are increasingly targeting backups as well, it may be necessary for the scheme and/or their service providers to pay a ransom in order to decrypt the data. Outside of the realm of pensions, there have been situations in which the ransom was paid, but the encryption key was unable to open the encrypted data, and the data was destroyed permanently. This is the worst case scenario. This would have disastrous effects on the administration of the scheme, including the inability to pay scheme pensions, the inability of members to receive their benefits or modify their investment choices, and/or the creation of delays with the transfer of money, including the investment of member and/or employer contributions.

**Data theft**

Theft of plan data is a risk that pension schemes face. It is possible that staff members would unwittingly download malware in this manner, possibly through e-mail attachments. This might follow a similar starting path as ransomware. The level of sophistication of data theft attempts varies. Teenagers have been known to steal data from huge companies by utilising generic hacking tools that they got on the dark web in certain cases. This is one end of the spectrum. On the other end of the spectrum, Advanced Persistent Threat (APT) attacks may involve professional hackers patiently probing systems over the course of a year or more, capitalising on any success to gain access to multiple systems, stealing data repeatedly, and then covering tracks in such a way that companies may be unaware that data has been stolen. Throughout the years, there have been countless instances of big data thefts, some of the most notable of which being Yahoo! and Equifax3. In addition to the breach of privacy, the stolen information might be used to scam members and other recipients in a variety of ways, such as by submitting bogus loan applications. Data pertaining to pension schemes may be highly valuable to con artists,

**International Journal of Research in Economics and Social Sciences(IJRESS)**
Available online at: http://euroasiapub.org
Vol. 13 Issue 8, August- 2023
ISSN(o): 2249-7382 | Impact Factor: 8.018
**(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)**

who may use stolen data to identify members who can then be targeted for pension scams or other types of identity theft. There is circumstantial evidence suggesting that information about pension plans in the UK is being traded on the dark web. Theft of data may result in the need for remediation costs to address breaches; the requirement to implement credit monitoring for affected members to prevent stolen data from being used to defraud those members; compensation for fraud and/or for distress caused by the theft; and regulatory fines for any deficiencies on controls that might have prevented theft. It is important to keep in mind that the data obtained might contain information of current as well as former members; for example, a breach at the health insurer Anthem in the United States resulted in the theft of approximately 80 million records, of which half linked to prior clients. When evaluating the possibility for exposure, schemes should take into account both legacy and current data, and they should only keep records for the minimum amount of time required. After the UK leaves the EU, violations of data protection will be subject to the UK General Data Protection Regulation (UKGDPR), which is very similar to the GDPR4 enacted by the EU. This regulation gives the Information Commissioners Office (ICO) the authority to levy fines of up to 4% of turnover or €20 million, whichever is greater. In spite of the fact that it may be counterintuitive to impose a punishment on a scheme, which would result in less assets being made available to pay for member benefits, it is important to point out that although the ICO has not penalised a scheme in recent years, it has fined a number of charities5, and trustees should not make the assumption that they will not be punished.

## Cyber theft and fraud

Theft of assets, in addition to data, is included in the realm of cybercrime risk. They might accomplish this goal in a variety of ways. For instance, cybercriminals might break into the systems that manage pension plans in order to reroute beneficiary payments. Alternately, they could engage in fraudulent activities involving the transfer of cash. One particularly egregious illustration of this was the cyberattack that led to the Bangladesh Central Bank SWIFT payment system being infiltrated, which in turn led to the fraudulent transfer of more than US$100 million. In the case of pension plans, there is already anecdotal evidence that within days of the statutory need for publicly posting the scheme's Statement of Investment Principles, this information and trustee signatures are being used to aid fraudulent disinvestment efforts. This is the case despite the fact that the publication of the Statement of Investment Principles is a necessary obligation.

**International Journal of Research in Economics and Social Sciences(IJRESS)**
Available online at: http://euroasiapub.org
Vol. 13 Issue 8, August- 2023
ISSN(o): 2249-7382 | Impact Factor: 8.018
**(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)**

### E-mail spoofing

This is a form of cyber fraud in which cyber thieves pose as legitimate senders of e-mails in order to defraud schemes and the people who are invested in them. For instance, a cybercriminal may send an email to a sponsor, purporting to be from the trustees, asking the sponsor to pay a false invoice or to modify the bank information of a third-party supplier. Alternately, a con artist might pose as a member who is ready to retire and ask for the money to be sent to their account by e-mail while impersonating the real member.

### Distributed denial of service (DDOS)

In a distributed denial of service (DDOS) assault, cybercriminals take control of many computers and flood host servers with unnecessary traffic in an effort to overwhelm systems and prevent internet access. The Internet of Things is being exploited more and more, and smart refrigerators and other apps are being used to support distributed denial-of-service assaults (DDOS). This increases the volume of traffic that thieves are able to control. Even though a pension scheme is not the target of the attack, if it shares a host with the intended victim, the internet services that the pension system provides might be compromised. Despite the fact that this may not normally have any substantial monetary impact on a pension plan, it may cause member unhappiness if self-service online options are unavailable for an extended length of time. In addition to this, it may leave members concerned about the safety of the benefits they get. This list does not contain every possible option. Cyber-jacking, which is when computers are hijacked in order to mine Bitcoin; cyber-vandalism, which is when websites are vandalised; and cyber-attacks on infrastructure are some of the other types of dangers.

### A. Cybersecurity Threats and Health Plans

Due to the growing frequency of cyberattacks and the significant costs associated with them, cybersecurity continues to be a top priority problem for governments and the commercial sector in the United States and throughout the rest of the globe. IBM estimates that the average cost of a data breach in the United States will be $9.44 million in 2022, representing an increase of 4.3 percent from 2021's figure.4 Ransomware assaults, in which thieves encrypt the data stored on a system and hold it hostage until the owner of the system pays a significant ransom, which is typically paid in cryptocurrency, have become an increasingly significant threat. According to the Financial Crimes Enforcement Network of the United States Department of the Treasury, suspicious activity reports submitted by financial institutions revealed that there were 1,489 ransomware-related incidents in 2021, resulting in nearly $1.2 billion in payments to cybercriminals. This figure is a significant increase from the $416 million that was reported in

**International Journal of Research in Economics and Social Sciences(IJRESS)**
Available online at: http://euroasiapub.org
Vol. 13 Issue 8, August- 2023
ISSN(o): 2249-7382 | Impact Factor: 8.018
**(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)**

2020.5 One of the most common and prominent targets of cyberattacks is the health care industry, which in the United States is recognised as one of the nation's sixteen essential infrastructure sectors. According to a study by the Office of Civil Rights (OCR) of the United States Department of Health and Human Services (HHS), the biggest number of persons have been impacted by cybersecurity breaches that have occurred among health care providers since 2015.6 The Federal Bureau of Investigation reports that in 2021, the Healthcare and Public Health Sector was the critical infrastructure sector in the United States that saw the highest number of ransomware attacks.7 As a continuation of this, in October 2022, CommonSpirit Health, which is the second-largest non-profit health system in the United States, was the victim of a ransomware assault. This attack caused the system to be disrupted for several weeks after it occurred and resulted in the inability to access some medical records.8 There is no exception for health plans and insurers from these assaults, and they have been victims of some of the most significant data breaches in the United States. 78.8 million customers were impacted when Anthem Inc. was the target of a cyberattack in 2015.9 In an incident that took place in 2014 against the health insurance provider Premera Blue Cross, cybercriminals reportedly "gained access to claims data, including clinical information, along with banking account numbers, Social Security numbers, birth dates, and other data" for 11 million individuals.10 More recently, in March 2022, Partnership HealthPlan of California revealed a hack that may have resulted in the loss of data belonging to 854,913 current and previous health plan members. The data that may have been stolen includes information on diagnosis, treatments, and prescriptions.11 Data breaches in the healthcare industry are also the most expensive. According to IBM's yearly study at worldwide data breach prices, the health care business has been the one with the highest expenditures for the past 12 years in a row. The average cost of a data breach in the health care industry was estimated to be $10.1 million in 2022, which was a 9.4% increase from 2021.12 The significance of health data to patients, providers, and plans, as well as to criminals, makes the health care industry a potential target for attacks. This is one reason why the health care industry is a prime target for assaults. Because cyberattacks on health data might impede the delivery of care, hackers are provided with increased influence over data owners as a result of these attacks. For instance, the Department of Labour was approached by a participant in a health plan who had been denied clearance for surgery and for whose payments for earlier treatment had not been provided. This was due to the fact that the necessary plan data to verify the individual's coverage had been encrypted as a result of a ransomware attack. Additionally, a ransomware assault that occurred in May 2022 on Costa Rica's national health service resulted in the cancellation of scheduled treatments and prevented the fulfilment of prescriptions for approximately 13 individuals.

**International Journal of Research in Economics and Social Sciences(IJRESS)**
Available online at: http://euroasiapub.org
Vol. 13 Issue 8, August- 2023
ISSN(o): 2249-7382 | Impact Factor: 8.018
**(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)**

Because of the crucial and even possibly life-or-death nature of this information, cybercriminals have the opportunity to demand far greater ransom payments than they would have otherwise. In the instance involving Costa Rica, the perpetrators requested a payment of 5 million Costa Rican colones (or the equivalent in Bitcoin) in order to decode the data. Theft of personally identifiable health information (PHI) is another source of high value for thieves. A recent publication made the following observation:

[PHI] is one of the most highly sought after commodities on the dark web and is worth an absolute fortune to hackers. According to Experian, hacked Instagram accounts sell for $7, while stolen medical information go for $1,000 apiece. In comparison, the value of a Social Security number is only one dollar. Credit card numbers may be purchased for around $5 each. In addition, lawbreakers with experience in drug smuggling and money laundering gladly buy medical records in order to get prescription prescriptions, make fake medical claims, or steal the information in order to create credit cards and take out illegal loans. In contrast to bank accounts and credit cards, which may be closed at any time, medical records are a rich reservoir of useful data points that are kept permanently.14

The use of stolen data for these reasons can, in turn, result in financial expenses being passed on to participants of health plans, much in the same way that identity theft can hurt individuals. Theft of personally identifiable information (PHI), maybe more than with other types of data, can result in larger effects that are not immediately quantifiable in dollars and cents but can be just as devastating to an individual, if not more so. According to a study published by the Institute of Medicine (IOM) in 2009, protected health information (PHI) can be "sensitive and potentially embarrassing." In addition, the following was noted in the IOM report:

In the event that there is a breach in security, those persons who have had unauthorised access to their health information face a variety of possible risks. It is possible that the publication of personal information will result in inherent harm merely due to the fact that the private information in question will become known to other people. The possibility of economic damage is still another risk. If the incorrect kind of information were to become widely known, it's possible that people might lose their jobs, their health insurance, or their homes. People might potentially suffer social or psychological suffering as a result of the situation. The disclosure that an individual is infected with HIV or another sort of sexually transmitted virus, for instance, might result in social isolation and/or other outcomes that are detrimental to the individual's mental health.

The one-of-a-kind character of personally identifiable health information is recognised by the regulations that govern the imposition of monetary fines for violations of the privacy and

**International Journal of Research in Economics and Social Sciences(IJRESS)**
Available online at: http://euroasiapub.org
Vol. 13 Issue 8, August- 2023
ISSN(o): 2249-7382 | Impact Factor: 8.018
**(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)**

security requirements outlined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as well as the other relevant aspects of the law. In particular, the rules require the Secretary of Health and Human Services to take into account, when determining the severity of a penalty, the nature and extent of the harm that was caused by the violation. They also stipulate that this may take into account "[w]hether the violation resulted in harm to an individual's reputation."

**Cybersecurity Frameworks**

The ERISA Advisory Council conducted research into governmental and commercial cybersecurity frameworks in 2016. These frameworks are utilised by businesses to assess and handle potential cybersecurity threats.43 Even though the 2022 Council did not conduct an exhaustive review of all of the existing cybersecurity frameworks, these frameworks are an essential component of comprehending how health plans, insurers, and their business partners are handling cybersecurity dangers. The National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Health Information Trust Alliance (HITRUST) Common Security Framework, and the ISO/IEC 27001 standard are examples of frameworks that are used often. These frameworks, in general, provide flexible ways to analysing the risks associated with cybersecurity, as well as creating and implementing policies, practises, procedures, and other measures for safeguarding data and responding to cyber attacks. It is not normally required under HIPAA or other laws that regulate cybersecurity practises that organisations employ a cybersecurity framework. However, regulators and other parties may take an organization's usage of such a framework into consideration when determining whether or not the organisation is performing its duties to secure data. For instance, a 2021 amendment to the HITECH Act directs the Department of Health and Human Services (HHS) to consider whether a covered entity or business associate had so-called "recognised security practises" in place for not less than the previous 12 months when deciding whether to lessen HIPAA fines, terminate a HIPAA audit early and favourably, or mitigate other agreed upon remedies for resolving potential violations of the HIPAA security rule.44 The NIST cybersecurity framework, the approaches contained in Health Industry Cybersecurity Practises: Managing Threats and Protecting Patients, which was developed by HHS in collaboration with the public-private partnership of the Healthcare and Public Health (HPH) Sector of Critical Infrastructure, and any other cybersecurity programmes and practises developed, recognised, or promulgated through regulations under other sections of the law are all examples of what the law considers to be recognised security practises.

International Journal of Research in Economics and Social Sciences(IJRESS)
Available online at: http://euroasiapub.org
Vol. 13 Issue 8, August- 2023
ISSN(o): 2249-7382 | Impact Factor: 8.018
**(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)**

**Increasing the quality of contacts with pension members through the use of technology**

Fintech is being used across a wide variety of financial services in order to improve how customers engage with such services. By rendering financial goods more easily available, transparent, and understandable, fintech has the potential to contribute to an increase in consumers' level of trust in these products. It may be used to collect and analyse data more effectively, which can help with product creation and personalization. Through the use of gaming mechanics and educational content, it can inspire involvement in monetary decision-making. These innovations are anticipated to be especially useful in contacts with millennials, who anticipate using technology to obtain financial services and who are now entering the workforce. Millennials are now entering the workforce. The most obvious change brought about by Fintech may be seen in the realm of financial advising. Even though the major application of this technology is presently in wealth management, insurance firms are beginning to utilise it as well. Robo-advice is typically less expensive and easier to obtain than traditional "human" counsel. As a result, it may be particularly helpful for defined contribution (DC) plans, in which members must make a variety of decisions on their finances despite the fact that their funds may be very little. Fintech businesses have "lower cost structures, greater customer reach, or superior ability to monitor or score risk," as stated by the Chief Scientific Adviser for the United Kingdom's government. As a result, these companies are able to improve the provision of financial advice to populations that were previously under-served.

**Digital communications**

The use of digital technology in communications, such as periodic reporting, marketing communications, and other forms of information, can be of assistance to the development of member involvement when it comes to fintech. It is possible for digital communications to entail little more than the electronic storage and distribution of documents. On the other hand, digital communications may involve "smart" communications, which incorporate the use of other forms of media, gamification, personalization, or interaction in order to attract readers.

Regulators are beginning to acknowledge the shift away from paper documents and towards electronic communications. As a result, they are increasingly allowing financial service providers to utilise electronic communications as the default choice for regulatory disclosure. For instance, the Securities and Exchange Commission (SEC) enables mutual funds to post their prospectus online, while the Australian Securities and Investments Commission (ASIC) has a "publish and notify" approach. It is more simpler and less expensive to monitor who has received and read electronic communications than it is to monitor who has received and read printed communications. However, there are significant hazards associated with digital

**International Journal of Research in Economics and Social Sciences(IJRESS)**
Available online at: http://euroasiapub.org
Vol. 13 Issue 8, August- 2023
ISSN(o): 2249-7382 | Impact Factor: 8.018
**(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)**

disclosure in terms of disclosure standards. It is essential that the material be framed correctly in order to prevent readers from being diverted from the information that is most pertinent by extra features. If the format of the printed material differs from the format of the electronic information, providers run the risk of being held liable for any resulting confusion or miscommunication. It is therefore possible that regulators may need to issue best-practice standards for digital disclosure in order to assist with making certain that customers will read and comprehend the information that is most pertinent to them. In general, the use of digital technology is anticipated to improve both the quality and efficiency of the interactions that take place between pension providers and the members of their organisations. Utilising push notifications, for instance, to gently prod individuals into checking their accounts or increasing their donations is one way in which intelligent communications may take advantage of behavioural insights. During their investigation into personal current accounts, the UK Competition and Market Authority came to the conclusion that "annual interest statements have virtually no effect on consumer actions." However, when consumers are provided with immediately actionable information, such as text alerts and internet banking, they are able to reduce their overdraft fees by almost 25 percent. Fintech makes it possible for pension providers and their members to communicate on demand outside of the statutory reporting periods. In Australia, members of superannuation schemes may access their accounts through a mobile phone app. In the UK, Aviva's Shape My Future app gives online tools and calculators to help members picture their lifestyle in retirement. In Australia, members of superannuation schemes can access their accounts through a mobile phone app.

**Platforms and dashboards**

The use of digital technology may also promote better openness and make it possible for individuals to manage their own data in a more effective manner, which may ultimately result in an increase in their bargaining power and a reduction in the cost of private pensions, particularly personal pensions. E-aggregators make comparison websites easier to use or provide individuals the ability to compile and evaluate their own data. One day, people could be able to control all aspects of their financial lives from a single centralised location. A number of nations have developed what are known as "pensions dashboards" to provide members and beneficiaries with an understandable and user-friendly summary of the expected financial aspects of their pensions (see Box 1 for further information). These dashboards differ in the amount of data that they hold as well as the functionality that they provide; however, research suggests that they can be an effective tool for disseminating information, encouraging people to take action, and especially for keeping track of multiple pension pots as individuals move between several different employers. The construction of a dashboard, on the other hand, comes

**International Journal of Research in Economics and Social Sciences(IJRESS)**
Available online at: http://euroasiapub.org
Vol. 13 Issue 8, August- 2023
ISSN(o): 2249-7382 | Impact Factor: 8.018
**(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)**

with a significant number of technical obstacles and expenses, and policy considerations must take into account not just functionality but also finance and governance. Consideration has to be given, for instance, to the question of whether the dashboard ought to be sponsored by the private sector or if advertising ought to be permitted. Concerning the digital disclosure of information, it is essential to make certain that the platforms in question do not result in lower levels of participation or encourage members to bypass essential information. For instance, plans to launch an auto-consolidation of small DC pots on Australia's pensions dashboard were postponed because inactive accounts in some cases offered better protection than active accounts; users of pension dashboards should be given all of the relevant information as well as a simple "one click" option to take action. This is because inactive accounts in some cases offered better protection than active accounts.

## Conclusion

Pension plans are exposed to a serious risk posed by cyber risk, which has the potential to compromise the security of member information, bring the administration of the plan to a halt, and steal money from both the plan and the employer. Trustees are ultimately accountable for ensuring that proper cyber risks are in place, and they should aim to ensure, at a bare minimum, that both in-house and third-party operations comply to fundamental principles of cyber hygiene. Insurance may also help offset losses and give vital assistance, but care must be taken to pay attention to any exclusions and other potential restrictions of protection in the policy.

## REFERENCE

[1] Accenture (2015), The Rise of Robo-Advice.
[2] Acord & Surely (2016), AI—The Potential for Automated Advisory in the Insurance Industry (February).
[3] Biener, C., Eling, M., & Schmit, J. (2013), Regulation in microinsurance markets: principles, practice and directions for future development (Working papers on risk management and insurance No. 127).
[4] CB Insights (2017a), Insurance Tech Startups Raise $1.7B Across 173 Deals in 2016 (January) https://www.cbinsights.com/blog/2016-insurance-tech-funding/
[5] CB Insights (2016a), Analyzing the Insurance tech Investment Landscape (July).
[6] Coombs, Nathan (2016) What is an algorithm? Financial regulation in the era of high-frequency trading, 45, Economy and Society.
[7] Gartner (2016), Measuring the Strategic Value of the Internet of Things for Industries (April 28).

**International Journal of Research in Economics and Social Sciences(IJRESS)**
Available online at: http://euroasiapub.org
Vol. 13 Issue 8, August- 2023
ISSN(o): 2249-7382 | Impact Factor: 8.018
**(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)**

[8] IHS Markit (2016), Usage-Based Insurance Expected to Grow to 142 Million Subscribers Globally by 2023 (6 May) http://press.ihs.com/press-release/automotive/usage-based-insurance-expectedgrow-142-million-subscribers-globally-2023-i.

[9] Keller, B & Hott, C (2015), Big data, Insurance and the Expulsion from the Garden of Eden (Geneva Association Insurance Economics Newsletter No.72).

[10] McKinsey (2010), The Internet of Things (March) www.mckinsey.com/industries/high-tech/ourinsights/the-internet-of-things.

[11] Mulder, JM (2016), 100 RegTech startups to follow (17 June) https://www.linkedin.com/pulse/100- regtech-startups-follow-jan-maarten-mulder.

[12] UK Transport Research Laboratory (2015), Provision of telematics research (2015).

**[13]** Zurich Fleet Intelligence (2016), Reduced fleet operating costs www.zurichfleetintelligence.com/usen/benefits.php.