

TUTDoR

Analytical hierarchy processes and Pareto analysis for mitigating cybercrime in the financial sector.

Item Type	Article
Authors	Akinbowale, Oluwatoyin Esther;Klingelhöfer, Heinz Eckart;Zerihun, Mulatu Fekadu
Publisher	Emerald
Rights	Attribution-NonCommercial-ShareAlike 4.0 International
Download date	2026-04-14 08:45:47
Item License	http://creativecommons.org/licenses/by-nc-sa/4.0/
Link to Item	https://hdl.handle.net/20.500.14519/2810

Analytical hierarchy processes and Pareto analysis for mitigating cybercrime in the financial sector

Oluwatoyin Esther Akinbowale, Heinz Eckart Klingelhöfer and
Mulatu Fekadu Zerihun

*Faculty of Economics and Finance, Tshwane University of Technology,
Pretoria, South Africa*

Abstract

Purpose – The purpose of this study is to use a decision support model based on the Analytical Hierarchy Process (AHP) and Pareto analysis (PA) for ranking the impact of different kinds of cybercrime in organisations in the financial sector to support decisions on cybercrime mitigation.

Design/methodology/approach – From a structured questionnaire to the staff of 17 licensed banks in South Africa in charge of management, administration and operations, the perceived effect of cybercrime on the organisation's goals, namely, organisation's profitability, goodwill, customers' satisfaction and risk management was derived. The pairwise comparison of the organisation's goals and identified forms of cybercrime was done using the AHP.

Findings – The results obtained indicate that there was a consensus (100% of the answers) that the effect of cybercrime has negatively impacted the organisation's objectives profitability and goodwill. Also, still 95.23% of the respondents agreed that the effect of cybercrime has negatively impacted the level of customers' satisfaction, while only 7.15% saw an impact on the organisation's risk management processes. Using these results in the AHP, analysis delivers a hierarchical order about the relevance of prevalent forms of cybercrime for the organisation's cybercrime mitigation. The PA further shows the magnitude of the forms of cybercrime relative to each other.

Practical implications – Hence, this study provides a decision support framework for organisational management in the quest to explore the impact of cyber fraud. It can serve as a practical guided approach for the application of AHP analysis for the existing and emerging forms of cybercrime.

Originality/value – The novelty of this study lies in the fact that the combination of the AHP and PA to support solving a multi-criteria decision problem relating to the prevalence of cybercrime has not been sufficiently highlighted by the existing literature.

Keywords Pareto analysis, Analytical hierarchy process, Cybercrime, Decision model, Multi critical decision

Paper type Research paper

1. Introduction

The cases of cyberattacks on the emerging economies are rising rapidly (Kshetri, 2019). The recent advances in information technology (IT) have been identified as one of the prime drivers of the financial sector which has continued to transform the sector (Ali *et al.*, 2017). This has assisted the financial sector to extend its services, and to gain some competitive edge with significant improvement in customers' satisfaction. For instance, the introduction of the e-banking platform has made transactions much easier and simpler compared to the traditional banking system. With e-banking, transactions and other related financial activities are carried out using IT devices instead of human resources in the traditional banking system. The e-banking services permit transactions without any physical



interaction between the bank and the customers as customers can easily access the bank's information and services via different internet platforms (Agrawal, 2016). However, the same avenue which serves as the agent of transformation is still being exploited for the perpetration of cybercrimes. This has a far reaching effect on the integrity and reputation of financial institutions by undermining public confidence.

Cyberspace is characterised by sharp and unethical practices with cybercrime on the increase over the years (Uma and Padmavathi, 2013). The exploitation of cyberspace for cybercrime such as securing information without authorisation, malware attacks, IP theft, fiscal fraud, extortion, online fraud, spying, disabling of networks, fake links, impersonation, data and cash theft are consequential to the customer, financial institutions and the economy at large (Detica Limited, 2011). In South Africa, 13,438 cybercrime incidences were reported in 2017 which reportedly cost the banking industry more than R 250m in gross losses and the cybercrime incidences grew by 20% from 2018 with an increase in the gross losses by 8% (South African Banking Risk Information Centre, 2018). In 2015, it was reported that there were a total number of 602 million cybercrime victims on a global scale with South Africa having an approximate 8.8 million of such cases (Symantec Report, 2016). There are similar reports on the cost of cybercrime occurrences globally (Centre for Strategic and International Studies, 2014; Serianu, 2016; Symantec Report, 2016; South African Banking Risk Information Centre, 2018). Cybercrime has constituted an increasing global threat, the resultant effects on the economy, financial institutions and society can no longer be downplayed (UK Finance, 2020). Therefore, the motivation for this study is the quest to reduce the occurrences of cybercrime by tackling cybercrime from the primary source rather than focusing on measures to minimise the impact after such occurrences. The proactive measures of tackling cybercrime have been identified as sustainable in the fight against cybercrime (Ali *et al.*, 2017; UK Finance, 2018; Malik and Islam, 2019). The determination of the impact of prevalent forms of cybercrime in the financial sector calls for a decision support model which allows dealing with multi-criteria decisions.

The objective of this study is to use the Analytical Hierarchy Process (AHP) and Pareto analysis (PA) as tools for ranking and visualising the impact of different kinds of cybercrime on the overall goal in organisations in the financial sector via different (multi) decision criteria. Based on survey data, at first, relative weights were allocated to different forms of cybercrime based on their pairwise comparison with respect to their importance on fulfilling the organisational targets, before the overall weight is calculated using the AHP. In addition, the Pareto distribution diagram is used to show the magnitude of the possible impact of each of the cybercrime forms relative to the organisation's cybercrime mitigating goals. Hence, this paper provides a decision support framework to assess the impact of different forms of cybercrime on the target system to tackle and mitigate the identified forms of cyber fraud in a sustainable way.

The rest of the paper is organised as follows: Section 2 presents the literature review, Section 3 presents the implementation of the AHP and Pareto distribution diagram and further discussions on the results obtained from an example were presented in Section 4 while Section 5 concludes the study with the summary of the findings and appropriate recommendations.

2. Literature review

Cybercrimes have been defined as fraudulent activities carried out with the use of computers, the internet and other IT devices, hence the crime is digital in nature (Okeshola and Adeta, 2013). Omodunbi *et al.* (2016) identified the forms of cybercrimes as fraudulent

electronic mails, impersonation, identity theft, blackmail, forgery, cyber harassment, hacking, spamming, automated teller machine (ATM) spoofing, piracy and phishing. Broadhurst *et al.* (2014) proposed a framework for tracking the evolution of the organisational forms that cybercrimes take to mitigate cybercrime occurrences. Cybercrime has become big business with the global impact exceeding \$450bn a year as crime, extortion, blackmail and fraud move (UK Finance, 2018). This estimate agrees significantly with the estimate reported by the Centre for Strategic and International Studies which puts the average global annual loss due to cybercrime as \$475bn per annum (Centre for Strategic and International Studies, 2014). Already in 2014, the losses from cybercrime for the four largest economies in the world, i.e. the USA, China, Japan and Germany), reached \$200bn (Centre for Strategic and International Studies, 2014). The exploration of borderless cyberspace through digitisation, adoption of the emerging IT and internet of things solutions, increasing ownership of smart devices, social medial usage has continued to increase the rate of transformation experienced in all sectors (Ali *et al.*, 2017; Malik and Islam, 2019). However, as good as this may sound, it is not without a challenge: the transformation comes with new risks and vulnerabilities that could undermine the digital advancement and transformation. Chief amongst the challenges of digitalisation is the global rise in cybercrime-related occurrences with the IT infrastructures and devices of financial institutions and the individuals becoming targets for perpetrators (Ali *et al.*, 2017). The prevalence of cybercrime has been linked to the vulnerability of victims, lack of awareness, data breaches, unauthorised intrusion in individual's and financial institutions, weak monitoring measures and security capabilities and poor website security (Dzomira, 2014; Kshetri, 2019).

The evolution of IT infrastructure has increased the reliance of financial institutions on information and communications technology (ICT) for business transformation. However, the trends and threats of cybercrime could pose a significant danger without effective mitigating measures (Dzomira, 2014). Another area where cybercrime is prevalent is in the area of online money transfers using smart devices or mobile phones (Dzomira, 2014). It was estimated that 14% of all Africans with operational accounts receive money via online mobile transfers (UNCTAD, 2015). Hence, there evolves a need for manufacturers to prioritise security during the design phase of such product's development to prevent system hacking and unauthorised intrusions. It will take the combined efforts from governments, financial institutions and civil society to fight cybercrime so that financial institutions can maximally explore the prospects of the digital infrastructure as a driver of the economy. To reach this, there is also a need for increased public sensitisation about the prevalence of cybercrime and precautionary measures. This is underlined by the fact, that, for example, in South Africa, it was estimated that about 20% of the social network users usually share their passwords with others, while 21% connect with people they do not know (Symantec Report, 2016). This means that the public should be very careful about information management when using cyberspace most especially the ones that are very sensitive.

Basically, cybercrime can be perpetrated within or outside an organisation. The employee of an organisation can take advantage of easy access to the bank's and customers' information to perpetrate crime. On the other hand, people outside an organisation can also exploit the weak security measures of the financial institutions and ignorance of unsuspecting customers to perpetrate fraud. It was estimated that 80% of the cybersecurity breaches stem directly or indirectly (i.e. through collaboration with external bodies) from the people within the organisation (Hinde, 2003). This is because insiders have easy access to information about the financial institution and its control measures. As such they could invent cover-up schemes which can promote the affinity for continuous perpetration of such crimes. This calls for the development of robust internal control measures, such as periodic

auditing, close monitoring, forensic investigation and may also include intermittent staff shuffles or redeployments. The vulnerability of customers and financial institutions to external cyberattacks can also be traced to low levels of sensitisation and the lack of proper online monitoring systems (Balan *et al.*, 2017). This points to the fact that financial institutions need to reinforce existing security apparatus and intelligent systems to be more proactive rather than being reactive.

Some previous researchers have indicated that most cybercrime incidences were perpetrated through phishing, data theft and bank verification number scam, credit/debit card fraud, money laundering, pharming, malware, hacking, virus and the use of electronic spam mails (Omodunbi *et al.*, 2016; Dzomira, 2014; Mugari *et al.*, 2016; Rao, 2019). The summary of the research findings and the nature of cybercrimes prevalent in financial institutions are presented in Table 1 and Figure 1.

From the literature reviewed in Table 1, the 13 identified forms of cybercrime are highlighted as follows:

- The first one is phishing. Phishing is a form of cybercrime involving the theft of personal information or identity of a subscriber or authorised businesses or financial institutions for fraudulent purposes (Boateng and Amanor, 2014; Omodunbi *et al.*, 2016). It is regarded as the most common type of identity theft (KPMG, 2017; Chaudhary, 2014; Mugari *et al.*, 2016).
- The second one is data theft. Data theft is the act of unlawful acquisition and possession of sensitive data, which could include an unencrypted credit card, source code, customers' information and employee records (Hedayati, 2012; AICPA, 2017).
- Thirdly, we have hacking, which is the act of gaining unlawful access to databases or systems of financial institutions to acquire customers' or organisational confidential information. The vulnerability of a weak security system is often exploited by perpetrators to gain unlawful access to organisation databases to steal information or to make the unauthorised transfer of cash from customers' accounts (Mugari *et al.*, 2016; Kumudha and Rajan, 2018).
- Malware represents the fourth item in this list, involving the secret installation of an unauthorised program into the computer system secretly with the aim of stealing sensitive information. The installation of the malicious software is to enable perpetrators unlawfully access the hard drive of the systems to collect sensitive information for fraudulent activities (Uppal *et al.*, 2014; UN, 2013). The malicious software can alter the network systems and other settings of the system without any notification or permission from the authorised users. The malicious software can be in the form of a virus capable of infecting the whole system or in the form of a normal program concealed for stealing personal and confidential information.
- The fifth item in this list is what is called the electronic spam mail that involves sending junk unsolicited e-mail to lure unsuspecting users to release sensitive information for fraud perpetration (Geeta, 2011).
- The sixth item is skimming. The act of skimming is common with ATM users. This involves the use of an electronic device on an ATM which scoops sensitive information from the credit card's whenever a customer uses the machine (Omodunbi *et al.*, 2016).
- The seventh one is online theft that often happens in the form of cash transfer or credit card theft. The online cash transfer involves the unlawful transfer of cash from the account of an unsuspecting customer once the sensitive information of

Author	Contribution	Identified forms of cybercrime
Omodunbi <i>et al.</i> (2016)	Analysis of cybercrimes occurrences in tertiary institutions in Ekiti-State, Nigeria	Phishing, data theft, theft of verification number, hacking, malware, spamming
UK Finance (2020)	Overview of payment industry fraud	Phishing, card theft, identity theft, data theft, online fraud
Ali <i>et al.</i> (2017)	Analysis of the effects of cyber threats on customers' behaviour in e-banking services	Phishing, vishing, malware, hacking, online fraud, denial of service attack, malware
Mugari <i>et al.</i> (2016)	Analysis the nature of cybercrime prevalent in the financial institutions in Zimbabwe	Hacking, phishing, malware, spamming
Business Ghana (2018)	Cyber security directive for financial institutions in Ghana	Electronic spam mail, malware, hacking, phishing, credit card theft
AICPA (2017)	Cost of certain types of cybercrimes in the USA	Phishing, malware, data theft, hacking, malware
Symantec Report (2016)	Cyber-crime and cyber security: Trends in Africa	Malware, hacking, phishing, data theft, spamming, credit card theft
Njeru and Gaitho (2019)	Investigating extent to which cybercrime influences performance of commercial banks in Kenya	Hacking, credit card theft, phishing
Detica Limited (2011)	The cost of cybercrime in the UK	Spying, phishing, online theft/ fraud, malware, hacking
Symantec Report(2018)	Evaluation of significant cybercrimes	Online theft/fraud, phishing, crypto extortion
Tiwari <i>et al.</i> (2016)	Analysis of cybercrime and security	Malware, denial of service attack, cyberstalking, online fraud, identity theft, phishing
Balan <i>et al.</i> (2017)	Data analysis of cybercrime in businesses	Online theft/fraud, hacking, phishing, malware
Dzomira (2014)	Assessment of the risk of cyber fraud to the financial institutions in Zimbabwe	e-transfer/online theft, credit card fraud, phishing, malware, spamming, pharming, hacking
Rao (2019)	Assessment of cybercrime in the banking sector in India	Hacking, phishing, spamming, vishing, skimming
McGuire and Dowling (2013)	Review of the evidence, summary of key findings and implications	Phishing, spamming, fake SMS, online theft, malware, hacking
Rezk <i>et al.</i> (2017)	Assessment of the impact of cybercrime on E-commerce	Cyber terrorism, spoofing, spamming, phishing, credit card fraud sim-box fraud
Bamrara <i>et al.</i> (2013)	Cyber attacks and defense strategies in India	Spoofing, online theft, hacking, malware, credit card fraud
Broadhurst <i>et al.</i> (2014)	Organisations and cyber crime	Malware, spamming, phishing, hacking, data theft, domain squatting, online theft
Okutan and Çebi (2019)	Development of a a framework for cybercrime investigation	Malware, spamming, phishing, hacking, data theft, online theft, cyber threat, cyberstalking, credit card fraud
Ajayi (2016)	Investigation of the challenges to enforcement of cybercrimes laws and policy	Malware, spamming, phishing, hacking, data theft, online theft, cyber threat, credit card fraud

Table 1.
The nature of cybercrimes identified in the financial institutions

(continued)

Table 1.

Author	Contribution	Identified forms of cybercrime
UN (2019)	Analysis of cybercrime	Cyberstalking, malware, spamming, phishing, hacking, data theft, online theft, cyber threat, credit card fraud, whaling
Ch <i>et al.</i> (2020)	Computational system for the classification of cybercrime offenses using machine learning	Spoofing, piracy, spamming, phishing, hacking, data theft, online theft, cyber threat, credit card fraud

Source: Own synthesis

such a user is unlawfully acquired (Omodunbi *et al.*, 2016). On the other hand, online credit card theft involves the decoding of the secret pins and login details of an unsuspecting user for fraudulent activities (Tan Harry, 2002; Sonepat and Sonepat, 2014).

- Spying represents the eighth in the list. It refers to the use of codes to infiltrate the website of financial institutions to obtain sensitive information illegally for fraud perpetration. Spyware is one of the software often used for spying and capturing information on the system or during the transmission of information between the system and other websites (Dzomira, 2014).
- Cyberstalking is the ninth and it involves the use of ICT to perpetrate series of actions aimed at threatening, attacking, harassing or verbally abusing an individual. (UN, 2019).
- Pharming as the tenth item involves the creation of a fake, duplicate website aimed at deceiving unsuspecting users to input their login credentials (UN, 2019).
- The last three in this list are vishing, spoofing and whaling. Vishing involves the use of social engineering devices or platforms such as telecommunications or smartphones to access private or organisation information for the purpose of fraud perpetration (Rao, 2019). While spoofing refers to making deceptive calls to individuals to request for sensitive or personal information or to siphon money (Ch, 2020), finally, whaling means pretending to be a higher-level executive in a company, lawyer, accountant or another in positions of authority and trust, to trick employees into sending them funds (UN, 2019).

Out of the 13 identified forms of cybercrime, 8 common forms of cybercrime were identified as the most predominant ones: phishing, data theft, hacking, malware, spam e-mail, skimming, online theft and spying. Hence, also in this study, using the AHP and PA, the analysis of their impact is considered exemplarily. Martin and Rice (2011) emphasised the need to understand and address the concerns of the stakeholders of financial institutions due to the growing rate of cybercrime. The increasing rate of cybercrime is inversely proportional to customers' satisfaction, organisation's profitability and goodwill. The negative impacts and severity of cybercrime have been identified as: loss of organisation goodwill and reputation, society, customers and stakeholders' dissatisfaction, loss of public confidence, loss of revenue and other associated risks (Saini *et al.*, 2012; Lagazio *et al.*, 2014).

Some of the identified indicators for measuring the impact of cybercrime on financial institutions include customer and employee satisfaction, product innovation, organisation's growth and productivity, market share and position in the stock market, financial losses, loss of customers and business partners or opportunities, loss of reputation and decrease in the organisation's market value (Goel and Shawky, 2009; Kraemer-Mbula *et al.*, 2013). The effect of cybercrime poses a great threat to the individual's and organisation's privacy, public safety and security risks. Furthermore, cyber-attacks can disrupt the ICT infrastructure such as data centres and networks in the financial institutions and society at large (CSIS, 2014). The Information Security Institute (2013) has highlighted some of the impacts of cybercrime as follow: loss of intellectual property and sensitive information or data, service disruptions, damage to the brand name and the organisation's reputation, compensation payments to victims and penalties for service or business disruptions, cost of countermeasures, insurance and risk mitigation, financial or revenue loss, loss of trade and competitiveness, job loss, etc.

To mitigate cybercrime, the gathering of intelligence reports, robust internal control policies, monitoring of online activities and effective response to suspected cases amongst others will assist in the consolidation of the security systems of the financial institutions. Gordon *et al.* (2003) proposed a generic cyber risk management framework for information security. The framework encompasses four steps of a cyber risk insurance decision plan, namely, information security risk audit, assessment of insurance coverage, evaluation of available policies and selection of suitable policy. It could be accompanied by the development of a real-time alert system capable of creating awareness for both financial institutions and their customers (Akinbowale *et al.*, 2020a, p. 945). Akinbowale *et al.* (2020b, p. 1253) also developed two simplified conceptual models for cyber fraud mitigation. The first model incorporates the principles of forensic accounting into the organisation structure while the second captured the detailed processes of investigation and comprehensive data analysis aimed at uncovering fraud. The feasibility of integrating forensic accounting and management control systems tools geared towards cybercrime mitigation has also been demonstrated (Akinbowale *et al.*, 2021, p. 1).

In addition, the nature of transactions, which often take place without any physical interaction between the bank and customers, can sometimes be risky and jeopardise the process of uncovering illicit acts. Hence, strict systems of authorisation should be put in place to reduce cybercrime occurrences.

3. Methodology

This study considered the use of a decision support model based on the AHP and PA for the determination and analysis of the existing and emerging forms of cybercrime. From the literature, the forms of cybercrime were first examined, followed by the identification of possible organisational goals to stem the tide of cybercrime, which form the criteria. From a structured questionnaire made available to the staff of 17 licensed banks in South Africa in charge of management, administration and operations the effect of cybercrime on the four factors: 1. organisation's profitability, 2. goodwill, 3. customers' satisfaction and 4. risk management was determined. The results obtained are presented in Section 4.1. The pairwise comparison of the importance of these factors (criteria) allows the organisation to determine their contribution to its goal as a basis for decisions on effective cybercrime mitigation.

3.1 The analytical hierarchy process

The AHP decision model was used for the ranking and pairwise comparisons of the different forms of cybercrime in this study. Its use offers a knowledge-based decision support system for determining the impact of each form of cybercrime on the overall (financial) objective of an organisation for effective decision-making (Jayant, 2011; Subramanian and Ramanathan, 2012). AHP provides a quantitative approach of pairwise comparison of criteria or competing factors and ranking of the alternatives (Vargas, 2010). The approach provides a mathematical and scientific decision support framework for resolving a multi-criteria decision problem and justifying the choices made in line with the organisation's goals (Coyle, 2004; Odu, 2019).

To do so, the AHP tries to rank the different factors and criteria. This means, that the first step in the application of AHP to a multi-criteria decision problem involves the identification of the organisation's goals and the competing criteria or factors. This is followed by the decomposition of the problem into a hierarchy based on the identified criteria or factors for pairwise comparison for each of the identified criteria or factors. During the pairwise comparisons, numerical values are allocated to the paired criteria or factors and based on this in the next step, the weights of each of the criteria or factors with respect to the higher ranking goal/criterion are determined. However, as the pairwise comparison between different factors/criteria can reveal contradictions in the relative weights, a consistency check needs to follow to see whether the resulting inconsistencies are still acceptable. If not, the comparative weights with respect to the higher-ranking goal/criterion need to be reassigned.

One of the main distinctive contributions of the AHP is the capability of converting empirical data into mathematical models when compared with other comparing techniques (Vargas, 2010). In the literature review, four criteria to address the negative impacts and severity of cybercrime have been identified: effective risk management, improvement in the organisation's profitability, improvement in the goodwill (integrity) of financial institutions and customers' satisfaction.

Once their (subjective) relationship with respect to the overall goal of the organisation is established, effective mitigating measures can be developed to address the factors, which promote cybercrime. The use of the Pareto distribution diagram for analysis will further allow for understanding the impact of the different kinds of cybercrime onto the organisation's objectives better.

From the literature survey presented in Section 2, the eight common forms of cybercrime are identified as: phishing, data theft, hacking, malware, spam e-mail, skimming, online theft and spying. In addition, cybercrime had been reported to have a negative impact on the four criteria: organisation's profitability, goodwill, customers' satisfaction and risk management (Goel and Shawky, 2009; Martin and Rice, 2011; Saini *et al.*, 2012; Kraemer-Mbula *et al.*, 2013; Lagazio *et al.*, 2014). Hence, an organisation may follow the goal of mitigating cybercrime to reduce its negative impact on these four criteria, while the eight common forms of cybercrime according to Section 2 are identified as the factors that need to be mitigated. The pairwise comparison of each of the contributing factors with the other factors can then be determined using the fundamental scale of pairwise comparison and random consistency analyses (Saaty, 2008).

After the identification of these four criteria and eight factors, the organisation allocates comparative weights to each pair of them on a scale of integers from 1–9 (and reciprocal 1/1 to 1/9), expressing the relative importance of one criterion in comparison to another one in the decision maker's opinion (Saaty, 2008). By referring to Weber and Fechner, Saaty (2008) argues that this comparison will usually be done by using positive integer values (and their

reciprocals) because they “are intrinsic to our ability to make comparisons”, but, of course, if found to be inadequate for such a pairwise comparison, one may extend the scale also to then more appropriate (and, perhaps, non-integer) values. The pairwise comparison scale for the AHP preferences as given by Saaty is presented in Table 2.

Applying this scheme at first to the four criteria identified earlier which define the organisation’s goal for mitigating cybercrime: organisation’s profitability (1), goodwill (2), customers’ satisfaction (3) and risk management (4), the possible results of such a pairwise comparison lead to a 4 × 4 comparison matrix as presented in Table 3. Based on the results obtained from the survey (presented in Section 4.1), the criteria are prioritised and weights are allocated to each criterion based on their importance.

The entries in this 4 × 4 matrix can be understood as follows: Criteria 1 and 2 are seen three times more important than criterion 3 (leading to the allocation of weight 3 in the third column of the first two rows). Criteria 1 and 2 are also seen seven times more important than criterion 4 (leading to the allocation of weight 7 in the fourth column of the first two rows). With respect to the comparison of the criteria 1 and 2, it is assumed that both are of equal importance, hence allocated a weight of 1 (leading to 1 in the second row of the first column and – equally – in the first row of the second column).

On the next, second level, the impact of the eight common forms of cybercrimes (as identified in the literature review) with respect to the four criteria is dealt with in a similar way, leading to 8 × 8 comparison matrices. These identified common forms of cybercrimes based on the results of Chapter 2 are presented in Table 4.

Figure 1 then shows the paired comparison of the eight different forms of cybercrime (Table 4) with respect to the four criteria (organisation’s profitability, goodwill, customers’ satisfaction and risk management) mentioned in Table 3 to address the negative impacts and severity of cybercrime.

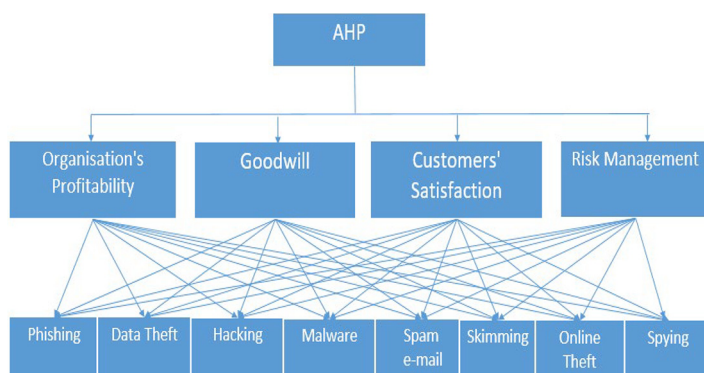
Table 2.
The pairwise comparison scale for the AHP preferences

Rating	Judgement
9	Extremely preferred
8	Very strongly to extremely
7	Very strongly preferred
6	Strongly to very strongly
5	Strongly preferred
4	Moderately to strongly
3	Moderately preferred
2	Equally to moderately
1	Equally preferred

Source: Saaty (2005)

Table 3.
The criteria and the corresponding weights allocated

Criteria	1	2	3	4
1	1.00	1.00	3.00	7.00
2	1.00	1.00	3.00	7.00
3	1/3	1/3	1.00	3.00
4	1/7	1/7	1/3	1.00
Sum	2.48	2.48	7.33	18.00



Source: Own Synthesis

Figure 1. Paired comparison with respect to the criteria for the factors

Coded factors	Common forms of cybercrime
A	Phishing
B	Spying
C	Malware
D	Data theft
E	Spam e-mail
F	Online theft
G	Hacking
H	Skimming

Table 4. The common forms of cybercrimes

Having the tables of paired comparison of the different criteria, leading to a square matrix A of relative weights, the next step is to try to bring the criteria or competing factors into a ranking and to get an indication of the magnitude of their weight to the superior criterion/goal. This can be done by solving equation (1) for the square matrix A , which delivers the eigenvalues λ and right eigenvectors x of the square matrix A :

$$Ax = \lambda x \tag{1}$$

where:

- A is the square matrix, containing the results of the pairwise comparison of the n (sub) criteria and factors (as given e.g. by Table 3),
- x is the right eigenvector of the length n for the n (sub-) criteria of the matrix A to a given eigenvalue and
- λ is the scalar quantity. The values of λ that satisfy the equation are the eigenvalues, leading to the corresponding values of x as the right eigenvectors.

Usually, a matrix of rank m has m (real or, in general, complex) eigenvalues, some of which might have an algebraic multiplicity of $k > 1$ (meaning its multiplicity as a root of the characteristic polynomial) and the sum of all eigenvalues equals the trace of the matrix (i.e. the sum of its diagonal elements). However, if the square matrix A is consistent (a

characteristic which needs to be checked later), all its rows can be calculated as multiples of the first one, so that it is of unit rank. Hence, it will only have one eigenvalue which will equal the trace of the matrix (which is n as all the diagonal elements are 1): $\lambda = n$. Therefore, the corresponding right eigenvector \mathbf{x} in its economic interpretation will deliver the ranking and weight of the criteria/competing factors – a reason why it is also called “priority vector”. This becomes even more obvious if it is normalised in a way that its components add up to 1 (100%).

Nevertheless, not always the square matrix A is consistent, so that more eigenvalues than only one may exist. Following the general derivation of Saaty (1977, 2008), one then has to use the maximum eigenvalue $\lambda_{max} \geq n$ to receive the priority vector, delivering the (absolute) priority of each of the criteria to the overall goal. Unfortunately, one then has to check whether the inconsistency is still acceptable. To do so, one calculates the consistency index (CI) and the consistency ratio (CR), respectively, according to equations (2) and (3) (Saaty, 1980; Saaty, 2008):

$$CI = \frac{\lambda_{max} - n}{n - 1} \quad (2)$$

$$CR = \frac{CI}{RI} \quad (3)$$

where:

λ_{max} is the maximum eigenvalue (which delivers the priority vector following the pairwise comparison),

n is the number of criteria and

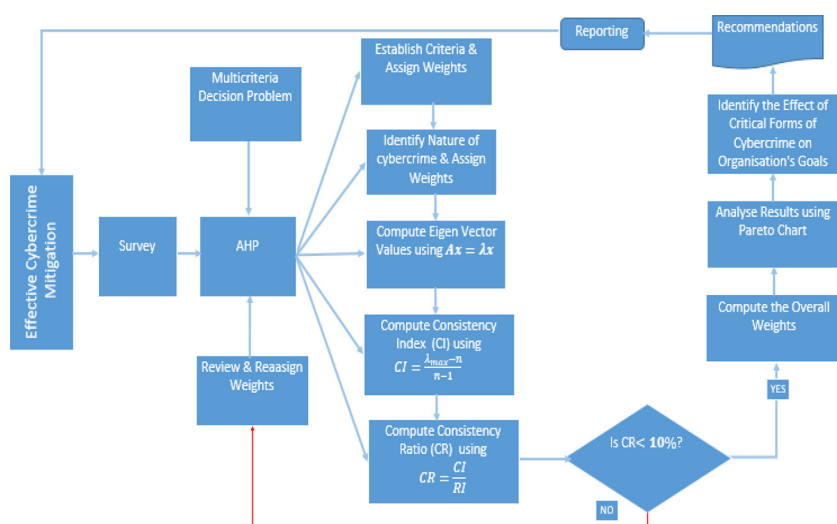
RI is the random consistency index, an index of the consistency for random judgments as given by Saaty (2008).

Then, the level of consistency of the decision maker’s choices during the paired comparisons could be said to be high when the CR is less than 0.10 (Saaty, 2008). If not, the comparative weights with respect to the higher-ranking goal/criterion need to be reassigned.

For Figure 1, this would be done four times for the eight factors on the second level with respect to the four different criteria on the first level and for the four different criteria on the first level to the overall goal. In case $CR < 10\%$ for all the criteria and factors, the next step is the computation of the total impact, the overall weight of each of the eight factors (i.e. of the eight different forms of cybercrime) on the organisational target. Statistical analysis such as the Pareto distribution diagram can then be used to visualise the ranks of the overall weights obtained from the AHP model.

3.2 The Pareto analysis

A Pareto distribution diagram is used here to visualise the ranks of the overall weights obtained from the AHP model for a better understanding of the impact of the different kinds of cybercrime on the organisation’s objectives better. The PA is a tool that helps in the identification of critical factors for effective monitoring and decision-making. The tool consists of three major steps, namely, classification, differentiation and allocation (Grosfeld-Nir *et al.*, 2007). The classification step involves the sorting out of attributes of a phenomenon to build a Pareto distribution diagram. The diagram can then be used to classify the identified attributes into classes based on their severity.



Source: Own Synthesis

Figure 2. Decision framework for the implementation of the AHP and Pareto distribution diagram analysis

The differentiation involves the setting of a specialised policy for each of the identified classes while the last step, the allocation, deals with the assignment of resources accordingly. An ideal Pareto distribution diagram is one in which about 20% of the identified attributes have an 80% weight in terms of the relative frequency, thereby identifying the critical factors (Grosfeld-Nir *et al.*, 2007).

For the implementation of the solution, which combines the AHP and PA for cybercrime mitigation in an organisation, the proposed framework is presented in Figure 2. The procedural steps as shown in the Figure include the following: firstly, is the establishment of criteria (based on the organisation's goals) and assignment of pairwise comparative weights. This is followed by the identification of the individually competing factors (nature of cybercrime) and again assignment of pairwise comparative weights. Next, is the computation of the priority vector for the identified criteria and factors and the computation of the CI and CR for each of the identified criteria and factors. After this, is the determination of the consistent levels of the computed CIs and CRs. If the CR is low ($CR < 10\%$), the judgement regarding the weights allocation and the pairwise comparison of the respective criterion/factor is said to be consistent; otherwise, the weights have to be reassigned for this criterion/factor because the pairwise comparison led to an inconsistent system. This means that the procedure will go back to Step ii for all those criteria/factors where $CR \geq 10\%$. In case $CR < 10\%$ for all the criteria and factors, the next step is the computation of the overall weight of each of the factors, in this case, the different forms of cybercrime, i.e. the impact (overall weight) of each of the factors (in this case: of the different forms of cybercrime) on the organisational target. The final stage of the procedure involves the analysis of results using the Pareto distribution diagram and the identification of the critical forms of cybercrimes for the organisation to decide on preventing or mitigating measures.

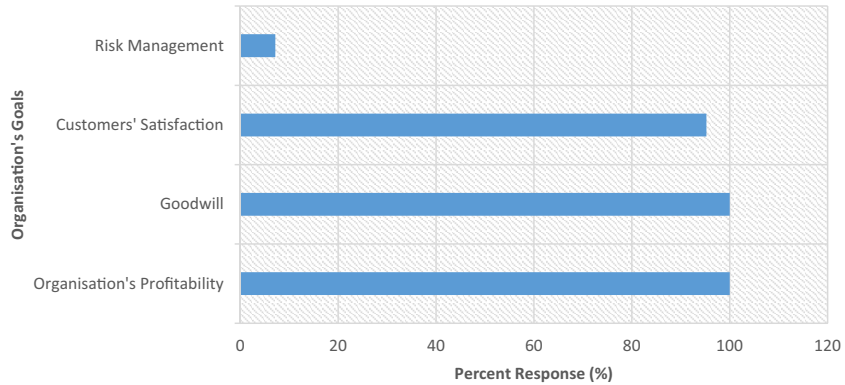


Figure 3.
Effect of cybercrime on the organisation's goal

Source: Survey

4. Results and discussion

4.1 Results obtained from the survey

Figure 3 shows the per cent response to the participants to the effect of cybercrime on the four criteria (organisation's goal) identified, namely, organisation's profitability, goodwill, customers' satisfaction and risk management) in the South African banking sector. The responses were obtained from 42 people who participated in the survey. The results obtained indicate that there was a consensus amongst all the respondents (100%) that the effect of cybercrime has negatively impacted the organisation's profitability and goodwill. In total, 95.23% answered that the effect of cybercrime has negatively impacted the level of customers' satisfaction while 4.78% refuted the claim. Only 7.15% of the respondents claimed that the effect of cybercrime has a negative impact on the organisation's risk management processes, while 92.85% refuted the claim.

4.2 Application of analytical hierarchy process for ranking the impact of cybercrime

Based on the results obtained from the survey (presented in Section 4.1), the criteria are prioritised and weights are allocated to each criterion based on their importance. The organisation's criteria (organisation's profitability and goodwill) on which the effect of cybercrime has the most negative impact are allocated higher weights followed by customers' satisfaction, while risk management has the least weight.

Table 5, which repeats the values of Table 3, shows the paired comparison matrix of the criteria identified by the respondents from the South African banking sector with respect to its goal for cybercrime mitigation. The competing criteria are paired based on their relative

Table 5.
The paired comparison matrix with respect to the criteria and the resulting priority vector (six comparisons)

Criteria	1	2	3	4	Priority vector (%)
1	1.00	1.00	3.00	7.00	40.20
2	1.0	1.00	3.00	7.00	40.20
3	1/3	1/3	1.00	3.00	14.30
4	1/7	1/7	1/3	1.00	5.40
Sum	2.48	2.48	7.33	18.00	

importance to the organisation's overall goal. The more important one criterion is seen in comparison to another one, the higher the value (on the scale from 1–9) and vice versa. In the following Table 5, (which repeats Table 3), criteria 2 and 3 are equally preferred and the criteria are three times more important than criterion 3 (criterion 3 only 1/3 of criteria 1 and 2) and seven times more important than criterion 4 (criterion 4 only 1/7 of criteria 1 and 2). For the following, it is further assumed that the four criteria identified earlier define the organisation's sub-objectives impacted by cybercrime: organisation's profitability (1), goodwill (2), customers' satisfaction (3) and risk management (4). Hence, the organisations indeed face multi-criteria decisions. The resulting paired comparison matrix with respect to the criteria and the resulting priority vector is presented in Table 5.

In Table 5, the priority vector of each of the criteria is an indication of the ranked priority of the sub-objectives based on computations obtained from their pairwise weights. The priority vector indicates the contribution and severity of each of the criteria (sub-objectives) to the organisation's goal. This further gives an indication of the magnitude of the weight of each of the criteria and their relative importance to the overall goal of the organisation.

The maximum eigenvalue λ_{max} is calculated thus:

$$\lambda_{max} = (0.420)(2.48) + (0.420)(2.48) + (0.1430)(7.33) + (0.0540)(18.00) = 4.10339$$

Here and in the following, the manual computation of the eigenvectors, the priority vectors, may be ambiguous and prone to error, hence the solutions were obtained computationally using the MATLAB 2018b software. However, it can also be done by solving the characteristic polynomial – and normalising the resulting eigenvector afterwards so that its components sum up to 1 (or 100%).

As the maximum eigenvalue $\lambda_{max} > 4 = n$, the square matrix A derived from Table 5 cannot be consistent. Hence, the next step is to calculate the CR to determine whether the level of consistency in the decision maker's judgement during the pairwise comparison is still acceptable (Saaty, 2008). The CI and ratio are calculated as follows from equations (2) and (3), respectively, considering that the RI for a 4×4 matrix is given as 0.89 (Saaty, 2008).

$$CI = \frac{4.10339 - 4}{4 - 1}$$

$$CI = 0.0344$$

$$CR = \frac{0.0344}{0.89}$$

$$CR = 0.0387$$

Hence, as $CR = 0.0387 < 10\%$, according to Saaty(2008) the level of consistency is indeed high. Therefore, it is possible to present the overall weight of the criteria as in Figure 4. This depicts the prioritisation of the organisation goals in ensuring effective cybercrime mitigation. From Table 5, the impact of criterion 1 (organisation's profitability) on the overall goal is 40.20%, while that of criterion 2 (goodwill) is 40.20%, criterion 3 (customers' satisfaction) is 14.30% and criterion 4 (risk management) is 5.40%. The priority vector (eigenvector) indicates the importance of each of the criteria to the organisation's goal. The

Figure 4.
Overall weight of the criteria

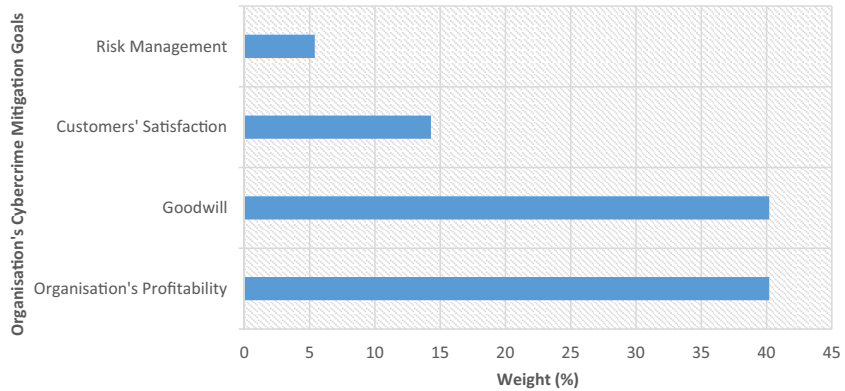
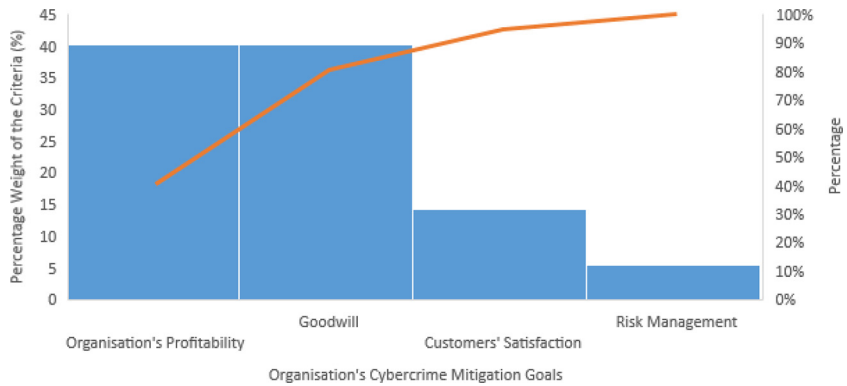


Figure 5.
PA of the per cent weight of the criteria (sub-objectives)



results imply that for this example, an organisation's profitability and goodwill are the most important criteria (sub-objectives) relative to the overall goal of the organisation. Compared to other criteria, they are 2.81 times more important than criterion 3 and 7.44 times more important than criterion 4.

The importance of the four mentioned criteria (sub-objectives) with respect to the overall organisation's goal is further depicted using a Pareto distribution diagram (Figure 5). Its left vertical axis is the per cent weight of the criteria while the right vertical axis represents the cumulative percentages over the criteria. The cumulative line at the centre of the plot is used for determining the cumulative significance of the criteria to the organisation's goal. Following the pairwise comparison of the criteria, the high start of the cumulative line indicates that criteria 1 and 2 (organisation's profitability and goodwill) are the most negatively impacted criterion compared to the other criteria, followed by criterion 3 (customers' satisfaction) while criterion 4 (risk management) is the least negatively impacted criterion.

In the same way as Table 5 for the 4 × 4 matrix before, Tables 6, 7, 8 and 9 present 8 × 8 matrices for the pairwise comparison for the factors on the second level (the different forms

of cybercrime) – and the resulting eigenvectors as priority vectors. The allocation of the weight was based on their prevalence as reported by the literature.

In Table 6, it is assumed that factor A (phishing) is five times more critical with respect to the first criterion on the higher level (sub-objective), organisation’s profitability, than factor B (spying) – and, *vc.* vs that factor B is only 1/5 of factor A. Furthermore, factor A is three times more critical than factor C (malware; factor C only 1/3 of factor A), seven times more critical than factor D (data theft; factor D only 1/7 of factor A), three times more critical than factor E (spam e-mails; factor E only 1/3 of factor A), two times more critical than factor F (online theft L; factor D only 1/2 of factor A), five times more critical than factor G (hacking; factor G only 1/5 of factor A) and nine times more critical than factor H (skimming; factor H only 1/9 of factor A).

With respect to the first criterion (organisation’s profitability), the impact of each of the factors (nature of cybercrime) in case of occurrence are as follow in this example: factor A: phishing (35.90%), factor B: spying (14.90%), factor C: malware (11.10%), factor D: data theft (5.60%), factor E: spam e-mail (10.50%), factor F: online theft (10.20%), factor G: hacking (5.50) and factor H: skimming (6.20%). Hence, the occurrence of factor A (phishing) would impact the highest on the sub-objective of consumer satisfaction followed by factor B (spying) and factor C (malware) with the least impacting one being the occurrence of factor F (skimming).

The maximum eigenvalue λ_{max} is calculated thus:

$$\lambda_{max} = (0.3590)(2.82) + (0.1490)(9.53) + (0.1110)(10.16) + (0.0560)(20.00) + (0.1050)(8.83) + (0.1020)(10.20) + (0.0550)(20.00) + (0.0620)(18.00)$$

$$\lambda_{max} = 8.864$$

Together with the RI for a 8×8 matrix as 1.40 (Saaty, 2008), one, therefore, receives for the CR:

$$CI = \frac{8.864 - 8}{8 - 1}$$

$$CI = 0.123$$

Factor	A	B	C	D	E	F	G	H	Priority vector (%)
A	1.00	5.00	3.00	7.00	3.00	2.00	5.00	9.00	35.90
B	1/5	1.00	3.00	5.00	1.00	2.00	1.00	2.00	14.90
C	1/3	1/3	1.00	3.00	1.00	2.00	3.00	1.00	11.10
D	1/7	1/5	1/3	1.00	1.00	1.00	1.00	1.00	5.60
E	1/3	1.00	1.00	1.00	1.00	1.00	3.00	2.00	10.50
F	1/2	1/2	1/2	1.00	1.00	1.00	5.00	1.00	10.20
G	1/5	1.00	1/3	1.00	1/3	1/5	1.00	1.00	5.50
H	1/9	1/2	1.00	1.00	1/2	1.00	1.00	1.00	6.20
Sum	2.82	9.53	10.16	20.00	8.83	10.20	20.00	18.00	

Table 6. The factors (forms of cybercrime) and their weights with respect to criterion (sub-objective) 1, organisation’s profitability (28 comparisons)

$$CR = \frac{0.0123}{1.40}$$

$$CR = 0.088$$

1000

In Table 7, with respect to the second criterion (goodwill), the impact of each of the factors (nature of cybercrime) in case of occurrence may be given as follows: factor A: phishing (41.60%), factor B: spying (8.80%), factor C: malware (11.60%), factor D: data theft (8.90%), factor E: spam e-mail (6.10%), factor F: online theft (8.90%), factor G: hacking (6.30) and factor H: skimming (7.80%). Factor A (phishing) is the cybercrime incidence with the highest impact on sub-objective goodwill followed by factor B (spying) and factor C (malware) with the least impact resulting from factor H (skimming).

The maximum eigen value λ_{max} and the CR are calculated thus:

$$\lambda_{max} = (0.416)(2.46) + (0.0880)(13.33) + (0.1160)(10.16) + (0.0890)(13.83) + (0.0610)(21.50) + (0.0890)(10.50) + (0.0630)(15) + (0.0780)(11)$$

$$\lambda_{max} = 8.655$$

$$CI = \frac{8.655 - 8}{8 - 1}$$

$$CI = 0.094$$

$$CR = \frac{0.094}{1.40}$$

$$CR = 0.067$$

Hence, as $CR = 0.067 < 10\%$, the level of consistency is also indeed high.

Table 7.
The factors and weights with respect to criterion 2, goodwill (28 comparisons)

Criteria	A	B	C	D	E	F	G	H	Priority vector (%)
A	1.00	7.00	5.00	7.00	9.00	3.00	5.00	3.00	41.60
B	1/7	1.00	1.00	1.00	3.00	1.00	1.00	1.00	8.80
C	1/5	1.00	1.00	2.00	3.00	1.00	3.00	1.00	11.60
D	1/7	1.00	1/2	1.00	3.00	1.00	2.00	1.00	8.90
E	1/9	1/3	1/3	1/3	1.00	2.00	1.00	1.00	6.10
F	1/3	1.00	1.00	1.00	1/2	1.00	1.00	2.00	8.90
G	1/5	1.00	1/3	1/2	1.00	1.00	1.00	1.00	6.30
H	1/3	1.00	1.00	1.00	1.00	1/2	1.00	1.00	7.80
Sum	2.46	13.33	10.16	13.83	21.50	10.50	15.00	11.00	

From Table 8, with respect to the third criterion (customers' satisfaction), the impact of each of the factors (nature of cybercrime) in case of occurrence may be given as: factor A: phishing (33.10%), factor B: spying (13.50%), factor C: malware (7.60%), factor D: data theft (16.30%), factor E: spam e-mail (8.90%), factor F: online theft (10.20%), factor G: hacking (6.10) and factor H: skimming (4.40%). Factor A (phishing) is the cybercrime incidence with the highest impact on goodwill followed by factor D (data theft) and factor B (spying) with the least impact resulting from factor H (skimming).

The maximum eigenvalue λ_{max} and the CR are calculated thus:

$$\lambda_{max} = (0.3310)(3.35) + (0.1350)(7.66) + (0.0760)(15.00) + (0.1630)(6.47) + (0.0890)(12.33) + (0.102)(9.33) + (0.0610)(18.00) + (0.0440)(24.00) +$$

$$\lambda_{max} = 8.541$$

$$CI = \frac{8.541 - 8}{8 - 1}$$

$$CI = 0.077$$

$$CR = \frac{0.077}{1.40}$$

$$CR = 0.055$$

Hence, with $CR = 0.055 < 10\%$, the level of consistency is also indeed high.

From Table 9, with respect to the fourth criterion (risk management), the impact of each of the factors (nature of cybercrime) in case of occurrence may be given as: factor A: phishing (27.40%), factor B: spying (13.60%), factor C: malware (23.80%), factor D: data theft (11.30%), factor E: spam e-mail (8.30%), factor F: online theft (4.20%), factor G: hacking (6.80) and factor H: skimming (4.70%). Factor A (phishing) is the cybercrime incidence with the highest contribution followed by factor C (malware) and factor B (spying) with the least impact resulting from being factor F (online theft).

Criteria	A	B	C	D	E	F	G	H	Priority vector (%)
A	1.00	3.00	7.00	1.00	5.00	3.00	7.00	5.00	33.10
B	1/3	1.00	2.00	1.00	2.00	1.00	3.00	3.00	13.50
C	1/7	1/2	1.00	1.00	1.00	1.00	1.00	1.00	7.60
D	1.00	1.00	1.00	1.00	1.00	1.00	3.00	7.00	16.30
E	1/5	1/2	1.00	1.00	1.00	1.00	1.00	3.00	8.90
F	1/3	1.00	1.00	1.00	1.00	1.00	1.00	3.00	10.20
G	1/7	1/3	1.00	1/3	1.00	1.00	1.00	1.00	6.10
H	1/5	1/3	1.00	1/7	1/3	1/3	1.00	1.00	4.40
Sum	3.35	7.66	15.00	6.47	12.33	9.33	18.00	24.00	

Table 8. The factors and weights with respect to criterion 3, customers' satisfaction (28 comparisons)

The maximum eigenvalue λ_{max} and the CR are calculated thus:

$$\lambda_{max} = (0.2740)(3.65) + (0.1360)(7.03) + (0.2380)(4.20) + (0.1130)(10.03) + (0.0830)(20.53) + (0.0420)(27.50) + (0.0680)(14.00) + (0.0470)(22.00) +$$

$$\lambda_{max} = 8.934$$

$$CI = \frac{8.934 - 8}{8 - 1}$$

$$CI = 0.133$$

$$CR = \frac{0.133}{1.40}$$

$$CR = 0.095$$

With $CR = 0.095 < 10\%$, the level of consistency is also still indeed high.

The overall weights (global weights) for the eight factors using the weights of the four criteria are computed as follows:

$$\text{Factor A : } 40.20(35.90) + 40.20(41.60) + 14.30(33.10) + 5.40(27.40) = 3736.79$$

$$\text{Factor B : } 40.20(14.90) + 40.20(8.80) + 14.30(13.50) + 5.40(13.60) = 1219.23$$

$$\text{Factor C : } 40.20(11.10) + 40.20(11.60) + 14.30(7.60) + 5.40(23.80) = 1149.74$$

$$\text{Factor D : } 40.20(5.60) + 40.20(8.90) + 14.30(16.30) + 5.40(11.30) = 877.01$$

Table 9.
The factors and weights with respect to criterion 4, risk management (28 comparisons)

Criteria	A	B	C	D	E	F	G	H	Priority vector (%)
A	1.00	2.00	1.00	3.00	7.00	5.00	3.00	7.00	27.40
B	1/2	1.00	1.00	1.00	2.00	5.00	1.00	3.00	13.60
C	1.00	1.00	1.00	3.00	7.00	5.00	3.00	3.00	23.80
D	1/3	1.00	1/3	1.00	2.00	5.00	1.00	3.00	11.30
E	1/7	1/2	1/7	1/2	1.00	5.00	3.00	1.00	8.30
F	1/5	1/5	1/5	1/5	1/5	1.00	1.00	2.00	4.20
G	1/3	1.00	1/5	1.00	1/3	1.00	1.00	1.00	6.80
H	1/7	1/3	1/3	1/3	1.00	1/2	1.00	1.00	4.70
Sum	3.65	7.03	4.20	10.03	20.53	27.50	14.00	22.00	

$$\text{Factor E} : 40.20(10.50) + 40.20(6.10) + 14.30(8.90) + 5.40(8.30) = 839.41$$

$$\text{Factor F} : 40.20(10.20) + 40.20(8.90) + 14.30(10.20) + 5.40(4.20) = 936.36$$

$$\text{Factor G} : 40.20(5.50) + 40.20(6.30) + 14.30(6.10) + 5.40(6.90) = 598.85$$

$$\text{Factor H} : 40.20(6.20) + 40.20(7.80) + 14.30(4.40) + 5.40(4.70) = 651.10$$

Table 10 and Figure 4 show the overall weight computed from the adjusted weight of the criteria for the eight factors.

Figure 6 shows the comparison of the overall impact of the eight factors (i.e. the eight forms of cybercrime) considered on the organisation’s goal via the sub-objectives. Hence, the four most critical factors, which represent the forms of highest impact on the goal in the order of ranking are in this study: phishing, spying, malware and online theft. Hence, to ensure effective mitigation of cybercrime, the findings of such a calculation will enable the

Coded factors	Uncoded factor	Overall weight	Overall weight (%)
A	Phishing	3,736.79	37.3679
B	Spying	1,219.23	12.1923
C	Malware	1,149.74	11.4974
D	Data theft	877.01	8.7701
E	Spam e-mail	839.41	8.3941
F	Online theft	936.36	9.3636
G	Hacking	598.85	5.9885
H	Skimming	651.10	6.5110
Sum		9,998.49	99.9849

Table 10. The overall weight for the material selection of eight forms of cybercrime via the four sub-objectives on the overall goal

Source: Own computation

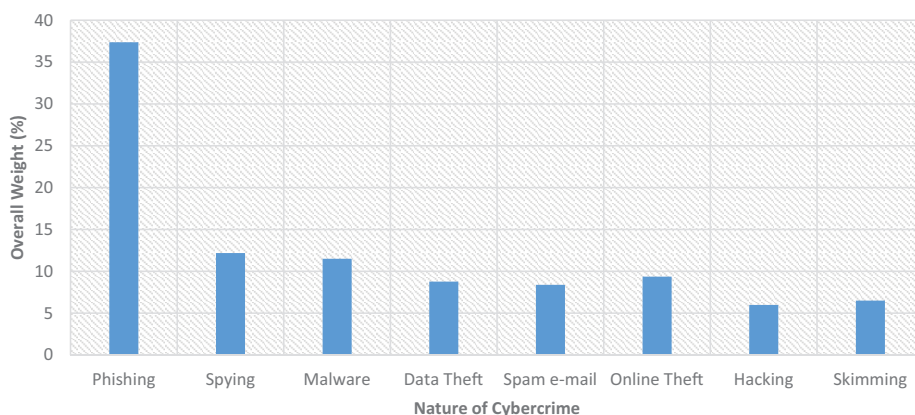


Figure 6. Overall weight of the considered eight forms of cybercrime with respect to the organisation’s objective via the four sub-objectives

Source: Own estimation

management to first understand the impact of cybercrime on its objectives – and therefore, assist in the development of sustainable solutions and effective allocation of resources for cybercrime mitigation.

The Pareto distribution diagram was used for visualising the ranking of the overall weights obtained from the AHP decision model in descending order (order of severity). The left vertical axis is the per cent weight of cybercrime if it occurs while the right vertical axis represents the cumulative percentages over the different forms of cybercrime. The cumulative line at the centre is used for determining the cumulative importance of the criteria with respect to the overall objective. The steepness of the cumulative line indicates how some forms of cybercrime have significantly more impact on the organisation’s goals than others (Figure 7). Using the Pareto distribution diagram analysis for the results obtained from the AHP decision model, the following overall weights were obtained for the different natures of cybercrime considered in this study: phishing (37.37%), spying (12.19%), malware (11.50%), data theft (8.77%), spam e-mail (8.39%), online theft (9.36%), hacking (5.99%), skimming (6.51%). Overall, in the case of occurrence factor A (phishing) has the highest overall weight followed by factor B (spying) and factor C (malware) with the least impact resulting from factor O (hacking).

5. Concluding remarks

The purpose of this study was to use a decision support model based on the AHP and PA for ranking the impact of different kinds of cybercrime in organisations in the financial sector to support decisions on cybercrime mitigation. This was achieved through the examination of the forms of cybercrime from the literature, followed by the identification of possible organisational goals to stem the tide of cybercrime, which form the criteria for the two steps. The prevalent forms of cybercrime in the financial sector were identified from a literature survey. From a structured questionnaire to the staff of 17 licensed banks in South Africa in charge of management, administration and operations, the perceived effect of cybercrime was highest on the organisation’s profitability and goodwill, followed by customers’ satisfaction and risk management. Based on these results, a framework using the AHP and PA was developed for the analysis of some identified forms of cybercrime in relation to the identified organisation’s goals. The novelty of this work lies in the combination of the AHP and PA to assist in solving a

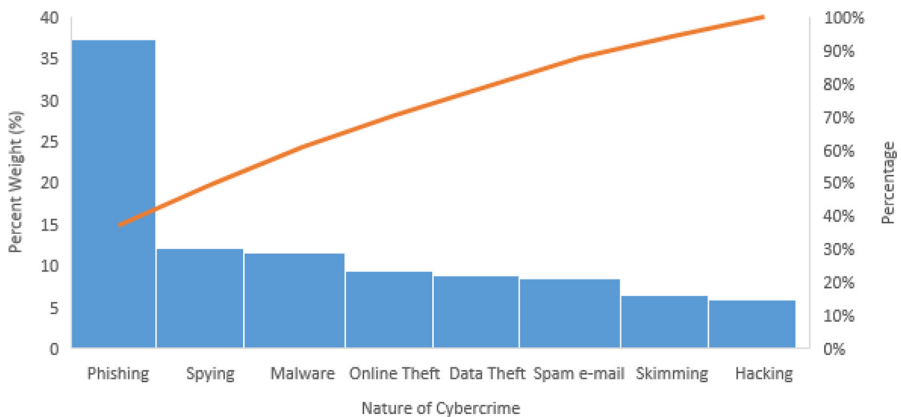


Figure 7.
Pareto distribution diagram for the nature of cybercrime occurrences

Source: Own estimation

multi-criteria decision problem relating to the prevalence of cybercrime. This study demonstrated the use of AHP and PA as a scientific means for an organisation to assess the impact of different forms of cybercrime on the target system. Starting from the pairwise comparison of the cybercrime mitigation goals and of the different forms of cybercrime, it develops a framework to determine the overall impact of each kind of cybercrime on the organisational goal. Hence, effectively, it transforms the multi-criteria decision problem into an equivalent one-dimensional one that only refers to the overall organisational target. Using an example, this study then shows how the eight most critical forms of cybercrime (according to the literature review: phishing, spying, malware, online theft, spam e-mail, data theft, hacking and skimming) may impact on the organisation's objectives such as organisation's profitability, goodwill, customers' satisfaction and risk management. Hence, this work provides a decision support framework for organisational management in the quest to explore the impact of cyber fraud. This provides a basis for the identification of the nature of cybercrime in the organisation and to decide where preventing/mitigation action promises to deliver the most effect with respect to the organisational goal.

Future works can consider the identification of other forms of cybercrime and the use of primary or secondary data to further validate the developed framework.

References

- Agrawal, S. (2016), "Cyber crime in banking sector", *Udgam Vigyati*, Vol. 3, pp. 1-19.
- Ajayi, E.F.G. (2016), "Challenges to enforcement of cyber-crimes laws and policy", *Journal of Internet and Information Systems*, Vol. 6 No. 1, pp. 1253-1271.
- Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2020a), "Analysis of cyber-crime effects on the banking sector using balance score card: a survey of literature", *Journal of Financial Crime*, Vol. 27 No. 3, pp. 945-958.
- Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2020b), "An innovative approach in combating economic crime using forensic accounting techniques", *Journal of Financial Crime*, Vol. 27 No. 4, pp. 1253-1271.
- Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M. (2021), "The integration of forensic accounting and the management control system as tools for combating cyberfraud", *Academy of Accounting and Financial Studies Journal*, Vol. 25 No. 2, pp. 1-13.
- Ali, L., Ali, F., Surendran, P. and Thomas, B. (2017), "The effects of cyber threats on customer's behaviour in e-banking services", *International Journal of e-Education, e-Business, e-Management and e-Learning*, Vol. 7 No. 1, pp. 70-78.
- American Institute of Certified Public Accountants (AICPA) (2017), "Top cybercrimes white paper. How CPAS can protect themselves and their clients", available at: www.aicpa.org/InterestAreas/InformatonTechnology/Resources/Privacy/CyberSecurity (accessed 2 February 2021).
- Balan, S., Otto, J., Minasian, E. and Aryal, A. (2017), "Data analysis of cybercrimes in businesses", *Information Technology and Management Science*, Vol. 20 No. 1, pp. 64-68.
- Bamrara, A., Singh, G. and Bhatt, M. (2013), "Cyber attacks and defense strategies in India: an empirical assessment of banking sector", *International Journal of Cyber Criminology*, Vol. 7 No. 1, pp. 49-61.
- Boateng, E.O. and Amanor, P.M. (2014), "Phishing, Smishing and Vishing: an assessment of threats against mobile devices", *Journal of Emerging Trends in Computing and Information Sciences*, Vol. 5 No. 4, pp. 297-307.
- Broadhurst, R., Grabosky, P., Alazab, M. and Chon, S. (2014), "Organizations and cybercrime: an analysis of the nature of groups engaged in cyber crime", *International Journal of Cyber Criminology*, Vol. 8 No. 1, pp. 1-20.

- Business Ghana (2018), "Bank of Ghana launches cyber security directive for financial institutions", available at: www.businessghana.com/site/news/business/175019/Bank-of-Ghana-launches-Cyber-Security-Directive-for-Financial-Institutions (accessed 2 February 2021).
- Centre for Strategic and International Studies (CSIS) (2014), *Net Losses: Estimating the Global Cost of Cybercrime. Technical Report*, Centre for Strategic and International Studies, Washington, DC.
- Ch, R., Gadekallu, T.R., Abidi, M.H. and Al-Ahmari, A. (2020), "Computational system to classify cyber crime offenses using machine learning", *Sustainability*, Vol. 12 No. 10, pp. 1-16.
- Chaudhary, G.K. (2014), "Development review on phishing: a computer security threat", *International Journal of Advance Research in Computer Science and Management Studies*, Vol. 29 No. 8, pp. 55-64.
- Coyle, G. (2004), *The Analytic Hierarchy Processes*, Pearson Educational, New York, NY.
- Dzomira, S. (2014), "Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe", *Risk Governance and Control: financial Markets and Institutions*, Vol. 4 No. 2, pp. 16-26.
- Detica Limited (2011), *The Cost of Cybercrime*, United Kingdom, pp. 1-32.
- Geeta, D.V. (2011), "Online identity theft-an indian perspective", *Journal of Financial Crime*, Vol. 18 No. 3, pp. 235-246.
- Goel, S. and Shawky, H.A. (2009), "Estimating the market impact of security breach announcements on the firm values", *Information and Management*, Vol. 46 No. 7, pp. 404-410.
- Gordon, L.A., Loeb, M.P. and Sohail, T. (2003), "A framework for using insurance for cyber-risk management", *Communications of the ACM*, Vol. 46 No. 3, pp. 81-85.
- Grosfeld-Nir, A., Ronen, B. and Kozlovsky, N. (2007), "The Pareto managerial principle: when does it apply?", *International Journal of Production Research*, Vol. 45 No. 10, pp. 2317-2325.
- Hinde, S. (2003), "Computer security: mapping the future", *Computers and Security*, Vol. 22 No. 8, pp. 664-669.
- Hedayati, A. (2012), "An analysis of identity theft: motives, related frauds, techniques and prevention", *Journal of Law and Conflict Resolution*, Vol. 4 No. 1, pp. 1-12.
- Information Security Institute (2013), Report, Technical University of Denmark (DTU), Diplomvej 381, DK-2800 Kgs. Lyngby, Denmark.
- Jayant, A. (2011), "An application of analytic network process to evaluate supply chain logistics strategies", *International J. of Analytic Hierarchy Process*, Vol. 4 No. 1, pp. 149-163.
- KPMG (2017), "Cybercrime survey report: insights and perspective", available at: www.kpmg.com (accessed 5 September 2020).
- Kraemer-Mbula, E., Tang, P. and Rush, H. (2013), "The cybercrime ecosystem: online innovation in the shadows?", *Technological Forecasting and Social Change*, Vol. 80 No. 3, pp. 541-555.
- Kshetri, N. (2019), "Cybercrime and cybersecurity in Africa", *Journal of Global Information Technology Management*, Vol. 22 No. 2, pp. 77-81.
- Kumudha, S. and Rajan, A. (2018), "A critical analysis of cyber phishing and its impact on banking sector", *International Journal of Pure and Applied Mathematics*, Vol. 119 No. 17, pp. 1557-1569.
- Lagazio, M., Sherif, N. and Cushman, M. (2014), "A multi-level approach to understanding the impact of cybercrime on the financial sector", *Computers and Security*, Vol. 45, pp. 58-74.
- McGuire, M. and Dowling, S. (2013), "Cybercrime: a review of the evidence, summary of key findings and implications", *Home Office Research Report*, Vol. 75, pp. 1-29. ISBN: 978-1-78246-245-3.
- Malik, M.S. and Islam, U. (2019), "Cybercrime: an emerging threat to the banking sector of Pakistan", *Journal of Financial Crime*, Vol. 26 No. 1, pp. 50-60.
- Martin, N. and Rice, J. (2011), "Cybercrime: understanding and addressing the concerns of stakeholders", *Computers and Security*, Vol. 30 No. 8, pp. 803-814.

- Mugari, I., Gona, S., Maunga, M. and Chiyambiro, R. (2016), "Cybercrime – the emerging threat to the financial services sector in Zimbabwe", *Mediterranean Journal of Social Sciences*, Vol. 7 No. 3, pp. 135-143.
- Njeru, P.W. and Gaitho, V. (2019), "Investigating extent to which cybercrime influences performance of commercial banks in Kenya", *International Journal of Economics, Commerce and Management*, VII, No. 8, pp. 489-514.
- Odu, G.O. (2019), "Weighting methods for multi-criteria decision making technique", *Journal of Applied Sciences and Environmental Management*, Vol. 23 No. 8, pp. 1449-1457.
- Okeshola, F.B. and Adeta, A.K. (2013), "The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna state, Nigeria", *American International Journal of Contemporary Research*, Vol. 3 No. 9, pp. 98-114.
- Okutan, A. and Çebi, Y. (2019), "A framework for cyber crime investigation", *Procedia Computer Science*, Vol. 158, pp. 287-294.
- Omodunbi, B.A., Odiase, P.O., Olaniyan, O.M. and Esan, A.O. (2016), "Cybercrimes in Nigeria: analysis, detection and prevention", *FUOYE Journal of Engineering and Technology*, Vol. 1 No. 1, pp. 37-42.
- Rao, H.S. (2019), "Cyber crime in banking sector", *International Journal of Research - Granthaalayah*, Vol. 7 No. 1, pp. 148-161.
- Rezk, A., Barakat, S. and Saleh, H. (2017), "The impact of cyber crime on E-Commerce", *International Journal of Intelligent Computing and Information Sciences*, Vol. 17 No. 3, pp. 85-96.
- Saaty, T.L. (1977), "A scaling method for priorities in hierarchical structures", *Journal of Mathematical Psychology*, Vol. 15 No. 3, pp. 234-281.
- Saaty, T.L. (1980), *The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation*, McGraw-Hill: New York, NY.
- Saaty, T.L. (2005), *Theory and Applications of the Analytic Network Process: Decision Making with Benefits, Opportunities, Costs, and Risks*, RWS Publications, Pittsburgh.
- Saaty, T.L. (2008), "Decision making with the analytic hierarchy process", *International Journal of Services Sciences*, Vol. 1 No. 1, pp. 83-98.
- Saini, H., Rao, Y.S. and Panda, T.C. (2012), "Cyber-crimes and their impacts: a review", *International Journal of Engineering Research and Applications*, Vol. 2 No. 2, pp. 202-209.
- Serianu (2016), "Africa cyber security report", available at: www.cybersecurityhub.gov.za/images/docs/AfricaCyberSecurityReport20161-002.pdf (accessed 5 September 2020).
- South African Banking Risk Information Centre (SABRIC) (2018), "Digital banking statistics", available at: www.icfp.co.za/article/sabric-digital-banking-crime-statistics (accessed 5 March 2021).
- Subramanian, N. and Ramanathan, R. (2012), "A review of applications of analytic hierarchy process in operations management", *International Journal of Production Economics*, Vol. 138 No. 2, pp. 215-241.
- Symantec Report (2016), "Cybercrime and cyber security: trends in Africa", available at: www.symantec.com/security-centre/threat-report (accessed 5 March 2021).
- Symantec Report (2018), "Symantec internet security threat report 2018: the top takeaways", available at: <https://thycotic.com/company/blog/2018/04/17/symantec-internet-security-threat-report-2018/> (accessed 5 March 2021).
- Sonepat, R. and Sonepat, S. (2014), "Analysis on credit card fraud detection methods", *International Journal of Computer Trends and Technology*, Vol. 8 No. 1, p. 45.
- Tan Harry, S.K. (2002), "E-fraud; current trends and international developments", *Journal of Financial Crime*, Vol. 9 No. 4, pp. 347-354.
- Tiwari, S., Bhalla, A. and Rawat, R. (2016), "Cybercrime and security", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 6 No. 4, pp. 46-52.

- UK Finance (2018), “Staying ahead of cybercrime”, UK Finance, 1 Angel Court London, EC2R 7HJ United Kingdom, pp. 1-16, available at: www.ukfnance.org.uk (accessed 20 January 2020).
- UK Finance (2020), “Overview of payment industry fraud”, available at: www.ukfnance.org.uk UK Finance, 1 Angel Court London, EC2R 7HJ United Kingdom (accessed 5 September 2020).
- Uma, M. and Padmavathi, G. (2013), “A survey on various cyber-attacks and their classification”, *International Journal of Network Security*, Vol. 15 No. 1, pp. 390-396.
- UN (2013), “United Nations Office on drug crime 2013”, *Comprehensive Study on Cybercrime*, United Nations, pp. 1-320, available at: www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed 15 August 2020).
- United Nations (2019), “Cybercrime, united nations office on drugs and crime, Austria”, available at: www.unodc.org (accessed 5 March 2021).
- UNCTAD (2015), “UNCTAD information economy report”, available at: www.unctad.org (accessed 5 March 2021).
- Uppal, D., Mehra, V. and Verma, V. (2014), “Basic survey on malware analysis, tools and techniques”, *International Journal on Computational Science and Applications*, Vol. 4 No. 1, pp. 103-112.
- Vargas, R.V. (2010), “Using the analytic hierarchy process (AHP) to select and prioritize projects in a portfolio”, Paper presented at PMI® Global Congress 2010 – North America, Washington, DC, Project Management Institute, Newtown Square, PA.

Further reading

- UK Finance (2019), “The cost of economic crime in the UK”, available at: www.ukfnance.org.uk UK Finance, 1 Angel Court London, EC2R 7HJ United Kingdom (accessed 5 March 2021).
- United Nations Office on Drug Crime (2013), *Comprehensive Study on Cybercrime*, United Nations UK.

Corresponding author

Oluwatoyin Esther Akinbowale can be contacted at: oluwatee01@gmail.com

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgroupublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com