Strathmore University

Law School

Incentivizing Transparency: Considering a limited liability clause as a motivation for reporting cybercrimes in Kenya

Submitted in partial fulfillment of the requirements of the Bachelor of Laws Degree, Strathmore University Law School

By

[Waititu Gorretti Wairimu]

[136934]

Prepared under the supervision of

[Mr. Cecil Abungu]

February 2024

Word count: 15,729

Contents

Acknowledgments

I would like to express my sincere gratitude Mr. Cecil Abungu, my supervisor, for his guidance and support throughout the course of this subject. His insights and constructive feedback have been instrumental in shaping the quality of my work.

I would also like to extend my appreciation to my family for their unwavering understanding and support during the challenging periods of this experience. Their encouragement throughout the project is greatly appreciated.

Lastly, I am sincerely grateful to my close friends who patiently endured my continuous discussions about this project throughout the entire year.

To all of you, thank you.

Dedication

To all who strive to safeguard our digital world.

Declaration

I, **WAITITU GORRETTI WAIRIMU,** do hereby declare that this research is my original work and that to the best of my knowledge and belief; it has not been previously, in its entirety or in part, been submitted to any other university for a degree or diploma. Other works cited or referred to are accordingly acknowledged.

Signed: ……..

Date: 15 February 2024

This dissertation has been submitted for examination with my approval as University Supervisor.

Signed: ……

[Cecil Abungu]

Abstract

Cyber-attacks pose significant threats to individuals, businesses and national security, necessitating robust cyber security measures to mitigate risks and safeguard critical infrastructure. While there has been a substantial surge in cyber-crime in Kenya, individuals and companies, especially, are reluctant to implement cyber security measures such as cyber-incident reporting. At the same time, there is insufficiency in the implemented legislation governing cyber security and cyber-crime. Through legal analysis, this research underscores the significance of proactive legislative measures in addressing cyber security concerns. By mitigating the fear of punitive measure and fostering a culture of transparency, a limited liability clause can incentivize organizations to report cyber threats promptly, thereby facilitating proactive responses and improving the country's cyber security posture.

List of Abbreviations

EUT	Expected Utility Theory
DDOS	Distributed Denial of Service
SMEs	Small and medium sized enterprises
NC4	National Computer and Cybercrimes Coordination Committee
CMCA	Computer Misuse and Cybercrimes Act
National KE-CIRT/CC	National Kenya Computer Incident Response Team Coordination Centre

List of Cases

Kenya

Bloggers Association of Kenya (BAKE) v Attorney General and 3 others [2020] eKLR.

List of Legal Instruments

Computer Misuse and Cybercrime Act (2018)

The Cyber Incident Reporting for Critical Infrastructure Act (2022).

The Cyber security Information Sharing Act (2015).

1.0 INTRODUCTION

1.1 BACKGROUND

While digitalization influences rapid advances in technology, cyber threat actors continue to adopt sophisticated cyber-attack techniques.[1] Cyber security has been an emerging issue in Kenya.[2] The statistics indicate that the number of cyber threats detected in Kenya has significantly increased in the last five years.[3] As more individuals utilize financial technology, banks have emerged as the number one target of cybercrime.[4]

Numerous legislative and policy efforts related to cyber security are being started and supported by the Kenyan government.[5] Some of the key legal regulatory frameworks include; Kenya Information and Communications Act 1998 and the Computer Misuse and Cybercrimes Act 2018 among others.[6] The Computer Misuse and Cybercrimes Act 2018, which was passed by the Kenyan government, serves as the country's main framework for the defense of vital information infrastructure and the regulation of cybercrime.[7]

Private sector cyber security is still far from adequate.[8] Assumptions are being made by some that the private sector will suffer the consequences if it fails to protect itself from cyber-attacks.[9] Contrary to what is sometimes claimed in public debate, there is very little difference between the public and private sectors.[10] With this, the reliability of cyber security in the public sector is impossible not unless there is strong or heightened cyber security measures in the private sector.[11] This is because supply and maintenance of much of the technology and critical

[1] Communications Authority Kenya, *Cyber security report* 2022, 8.
[2] Serianu, *Kenya cyber security report*, 2015, 22.
[3] Communications Authority Kenya, *Cyber security report* 2022, *6.*
[4] Obura F, 'Kenya worst hit in East Africa by cybercrime,' The Standard, 2017, https://www.standardmedia.co.ke/article/2001235820/kenya-worst-hit-in-eastafrica-by-cyber-crime 2017.
[5] National computer and cybercrimes co-ordination committee, *Kenya Cyber security strategy*, 2022, 1.
[6] National computer and cybercrimes co-ordination committee, *Kenya Cyber security strategy*, 2022, 1.
[7] National computer and cybercrimes co-ordination committee, *Kenya Cyber security strategy*, 2022, 2.
[8] Amitai E, 'The private sector: a reluctant partner in cyber security' *Georgetown Journal of International Affairs, 2014, International Engagement on Cyber IV*, 2014, 74, https://www.jstor.org/stable/43773650 on 26 December 2022.
[9] Amitai E, 'The private sector: a reluctant partner in cyber security' *Georgetown Journal of International Affairs, 2014, International Engagement on Cyber IV*, 2014, 74, https://www.jstor.org/stable/43773650 on 26 December 2022.
[10] Amitai E, 'The bankruptcy of Liberalism and Conservatism' 128 *Political science quarterly* 1, 2013, 43.
[11] Healey J, 'Who's in control: balance in cyber's public-private sector partnerships' 18(3) *Georgetown Journal of International affairs*, 2017, 126.

infrastructure used by the government is mandated to the private sector.[12] The public sector also awards some contracts to the private sector for instance logistical support.[13] Thus, it is crucially important to have robust cyber security measures in the private sector.

Among other cyber security measures cyber Incident Reporting is one of the cyber security measures which ought to be adopted. The overarching law, the Computer Misuse and Cybercrime Act provides for reporting of cyber-attacks, intrusions or disruptions to the National Computer and Cybercrimes Co-ordination Committee for resolution.[14] It also imposes a penalty for contravention of the said section.[15]

Regulators require companies to disclose security incidents such as data breaches. Private companies, however, often hesitate to report cyber-attacks because it is difficult to attribute liability, leading them to the question whether it is worth the effort.[16] They fear negative consequences such as damage to their reputation, loss of consumer trust, and potential lawsuits hence they end up choosing to negotiate with cybercriminals to avoid such damage.[17] There are also concerns about the time and the financial resources required to pursue legal action and the belief that it is unlikely to result in the recovery of losses.[18] In most cases, the incident may not be considered significant enough to justify involving the authorities, and the company may prefer to handle it internally.[19] Furthermore, some companies fear that involving the authorities may cause further disruption to their operations as they investigate the incident.[20]

[12] Amitai E, 'The private sector: a reluctant partner in cyber security' *Georgetown Journal of International Affairs, 2014, International Engagement on Cyber IV,* 2014, 74, https://www.jstor.org/stable/43773650 on 26 December 2022.
[13] Amitai E, 'The private sector: a reluctant partner in cyber security' *Georgetown Journal of International Affairs, 2014, International Engagement on Cyber IV,* 2014, 74, https://www.jstor.org/stable/43773650 on 26 December 2022.
[14] Section 40(1), *Computer Misuse and Cybercrime Act* (2018).
[15] Section 40(4), *Computer Misuse and Cybercrime Act* (2018).
[16] Swinhoe D, 'Why businesses don't report cybercrimes to law enforcement' Computer Security Online, 20 May 2019 https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html on 20 February 2023.
[17] James K, 'How legal loopholes are hurting Kenya's cybercrime fight' Business Daily Africa on 24 February 2022 How legal loopholes are hurting Kenya's cybercrime fight - Business Daily (businessdailyafrica.com) on 20 August 2023.
[18] https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/reporting-cybercrime.html on 20 February 2023.
[19] Swinhoe D, 'Why businesses don't report cybercrimes to law enforcement' Computer Security Online, 20 May 2019 https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html on 20 February 2023.
[20] https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/reporting-cybercrime.html on 20 February 2023.

On the flip side, reporting such incidents can increase the likelihood of identifying and capturing the perpetrator, which can protect businesses from further harm, particularly in cases of cyber-extortion.[21] However, failing to report such incidents can make it difficult to comprehend the nature and scope of an attack which can hinder the development of a successful containment strategy.[22] Regrettably, in Kenya, cybercrime is widely prevalent, but law enforcement officials receive minimal reports of these offenses, resulting in significant underreporting.[23]

A limited liability clause excludes liability towards companies after reporting cyber-attacks. Having a limited liability clause incorporated into the current legal framework can incentivize reporting through reducing the possible negative consequences for companies that come forward with information on such crimes.[24] However having unlimited liability can make it unlikely that companies will shy away from reporting cybercrimes due to heightened financial risks such as financial loss as a result of data breach, reputational damage, legal consequences such as lawsuits and other negative business repercussions.[25] Similarly, unlimited liability may leave companies exposed to extensive legal liability hence making reporting cybercrimes a risky endeavor.

1.2 PROBLEM STATEMENT

Section 40 of the Computer Misuse and Cybercrimes Act outlines the obligation to report cyber-attacks in both public and private domains, and failure to comply with this requirement carries a penalty. This current law falls short in addressing the issue of cybercrime reporting, given that organizations may be inclined to conceal their vulnerabilities to protect their image. In fact, the provision of the law may exacerbate this issue by penalizing companies that do not report such attacks. Clearly, this is not a sufficient incentive. Consequently, this project aims to explore whether an amendment of section 40 of the 2018 Computer Misuse and Cybercrimes Act to include a limited liability clause could better motivate private companies in Kenya who are victims of cyber-attacks to take responsibility by reporting such incidents.

---

[21] Cierra P, 'Silent threat; FBI warns against trend of not reporting cyber attacks' WTHR, 11 August 2022 https://www.wthr.com/article/news/investigations/13-investigates/silent-threat-fbi-warns-against-trend-of-not-reporting-cyberattacks-ransomware/531-6cbee4c4-c23a-4d13-af20-ffb2fe6aa3a4 on 2 January 2023.

[22] Frankline S, 'This is why Kenyan firms are vulnerable to cyber-attacks' The Standard, 23 May 2017 https://www.standardmedia.co.ke/business/sci-tech/article/2001240803/this-is-why-kenyan-firms-are-vulnerable-to-cyber-attacks on 13 January 2023.

[23] Bloggers Association of Kenya (BAKE) v Attorney General and 3 others [2020] eKLR.

[24] https://www.fsb.org/wp-content/uploads/FSSCC-1.pdf on 20 August 2023.

[25] Cybersecurity and Infrastructure Security Agency, *Enhancing resilience through cyber incident data sharing and analysis*, 2015, 7.

1.3 RESEARCH OBJECTIVES

1. To determine the methods employed by cybercriminals and assess the scope and severity of the impact of cybercrime.
2. To evaluate the importance of reporting in promoting transparency and accountability and to assess the current legal framework for reporting and its limitations.
3. To explore the content and implications of a limited liability clause and assess its potential benefits in promoting reporting behavior in the private sector.

1.4 RESEARCH QUESTIONS

1. What are the mechanics of cybercrime and the extent of the damage it can cause?
2. What is the significance of reporting in ensuring transparency and accountability, and what is the current legal framework for reporting and its limitations?
3. What is the content and significance of a limited liability clause, and how can its implementation effectively encourage reporting behavior within the private sector?

1.6 JUSTIFICATION

Cybercrime is not only a national problem but also a global one. Despite being required to report cyber-attacks, private companies are concealing such incidents and absorbing the resulting losses. Conducting this study is beneficial in many ways. It can foster collaboration between policymakers and private companies, promoting the exchange of information and expertise hence resulting in a more effective response to cybercrime. This research can also encourage private entities to enhance their cyber security practices by offering incentives, benefiting both public and private sector organizations. Furthermore, this study can inform the creation of guidelines and standards by entities to strengthen their cyber security. Authorities can also benefit from the study's findings as they can identify trends, patterns, and emerging threats, ultimately improving their ability to prevent and respond to cyber-attacks.

1.7 THEORETICAL FRAMEWORK

The Expected Utility Theory (EUT) was formulated by Daniel Bernoulli in the 18th Century. The theory has been used in economics to explain various phenomena such as purchasing

insurance and the relationship between spending and saving.[26] This theory has also been applied as a normative theory in decision analysis, particularly in situations of uncertainty.[27]

Essentially, the theory proposes that when making decisions involving risky or uncertain prospects, the decision maker compares the utilities of each option; utility here refers to the desirability or value of the outcome.[28] The decision maker chooses the option that maximizes their expected utility, based on the rational decision making principles or axioms that take into account individual preferences and even risk aversion.[29] The theory is based on axioms, such as transivity, independence, completeness and substitutability, which govern rational behavior under uncertainty.[30] Specifically, the expected utility of an act is calculated as a weighted average of the utilities of each possible outcome, with each outcome weighted according to its probability, and the act with the highest expected utility (gainful) is considered the best option.[31]

The theory of expected utility has been subject to criticism, with various studies demonstrating that many of the axioms that underpin the theory can be violated under certain conditions.[32] March and Simon have highlighted that the process of calculating expected utilities requires an extremely complex understanding of the available options, potential outcomes, and the values of those outcomes, which may be difficult or impossible for individuals to accurately assess.[33] Nonetheless, the theory assumes that individuals have access to complete and accurate information about the probabilities involved, whereas in reality, information is often limited and imperfect.[34] As a result, it is unclear whether it is possible to truly maximize utility in practice.

[26] Davis J, 'Expected Utility Theory' in Mongin P (ed) *The handbook of economic methodology*, Edward Elgar Publishing, Cheltenham England,1998, 1.
[27] Davis J, 'Expected Utility Theory', 8.
[28] Friedman M and Savage L, 'The Utility analysis of choices involving risks' 56(4) *Journal of Political Economy*, 1948, 279.
[29] Tversky A, 'Additivity analysis of risky choices' 75(1) *Journal of Experimental Psychology*, 1967, 27.
[30] Tversky A, 'A critique of expected utility theory: descriptive and normative considerations' 9(1) *Erkenntnis Journal*, 1975, 163.
[31] Stanford Encyclopedia of Philosophy, fall 2019 edition.
[32] Harrison G, 'Expected utility theory and the experimentalists' *Physica-Verlag HD*, 1994, 43 https://link.springer.com/chapter/10.1007/978-3-642-51179-0_ on 3 March 2023.
[33] March J and Simon H, 'Organizations' John Wiley and Sons, New York, 1958, 54.
[34] Mosteller F and Nogee P, 'An experimental measurement of utility' 59(5) *Journal of Political Economy*, 1951, 371.

In addition, when viewed from a standard perspective, utility theory is considered inadequate as a descriptive model of individual choice behavior.[35] Therefore, a more comprehensive analysis of rational decision-making under conditions of risk should take into account the interpretation problem as well as the issue of values and their legitimacy.[36] Such an analysis is more likely to be explanatory or therapeutic rather than normative in nature.[37]

Despite the criticisms leveled against it, the normative expected utility theory has found widespread use in variety of fields including economics, public policy, ethics, psychology and even epistemology as a means of tackling practical questions.[38] Incorporation of the limited liability clause increases the utility hence this increases the possibility of entities making informed decisions by reporting cyber-crime thereby maximizing their expected utility. Therefore, this theory may be used to inform the incorporation of a limited liability clause to enhance the effectiveness of the Computer Misuse and Cybercrimes Act of 2018.

1.8 LITERATURE REVIEW

The existing research in Kenya exists around cyber security in the developing e-commerce context. Technology has become an essential part of many business activities, but its widespread use also creates a vulnerability that can compromise the confidentiality and even integrity; technology has opened up a tunnel of attacks.[39] According to Peterson Obara, Gladys Monchari and Christopher Jilo, Internet usage in Kenya has grown rapidly resulting in the development of Internet Service Providers consequently Internet access points.[40] Small Medium Enterprises have fallen victims of cyber-attacks leading to massive loss of businesses due to lack of capabilities in implementation of effective information security measures as compared to large organizations.[41] It has been discovered that Cybercrime is prevalent in Nairobi but it is largely unreported due to

[35] Tversky A, 'A critique of expected utility theory: descriptive and normative considerations, 173.
[36] Tversky A, 'The intrasivity of preferences' 76(1) *Psychological Review*, 1969, 31.
[37] Tversky A, 'A critique of expected utility theory: descriptive and normative considerations, 173.
[38] Stanford Encyclopedia of Philosophy, Fall 2019 Edition.
[39] Wekundah R, 'The effects of cyber-crime on e-commerce: a model for SMEs in Kenya' published LLM Thesis, University of Nairobi, Nairobi, 2015, 1.
[40] Ogutu P, Monchari G and Jilo C, 'Effects of cybercrime on state security: Types, impact and mitigations with fibre-optic deployment in Kenya' 2011(1) *Journal of Information Assurance & Cyber security*, 2011, 4.
[41] Muhati E, 'Factors affecting cyber security in Kenya- A case of Small Medium Enterprises' unpublished LLM Thesis, Strathmore University, Nairobi, 2018, 3.

unavailability of sensitization programs and inefficient e-laws.[42] ISPs in collaboration with the Criminal Investigation Department and the Communications Commission of Kenya have established and are implementing cyber security measures in order to counter the growing cybercrimes such as spamming and even use of malicious code such as viruses or Trojans.[43]

1.8.1 Corporate Responsibility in reporting cybercrime as a cyber-security measure

Corporate security encompasses directors who address the element of risk management and secure the business from a wide range or hazards such as cyber-attacks, natural disaster, espionage and supply-chain disruption.[44] National security capabilities are not essentially a factor in business planning.[45] As cyber-attacks and irregular warfare by proxies are most likely to be directed towards a corporate's assets, business owners should be considered central to the country's security.[46] Corporations are making valiant efforts to protect themselves from offline and online attacks for commercial reasons.[47] They do not consider such attacks and their response as elements of national security whereas[48] the central interest of the nation is security as it is a prerequisite for a state's orderly development.[49] However, it is worth noting that economic security, an engine room for a strong economy, is a key element of national security as such attacks have a potential to weaken national resilience.[50]

[42] Ogutu P et al, 'Effects of cybercrime on state security: Types, impact and mitigations with fibre-optic deployment in Kenya' 2011(1) *Journal of Information Assurance & Cyber security*, 2011, 6.
[43] Ogutu P et al, 'Effects of cybercrime on state security: Types, impact and mitigations with fibre-optic deployment in Kenya' 2011(1) *Journal of Information Assurance & Cyber security*, 2011, 10.
[44] Bergin A, 'All in a day's work: business and Australian disaster management', 12(1) Journal of Policing, Intelligence and Counter Terrorism, 2017, 1.
[45] Bergin A, Williams D and Wilde R, 'From board to situation room: why corporate security is national security' *Australian Strategic Policy Institute*, 2019, 6 https://www.jstor.org/stable/resrep23021 on 7 March 2023.
[46] Grizold A, 'The concept of national security in the contemporary world' 11(3) *International Journal on World Peace,* 1994, 51.
[47] Bergin A, 'All in a day's work: business and Australian disaster management', 12(1) *Journal of Policing Intelligence and Counter Terrorism*, 2017, 1.
[48] Bergin A, Williams D and Wilde R, 'From board to situation room: why corporate security is national security' *Australian Strategic Policy Institute*, 2019, 6 https://www.jstor.org/stable/resrep23021 on 7 March 2023.
[49] Blanchette J, 'Ideological security as national security' Center for strategic and International Studies, 2020, 2 https://www.jstor.org/stable/resrep27056 on 3 March 2023.
[50] R Shah, 'Protecting critical infrastructure in an era of IT and OT convergence', Policy Brief 18/2019, Canberra, ASPI, 2019 https://www.aspi.org.au/report/protecting-critical-national-infrastructure-era-it-and-ot-convergence on 3 March 2023.

Additionally, Amitai recognizes that the private sector is far from protecting itself from cyber-attacks. Some of them believe that the government may be exaggerating cyber threats.[51] Others regard such measure as unfunded mandates demanding that the government should cover the costs that come with it.[52] They even hold the opinion that through regulations, they are forced to comply hence hindering flexibility of the corporation and the ability to innovate.[53] For such reasons, corporations have been reluctant in adopting strong and effective cyber security measures such as information sharing and reporting cyber threats.[54] They fail to realize that there is little to no difference between the public and private sphere and for there to be a reliable security, there needs to be heightened cyber security measures in the private sector.[55]

Besides it being a legal requirement, reporting is a duty or obligation entrusted upon the corporate world also that extends beyond safeguarding their interests and that of its investors; it also includes protection of the public domain and the nation's security as a whole.

1.8.2 On whether incorporation of the liability protection approach as a way forward will increase cybercrime reporting behavior

Although certain developing technologies like cloud computing may appear to lessen the cyber security risks, other advancing technologies used by criminal organizations or even terrorist groups ensure that technology alone cannot fully eradicate the cyber security risks that businesses encounter.[56] Given the worldwide scope of corporations, it is essential for an international movement toward corporate reporting of cyber-related activities and risks to take place.[57] Chiji, Adewale, Olutola and Bello also admit that restoration of trust between the public

[51] Amitai E, 'Cyber security in the private sector' 28 *Issues in Science and Technology* 1, 2011, 59.
[52] Yadron D, 'Companies wrestle with the cost of cyber security' *The wall street Journal*, 2014 https://www.wsj.com/articles/no-headline-available-1393371844 on 8 March 2023.
[53] Amitai E, 'Cyber security in the private sector' 28 *Issues in Science and Technology* 1, 2011, 59.
[54] Amitai E, 'The private sector: a reluctant partner in cyber security' *Georgetown Journal of International Affairs, 2014, International Engagement on Cyber IV*, 2014, 70, https://www.jstor.org/stable/43773650 on 26 December 2022.
[55] Healey J, 'Who's in Control: Balance in Cyber's Public-Private Sector Partnerships' 18(3) *Georgetown Journal of International affairs*, 2017, 126.
[56] Gordon L, Loeb M and Lucyshyn W, 'Cyber security Investments in the private sector: The Role of Governments' *Georgetown Journal of International Affairs*, 2014, 79 https://www.jstor.org/stable/43773651 on 7 March 2023.
[57] Robinson N, 'Information sharing for Cyber-Security: Evidence from Europe' *Asan Institute for Policy* studies, 2013, 71 https://www.jstor.org/stable/resrep08108 on 7 March 2023.

and criminal justice system which includes the police is critical in order to motivate the members of the community to report cybercriminal activity.[58]

According to Gordon, Loeb and William, the dissemination of information across various entities, including network operators, information systems, hardware and software providers, and intelligence organizations, is critical in preventing, detecting, and responding to cyber-attacks.[59] Therefore, effective cyber security hinges on information sharing. To enhance cyber security, governments should establish and enforce incentives that promote better sharing of information concerning cyber threats and vulnerabilities.[60]

To ensure effective cyber security incentives, the incorporation of information sharing should be a significant component of legislation drafting. Legislators must pay close attention to the factors that facilitate or hinder the sharing of information. The practice is beneficial in numerous ways; for instance, companies can learn from each other's mistakes, enabling them to enhance their cyber security measures.[61] Moreover, if the government can access this information, it offers insight into the level of security of critical infrastructures, providing a foundation for informed long-term policy intervention.[62]

Summarily, companies crave for an incentive to encourage reporting of cybercrimes. Therefore incorporation of a liability protection clause could be successful in many ways such as encouraging reporting, fostering partnerships and even promotion of prevention programs.

[58] Chiji E, Adewale A, Olutola A, Bello P, 'Cyber-related crime in South Africa: extent and perspectives of state's role-players' 31 *Acta Criminilogica: African Journal of Criminology and Victimology* 3, 2018, 102.
[59] Gordon L, Loeb M and Lucyshyn W, 'Cyber security Investments in the private sector: The Role of Governments' *Georgetown Journal of International Affairs*, 2014, 79 https://www.jstor.org/stable/43773651 on 7 March 2023.
[60] Gordon L et al, 'Cyber security Investments in the private sector: The Role of Governments' *Georgetown Journal of International Affairs*, 2014, 79 https://www.jstor.org/stable/43773651 on 7 March 2023.
[61] Robinson N, 'Information sharing for Cyber-Security: Evidence from Europe' *Asan Institute for Policy studies*, 2013, 71 https://www.jstor.org/stable/resrep08108 on 7 March 2023.
[62] Gal-Or E, Ghose A, 'The economic incentives for sharing security information' 16(2) *Information Systems Research*, 2005, 187.

1.8.3 CONTRIBUTION

As previous studies in Kenya have focused on cyber security in the e-commerce sector especial small medium enterprises, this study focuses on the reporting element, a shortcoming towards achieving strong cyber security measures, in the private realm. This study will address the shortcoming in itself, the legal framework as well as providing an idea of liability protection as an incentive to try and curb non-reporting incidents in the country. Nonetheless, this study fits into various fields including cyber security, information technology and even public policy.

In the field of public policy, this study would contribute in the development of regulations, policies and even incentives through understanding the basis of the barriers that hinder cyber incident reporting. The research on this area can also inform the design and growth of more effective incident reporting systems in the field of information technology. It may also provide more insights on how to streamline the reporting process making it user-friendly for private entities. Lastly, in the field of cyber security, this study may shed light on the effectiveness of incident reporting practices, identify the shortcomings in reporting practices and highlight the importance of information sharing in mitigation of cyber risks hence provide assistance in improving incident responses and security practices.

1.9 METHODOLOGY

The nature of research to be adopted will generally be desk-based, qualitative research. Primary sources such as the Computer Misuse and Cybercrimes Act will be utilized to show Kenya's position on transparency in cases of cyber-attacks. Secondary sources such as journal articles, books will also be utilized. Also, both an inductive and deductive method will be used where general lessons will be drawn from studies and the set premises from the objectives with logical reasoning will be used to draw a conclusion respectively.

First, I intend to determine the mechanics employed by cyber criminals while assessing the scope and severity of the impact of such attacks. To determine this, a case study of two specific phenomena will be used hence an inductive method of arriving at the claim will be used. To achieve this journal articles, newspaper articles, reports will be relied on. This is so as to have an in-depth appreciation of the issues that are emerging in the real-life context.

In the second limb of this study, I have the intention of assessing the current legal framework for cyber security; transparency in cyber-attacks and the importance of promoting transparency and accountability. This is with the aim of determining the mandate issued by the law to corporations. A doctrinal analysis will be used through assessing the structure and content of the texts in order to identify and show the gap in law which has consequently led to its ineffectiveness. This will be done through reliance on the relevant statute such as the Computer Misuse and Cybercrimes Act and articles, books for the second part of the objective.

Finally, this study will assess the limitation of liability approach as the way forward and the benefits of its implementation. This will adopt a case study method involving the implementation of the limited liability approach for protection against suits of cybercrime. It will be dominantly relying on sources such as scholarly articles, cases and even books. Through analyzing and drawing general lessons from this study an answer will be arrived at through identification of a solution. Two relevant cases will be identified, discussed and analyzed thematically. This ensures that there is a detailed understanding of the cases for generation of insights into the way forward; a limited liability approach.

1.10 CHAPTER BREAKDOWN

Chapter one lays the foundation of this study. It outlines in detail, the research objectives, research questions, hypothesis, justification, the theoretical framework for the study among others. Chapter two will seek to determine the various methods employed by cyber criminals in executing such attacks. This includes; phishing, social engineering and malware attacks among others. It will go ahead and assess the extent to which the cybercrime occurs; the victims and even the sectors affected. Additionally, it will assess the extent of damage caused by the cybercrime. This may include either financial loss or reputational damage.

Chapter three will carry out an evaluation on the importance of reporting in promotion of transparency and accountability while looking at the potential drawbacks such as risks of privacy. It will also assess the current legal framework for reporting cybercrimes and how it negatively affects reporting practices of private companies.

Chapter four will delve into the conceptual understanding of the limited liability clause and its significance in fostering reporting behavior. The focus will be on how such clauses protect

entities from financial and legal liabilities while encouraging transparency and accountability. Additionally it will look into its effectiveness in promoting reporting behavior.

Finally, chapter five will offer recommendations on how the Computer Misuse and Cybercrimes Act should be revised to include a limited liability clause to incentivize reporting of cybercrimes by private entities.

2.0 Cybercriminal Methods and Impact Severity

2.1 Introduction

In attempting to understand cybercrime, this chapter will first seek to determine how various authors generally classify cyber-attacks. Thereafter, it will demonstrate the nitty-gritty of cybercrime and its technicalities which relates to how they occur. Lastly, the chapter will delve into determining various negative impacts that occur when such online crimes occur.

2.2 Understanding the various classifications of cybercriminal activities

Cybercrime has become an increasingly menacing business and has evolved from being a hobby to being a lucrative business.[63] Cybercrime is as real as other criminal activities that involve actual people, crimes and even victims.[64] Various authors categorize cybercrime in differently. Sukhai delineates it into three categories: using computer as targets, tools for traditional crimes like credit card fraud and as an accessory like for storing illegal or stolen information.[65] Nurse, Katyal, Bossler and Berenblum further subdivide the first category into unauthorized access, unauthorized disruption and electronic identity theft[66] illustrated by instances like Defense Department breaches, the ILoveYou worm and identity theft respectively.[67] In contrast, Shinder categorizes cybercrime into pre-intrusion activities, password-cracking methods and technical exploits like trojans, viruses, and worms.[68]

2.3 Understanding the mechanics of cyber-attacks

2.3.1 Pre-intrusion acts

Pre-intrusion activities follow a sequence starting with pre-attack activities, gaining initial access, attaining full system access, planting "back doors" for future access to covering tracks.[69] The pre-intrusion phase involves gathering information on the target before initiating the attack.

[63] Huang K, Siegel M, Madnick S, 'Systematically understanding the cyber-attack business: A survey' 51 *Association for Computing Machinery Surveys* 4, 2018, 1.
[64] Hynds L, 'Hacker cracker' 149 *Royal Society of Arts Journal* 5500, 2002, 42.
[65] Sukhai N, 'Hacking and cybercrime' Proceedings of the 1st annual conference on information security curriculum development, Kennesaw Georgia, 2004, 129.
[66] Bossler A, Berenblum T, 'New directions in cybercrime research' 42 *Journal of crime and justice* 5, 2019, 495.
[67] Katyal N, 'Criminal law in cyberspace' 149 *The University of Pennsylvania* 4, 2001, 1013.
[68] Shinder D, 'Understanding network intrusions and attacks' in Tittel E (ed) *Scene of the cybercrime,* 1ed, Syngress Publishing, Massachusetts, 2002, 449.
[69] Shinder D, 'Understanding network intrusions and attacks' in Tittel E (ed) Scene of the cybercrime, 1ed, Syngress Publishing, Massachusetts, 2002, 431.

Information gathering includes determining the goal of the attack, the target, which could be the network or system, to be compromised to achieve the goal and identifying the weaknesses of the target for exploitation.[70] This could also encompass taking the necessary steps to disguise the attacker's identity or putting preliminary devices or programs in place for gathering information for easier access into the system when the time for the attack comes. Some of the pre-attack activities include: port scanning for identification of potential targets and their weaknesses, IP spoofing for disguising of the attacker's identity, placing of Trojans on target's system, placing tracking devices or software such as keystroke loggers on the target system, placing protocol analyzers such as sniffers for capturing transmissions to and from the target system.[71]

2.3.2 Gaining of access

Password cracking is another art utilized by cybercriminals to gain access to a computer system. It involves getting into a system by 'tricking' the system into thinking that you're an authorized user.[72] In most instances, this is done by utilizing a valid account name and password. According to computer security, there are three ways of validating user identity: the 'what you know' method, with the password being what you know; the 'what you have,' which requires physical possession of an object, for instance, a smart card; and the 'what you are,' which uses biometric data like fingerprint or an iris scan.[73] Most networks rely on the 'what you know' method; therefore, anyone who knows or is able to guess the correct password with a valid username can gain access.[74] Acquiring of valid passwords can be done through brute force, which is done through utilization of a program that runs through all words in a dictionary file and other possible character interactions, recovery and exploitation of passwords stored on the system, utilizing password decryption software or even social engineering.[75]

[70] Shinder D, 'Understanding network intrusions and attacks' in Tittel E (ed) Scene of the cybercrime, 1ed, Syngress Publishing, Massachusetts, 2002, 431.
[71] Shinder D, 'Understanding network intrusions and attacks' in Tittel E (ed) Scene of the cybercrime, 1ed, Syngress Publishing, Massachusetts, 2002, 432.
[72] https://www.techtarget.com/searchsecurity/definition/password-cracker on 2 January 2024.
[73] https://www.techtarget.com/searchsecurity/definition/password-cracker on 2 January 2024.
[74] https://www.techtarget.com/searchsecurity/definition/password-cracker on 2 January 2024.
[75] https://www.kaspersky.com/resource-center/definitions/brute-force-attack on 2 January 2024.

Unauthorized access involves gaining entry to a target's programs or files without authorization.[76] Intrusion could occur either electronically or physically. Electronically could involve password theft or through utilization of trap doors.[77] Additionally, it involves exploiting vulnerabilities to bypass security protocols or utilizing predefined shortcuts in programs.[78] On the other hand, physical intrusion involves physically breaking into storage locations. It can be aimed at government systems, individuals' private files, or even commercial entities.[79] This leads to invasion of privacy, jeopardizing of trade secrets and proprietary information, usually for financial gain.

Nonetheless unauthorized disruption involves interference with the functionality of a computer software or hardware without permission.[80] This could be through utilization of malware, which are malicious codes that are aimed to damage the network, such as viruses, worms, logic bombs, Trojan horses, ransomware and denial-of-service attacks.[81]

2.3.3 Technical exploits

A virus is a program that alters other computer programs, thereby causing the infected computer program to replicate the virus itself.[82] The virus modifies the original program to facilitate its own multiplication.[83] Once the computer program is infected, it covertly requests the computer's operating system to include a copy of the virus code into the targeted program.[84] At the instance the infected computer connects with another, whether through the internet, direct connection or shared storage, for example, floppy disks, the virus can extend its reach beyond the initial host

[76] Nurse J, 'Cybercrime and you: how criminals attack and the human factors that they seek to exploit', The Oxford Handbook of Cyberpsychology, 2018, 4 https://arxiv.org/abs/1811.06624v1 on 9 September 2023.
[77] Nurse J, 'Cybercrime and you: how criminals attack and the human factors that they seek to exploit', The Oxford Handbook of Cyberpsychology, 2018, 4 https://arxiv.org/abs/1811.06624v1 on 9 September 2023.
[78] Nurse J, 'Cybercrime and you: how criminals attack and the human factors that they seek to exploit', The Oxford Handbook of Cyberpsychology, 2018, 4 https://arxiv.org/abs/1811.06624v1 on 9 September 2023.
[79] Nurse J, 'Cybercrime and you: how criminals attack and the human factors that they seek to exploit', The Oxford Handbook of Cyberpsychology, 2018, 4 https://arxiv.org/abs/1811.06624v1 on 9 September 2023.
[80] Katyal N, 'Criminal law in cyberspace' 149 *The University of Pennsylvania* 4, 2001, 5.
[81] Katyal N, 'Criminal law in cyberspace' 149 *The University of Pennsylvania* 4, 2001, 5.
[82] Jahankhani H, Al-Nemrat A, Hosseinian-Far A, 'Cybercrime classification and characteristics' in (ed) *Cybercrime and cyber terrorism investigator's handbook*, 1st ed, Syngress, 2014, 161.
[83] Kurzban S, 'Viruses and worms- what can they do'? 7 *ACM SIGSAC Review* 1, 1989, 17.
[84] Kurzban S, 'Viruses and worms- what can they do'? 7 *ACM SIGSAC Review* 1, 1989, 17.

system.[85] The extent of damage caused by a virus is dependent on the additional code embedded in it, besides the self-replicating code.

A worm is a self-replicating program that can duplicate itself independently, unlike viruses that require human actions for transmission.[86] For instance, the ILoveYou bug combined characteristics of both viruses and worms.[87] It propagated across networks without human input, thereby resembling a worm. It can also breed on host computers' hard drives like a virus.[88] This bug spread rapidly over computers causing disruptions in companies and government agencies.[89]

A logic bomb is a set of programmed instructions within either a software or hardware that triggers specific actions under certain conditions or at a designated time.[90] These specified actions could range from harmless messages to destructive activities, e.g., data erasure. Logic bombs can remain concealed until activated by a pre-condition.[91] They could be utilized to facilitate real-world attacks, such as disruption of bank systems.[92] In contrast, a Trojan horse is a useful program with hidden malicious code that may either introduce viruses or even permit unauthorized access. Trojan horses are commonly used to introduce viruses into a computer system.[93]

Distributed Denial of Service (DDOS), which is a technical exploit, is launched from the owner's computer and are attacks on websites stopping them from communicating with other computers.[94] For this attack to occur, an individual obtains unauthorized access to a computer

[85] Shinder D, 'Understanding network intrusions and attacks' in Tittel E (ed) Scene of the cybercrime, 1ed, Syngress Publishing, Massachusetts, 2002, 452.
[86] Kurzban S, 'Viruses and worms- what can they do'? 7 *ACM SIGSAC Review* 1, 1989, 19.
[87] Griffiths J, 'I love you': How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on' CNN Business, 3 May 2020 https://edition.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html on 2 January 2024.
[88] Griffiths J, 'I love you': How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on' CNN Business, 3 May 2020 https://edition.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html on 2 January 2024.
[89] Griffiths J, 'I love you': How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on' CNN Business, 3 May 2020 https://edition.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html on 2 January 2024.
[90] https://www.techtarget.com/searchsecurity/definition/logic-bomb on 4 January 2024.
[91] https://www.techtarget.com/searchsecurity/definition/logic-bomb on 4 January 2024.
[92] https://www.techtarget.com/searchsecurity/definition/logic-bomb on 4 January 2024.
[93] Shinder D, 'Understanding network intrusions and attacks' in Tittel E (ed) Scene of the cybercrime, 1ed, Syngress Publishing, Massachusetts, 2002, 451.
[94] https://www.cisa.gov/news-events/news/understanding-denial-service-attacks on 14 January 2024.

system, and then places a software code that renders the system a 'Master.'[95] Additionally, the individual also breaks into other networks that act as intermediaries to place a code that turns the systems to agents or 'zombies' or 'slaves.'[96] Each Master has the ability to control multiple agents and the attack is initiated either remotely or by programmed commands sending information to the agents.[97] Upon receiving this information, the agents initiate multiple connection requests towards the target of the attack. Usually, they use a spoofed IP address to conceal the actual source of the request.[98] These agents then generate a substantial amount of traffic from different origins in a coordinated manner.[99] The high volume of SYN requests overwhelms the destination computer's capacity to acknowledge and complete interaction with each sender, consequently leading to Distributed Denial of Service.[100] DDOS attacks are challenging to trace as attacks come from remote computers with multiple source addresses with none as the attack's originator, hence often necessitating extensive investigations.[101]

Ransomware encrypts an individual's information and only permits subsequent access if ransom is paid, mostly by bitcoin or cryptocurrency.[102] The growth of ransomware has been phenomenal, especially in its use as a profit center for cybercriminals.[103] This increasing prevalence could be motivated by its high success rate. Victims tend to make a simple decision of cost versus benefit for individuals and organizations.[104] Mostly, they find the cost of paying the ransom is significantly less than the benefit of having access to the files; therefore, the ransom ends up being met. It is evident that criminals have found a key weakness in their targets and are carefully crafting crimes in order to exploit them. To further support their plight, they are making efforts to ensure that the paying of ransoms is seamless and 'painless.'[105]

---

[95] Katyal N, 'Criminal law in cyberspace' 149 *The University of Pennsylvania 4*, 2001, 8.
[96] Katyal N, 'Criminal law in cyberspace' 8.
[97] Katyal N, 'Criminal law in cyberspace' 8.
[98] https://www.cisa.gov/news-events/news/understanding-denial-service-attacks on 14 January 2024.
[99] https://www.cisa.gov/news-events/news/understanding-denial-service-attacks on 14 January 2024.
[100] https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection on 14 January 2024.
[101] Nurse J, 'Cybercrime and you: how criminals attack and the human factors that they seek to exploit,' The Oxford Handbook of Cyberpsychology, 2018, 6 https://arxiv.org/abs/1811.06624v1 on 9 September 2023.
[102] https://www.techtarget.com/searchsecurity/definition/ransomware#:~:text=Ransomware%20is%20a%20type%20of,accessing%20their%20files%20and%20systems on 14 January 2024.
[103] Nurse J, 'Cybercrime and you: how criminals attack and the human factors that they seek to exploit', The Oxford Handbook of Cyberpsychology, 2018, 15 https://arxiv.org/abs/1811.06624v1 on 9 September 2023.
[104] Nurse J, 'Cybercrime and you: how criminals attack and the human factors that they seek to exploit', The Oxford Handbook of Cyberpsychology, 2018, 15 https://arxiv.org/abs/1811.06624v1 on 9 September 2023.
[105] Nurse J, 'Cybercrime and you: how criminals attack and the human factors that they seek to exploit', The Oxford Handbook of Cyberpsychology, 2018, 16 https://arxiv.org/abs/1811.06624v1 on 9 September 2023.

2.3.4 Social engineering

Social Engineering, as one of the arts utilized by cybercriminals, is used to launch attacks to information security systems. It is perceived as the art of exploiting the weakest layer of Information Security systems, which is the people using the systems.[106] As the intention of the attacker varies, this form of attack is usually targeted towards users perceived to have access to sensitive information or possess rich knowledge.[107] Social Engineering involves gathering of information and exploitation. This gathered information is used to customize attacks. Phishing is a form of social engineering crime. It has its variants which include: voice phishing or vishing and smishing or SMS phishing.[108] These attacks have been highly successful and have cost its victims losses. While phishing involves using fake websites, for instance, to deceive an online user, vishing involves fraudulent calls to extract personal information.[109] Smishing on the other hand, employs text messages to extract personal information. Phishing can occur in various ways, which includes: Trojan horses, spoofing emails, hacking and even fake social network accounts.[110]

[106] Shinder D, 'Understanding network intrusions and attacks' in Tittel E (ed) Scene of the cybercrime, 1ed, Syngress Publishing, Massachusetts, 2002, 313.
[107] Shinder D, 'Understanding network intrusions and attacks', 313.
[108] Obuhuma J, Zivuku S, 'Social- Engineering based cyber-attacks in Kenya' IST- Africa Conference, Kampala, 2020, 2.
[109] Obuhuma J, Zivuku S, 'Social- Engineering based cyber-attacks in Kenya' 2.
[110] Shinder D, 'Understanding network intrusions and attacks', 489.

2.4 Assessing the impacts of cyber-attacks

Where there is commerce, there is a risk of cybercrime. Due to technological advancements, the threat landscape of cyber-attacks is rapidly changing and the potential impact of such attacks is uncertain due to the lack of effective metrics, tools and frameworks to understand and assess the harm organizations face from cyber-attacks.[111] There have been challenges in quantifying harm from cyber-attacks on organizations.[112] However, there are various approaches to quantifying harm, including monetary metrics, stock market fluctuations, and qualitative severity levels.[113]

2.4.1 Taxonomy of cyber-harm

Cyber-harm could be structured into five main types: physical or digital harm, economic harm, psychological harm, reputational harm, and social and societal harm.[114] This shows the multifaceted consequences of cyber-attacks. Physical or digital harm, which relates to a familiar organisational harm, is descriptive of a negative effect on someone or something as a result of a cyber-attack.[115] This would consist of corrupted data files, damaged or unavailable systems or even theft of sensitive information. Economic harm relates to negative financial consequences that can affect individuals, organisations and nations.[116] Similarly, psychological harm relates to disturbances to an individual's mental well-being and psyche.[117] Reputational harm pertains to an opinion held by the public in relation to the cyber-attack, whereas societal harm relates to a broader societal context of cyber-harm.[118] Each type has multiple sub-types that provide a detailed breakdown of the different ways harm can manifest in each category. For instance, psychological harm could manifest itself in form of frustration, anxiety, depression or even

[111] Agrafiotis I, Nurse J, Goldsmith M, Creese Sadie, Upton D, 'A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate' 4 *Journal of Cybersecurity* 1, 2018, 1.
[112] Agrafiotis I, Nurse J, Goldsmith M, Creese Sadie, Upton D, 'A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate' 4 *Journal of Cybersecurity* 1, 2018, 4.
[113] Agrafiotis I, *et al*, 'A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate', 4.
[114] Agrafiotis I, *et al*, 'A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate', 1.
[115] Agrafiotis I, *et al*, 'A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate', 7.
[116] Agrafiotis I, Bada M, Cornish P, Creese S, Goldsmith M, Ignatuschtschenko E , Roberts T , Upton D, 'Cyber harm: concepts, taxonomy and measurement' Saïd Business school, Working Paper Number 23, 2016, 20 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2828646 on 11 February 2024.
[117] National Collaborating Centre for Mental Health, *Self-harm: the short-term physical and psychological management and secondary prevention of self-harm in primary and secondary care*, 2004, 1.
[118] Agrafiotis I, *et al*, 'Cyber harm: concepts, taxonomy and measurement', 14.

suicidal thoughts[119] while reputational harm could be in the form of a reduction in corporate goodwill.[120]

2.4.2 The Ripple-effect of cyber-attacks

Cyber-harm may propagate. This is where one type of harm can lead to others in a cascading effect. This is evident from the JP Morgan case which is one of the largest banks in the USA. It suffered a cyber-attack where hackers gained administrator access to their servers.[121] The breach exposed information such as names, phone numbers, email addresses and even physical addresses of account holders. The Bank had increased its cybersecurity budget by $250 million per year just before the attack. However, the company had to replace most of its IT infrastructure and hired over 1000 employees to monitor its systems. Nevertheless, the affected customers had to monitor their finances to prevent fraud and financial scams. This case study emphasizes the financial burden and the impact on the affected customers who had to safeguard their finances.

The impact caused by a cyber-attack to a firm depends on whether it conveys new information or not.[122] If an attack does not change the assessment of the risk or loss distribution if its impact is limited to the direct costs incurred.[123] However, if the attack reveals new information or leads to overreactions, it can have broader consequences. Cyber-attacks involve the loss of financial information, which may significantly have a negative impact on the stock prices.[124] In addition to this, deteriorating credit ratings, decreasing capital expenditures may be experienced by firms that become victims of cybercrime.

[119] Buchanan T, Whitty T, 'The online dating romance scam: causes and consequences of victimhood' 20 *Psychology, Crime & Law* 3, 2013, 31.
[120] Agrafiotis I, *et al*, 'Cyber harm: concepts, taxonomy and measurement', 21.
[121] Karabus J, 'JP Morgan must face suit from ray-ban maker after crooks drained $272m from accounts' The Register, 6 January 2023 https://www.theregister.com/2023/01/06/jp_morgan_lawsuit_essilor/ on 14 January 2024.
[122] Kamiya S, Kang J, Jungmin K, Milidonis A and Stulz R, 'What is the impact of successful cyber-attacks on targeted firms' National Bureau of Economic Research, Working Paper Series Number 24409, 2018, 1 https://www.nber.org/papers/w24409 on 16 September 2023.
[123] Kamiya S, Kang J, Kim J, Milidonis A and Stulz R, 'What is the impact of successful cyber-attacks on targeted firms' National Bureau of Economic Research, Working Paper Series Number 24409, 2018, 2 https://www.nber.org/papers/w24409 on 16 September 2023.
[124] Kamiya S, Kang J, Kim J, Milidonis A and Stulz R, 'What is the impact of successful cyber-attacks on targeted firms' National Bureau of Economic Research, Working Paper Series Number 24409, 2018, 2 https://www.nber.org/papers/w24409 on 16 September 2023.

2.5 Conclusion

Cybercrime has become an emerging and multifaceted issue affecting individuals, organizations and society at large. This is evident through various means all of which have far reaching consequences. The intricate steps taken by cybercriminals to exploit weaknesses and cause disruption in computer networks are clear. Notably, the various impacts including a cascade of impacts caused by cybercrime have been highlighted. In essence, we see the severity of cybercrime and its complexity as well and the need to robust cyber-security measures to address its progressive nature.

3.0 The significance of cyber-incident reporting: Evaluating the current legal framework

3.1 Introduction

Due to global technological advancements, the significance of transparency and accountability in cybersecurity cannot be overstated. Reporting mechanisms stand vital in ensuring this. This chapter will delve into evaluating why organizations avoid reporting cyber-attacks and thereafter it will seek to evaluate the significance of cyber-incident reporting as a catalyst for transparency and accountability. Additionally, it will scrutinize the existing legal framework that seeks to regulate reporting practices. Through this, its strengths and weaknesses will aim to illuminate the need for a reform of the current legal framework.

3.2 Evaluating the significance of cyber-incident reporting

Due to the high number of cyber breaches there is need for cybersecurity.[125] Cyber security fundamentally revolves around protecting against threats that uniformly involve the possibility of either an attack or a breach.[126] It involves defending against malicious attacks on data and computer networks.[127]

Cyber threats pose a significant challenge as a result of its borderless and unpredictable nature.[128] Its effects can extend beyond the online realm affecting even the real-world security.[129] Complete protection may be unachievable; however, having defenses in place may assist in mitigating the risk.

Cyber-incident reporting is a form of cyber security that organizations are often hesitant to practice. Its ultimate aim of it is to identify the culprit and minimize such occurrence by

[125] Craigen D, Diakun-Thibault N and Purse R, Defining cybersecurity, 4 *Technology Innovation Management Review* 10, 2014, 13.
[126] Craigen D, Diakun-Thibault N and Purse R, Defining cybersecurity, 4 *Technology Innovation Management Review* 10, 2014, 14.
[127] Peslak A, Hunsinger S, What is cybersecurity and what cybersecurity skills are employers seeking? 20 *Issues in Information Systems* 2, 2019, 63.
[128] Barrachin M, Pipikaite A, We need a global standard for reporting cyber-attacks, Harvard Business Review, 6 November 2019 https://hbr.org/2019/11/we-need-a-global-standard-for-reporting-cyber-attacks on 15 November 2023.
[129] Craigen D, *et al*, Defining cybersecurity, 14.

preventing another incident from happening.[130] However, the authorities may only assist where they are aware of the incident.

Notifying the relevant authorities helps businesses to better protect their time and money for instance; in a ransom ware attack, blocked information may be decrypted to prevent business losses.[131] A detailed assessment of the harm such as details on the ransom payment, financial loss or compromised data is required when filing a report on the breach.[132] Over time, this data could be aggregated to quantify the types and the impact of cybercrimes. This data may be used to educate users on cybercrime prevention and may aid law enforcement in resolving cases while at the same time allowing the government to understand various trends and changes in the cyber threat environment.

At the same time it raises awareness on the seriousness of the risks associated with the use of IT systems.[133] Reporting cyber-crime maintains regulatory compliance and also prevents costly security events as cyber threats are expected to reach a staggering amount in the near future.[134] It aids in the identification of vulnerabilities, understanding the attack's intent, and tracing the source of the attack.[135] Nonetheless law enforcement may assist in recovering payments from ransomware attacks and prevent fraudulent transfers or transactions thereby mitigating harm and financial losses.

[130] Cierra P, 'Silent threat; FBI warns against trend of not reporting cyber attacks' WTHR, 11 August 2022 https://www.wthr.com/article/news/investigations/13-investigates/silent-threat-fbi-warns-against-trend-of-not-reporting-cyberattacks-ransomware/531-6cbee4c4-c23a-4d13-af20-ffb2fe6aa3a4 on 19 September 2023.
[131] Cierra P, 'Silent threat; FBI warns against trend of not reporting cyber attacks' WTHR, 11 August 2022 https://www.wthr.com/article/news/investigations/13-investigates/silent-threat-fbi-warns-against-trend-of-not-reporting-cyberattacks-ransomware/531-6cbee4c4-c23a-4d13-af20-ffb2fe6aa3a4 on 19 September.
[132] Cierra P, 'Silent threat; FBI warns against trend of not reporting cyber attacks' WTHR, 11 August 2022 https://www.wthr.com/article/news/investigations/13-investigates/silent-threat-fbi-warns-against-trend-of-not-reporting-cyberattacks-ransomware/531-6cbee4c4-c23a-4d13-af20-ffb2fe6aa3a4 on 19 September.
[133] Bougaardt G, Kyobe M, 'Investigating the factors inhibiting SMEs from recognizing and measuring losses from cybercrime in South Africa', ICIME Proceedings of the 2nd International Conference on Information Management and Evaluation, Toronto, Canada, 2011, 169.
[134] Mackay J, 'The importance of security incident reporting' Metacompliance, https://www.metacompliance.com/blog/cyber-security-awareness/the-importance-of-security-incident-reporting on 17 September 2023.
[135] Mencini D, 'The benefits and risks of notifying law enforcement' Morrison and Foerster, 9 February 2023 https://www.mofo.com/resources/insights/200114-benefits-risks-notifying-law-enforcement on 18 September 2023.

In addition, reporting involvement with law enforcement strengthens an organization's narrative when communicating with stakeholders, including customers, regulators, and the public.[136] It demonstrates a proactive response to the breach.

Cyber resilience encompasses cyber-incident reporting.[137] It strengthens the cybersecurity resilience of the financial sector while also serving as an early warning system to financial services sector on significant cyber incidents.[138] Accountability also ensures identification of common tactics and techniques used by threat actors and provide insights into the vulnerabilities that threat actors may exploit to gain unauthorized access into firms.[139]

Reporting would enhance both the volume and timeliness of incident reporting, allowing governments to issue early warnings to businesses about emerging threats or potential problems.[140] This capability to provide "indications and warning" enables companies to take preparatory actions before cyber threats materialize, potentially preventing incidents. Timely warnings are more credible and effective in prompting companies to address vulnerabilities or prioritize cybersecurity upgrades.[141]

3.3 Understanding the bars to cyber-incident reporting

Cybercrime has become part of our everyday lives with a significant number of individuals becoming victims of identity theft and consumer fraud among other crimes.[142] Organizations are nonetheless often hesitant to publicly disclose cyber incidents due to concerns about revealing vulnerabilities or financial damage. They ask themselves a simple question of 'what is the

[136] Mencini D, 'The benefits and risks of notifying law enforcement' Morrison and Foerster, 9 February 2023 https://www.mofo.com/resources/insights/200114-benefits-risks-notifying-law-enforcement on 18 September 2023.
[137] https://www.fsb.org/wp-content/uploads/FSSCC-1.pdf on 22 September 2023.
[138] Daniel M, 'Reporting cyber-attacks will soon be mandatory. Is your company ready?' Harvard Business Review, 2023 https://hbr.org/2023/04/reporting-cyberattacks-will-soon-be-mandatory-is-your-company-ready on 23 September 2023.
[139] https://www.fsb.org/wp-content/uploads/FSSCC-1.pdf on 22 September 2023.
[140] Daniel M, 'Reporting cyber-attacks will soon be mandatory. Is your company ready?' Harvard Business Review, 2023 https://hbr.org/2023/04/reporting-cyberattacks-will-soon-be-mandatory-is-your-company-ready on 23 September 2023.
[141] Daniel M, 'Reporting cyber-attacks will soon be mandatory. Is your company ready?' Harvard Business Review, 2023 https://hbr.org/2023/04/reporting-cyberattacks-will-soon-be-mandatory-is-your-company-ready on 23 September 2023.
[142] Weijer V, Steve G, Leukfeldt R, Bernasco W 'Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud and hacking' 16 *European Journal of Criminology* 4, 2019, 486.

point?'[143] They fail to realize that such crimes may be a silent threat but they usually have a great potential impact on a country's economy and national security.[144] Often, it is acknowledged that the hesitancy is due to fear of negative publicity but not reporting sometimes still results in such publicity.[145]

3.3.1 Obstacles in reporting cybercrime

One of the barriers is the existence of an ambiguity in understanding what constitutes a cybercrime and when a victim should report it.[146] Alternatively, there also lies a complexity in identifying when a cybercrime occurs and recognizing them afterward.[147] Moreover, there is limited knowledge about how to report cybercrimes to the appropriate authorities thereby making it a challenge for the individuals to engage in the reporting process.[148]

There is also a perception that no satisfactory results would be gotten from reporting cybercrimes.[149] This is because identifying these cyber threat actors has proven to be notoriously difficult given the level of sophistication used in carrying these attacks.[150] Lack of transparency with regard to the feedback received by victims after reporting cybercrimes is also evident.[151] This deters building up of confidence in the reporting process.

Another reason for the underreporting of cyber incidents is a recent trend towards ransomware attacks.[152] Ransomware is a type of malware that encrypts data until a ransom is paid by the

[143] Swinhoe D, 'Why businesses don't report cybercrimes to law enforcement' Computer Security Online, 30 May 2019 <https://www.csoonline.com/article/567307/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html> on 2 February 2024.
[144] Cierra P, 'Silent threat; FBI warns against trend of not reporting cyber attacks' WTHR, 11 August 2022 https://www.wthr.com/article/news/investigations/13-investigates/silent-threat-fbi-warns-against-trend-of-not-reporting-cyberattacks-ransomware/531-6cbee4c4-c23a-4d13-af20-ffb2fe6aa3a4 on 19 September 2023.
[145] Cierra P, 'Silent threat; FBI warns against trend of not reporting cyber attacks' WTHR, 11 August 2022 https://www.wthr.com/article/news/investigations/13-investigates/silent-threat-fbi-warns-against-trend-of-not-reporting-cyberattacks-ransomware/531-6cbee4c4-c23a-4d13-af20-ffb2fe6aa3a4 on 19 September 2023.
[146] Bidgoli M, Grossklags J, End user cybercrime reporting: what we know and what we can do to improve it, 5.
[147] -<https://www.mattnj.com/news-events/cyber-crime-cases-why-are-hacks-going-unreported> on 3 February 2024.
[148] Bidgoli M, Grossklags J, End user cybercrime reporting: what we know and what we can do to improve it, 5.
[149] Bidgoli M, Grossklags J, 'End user cybercrime reporting: what we know and what we can do to improve it,' IEEE International Conference on Cybercrime and Computer Forensics, Vancouver, Canada, 2016, 5.
[150] Swinhoe D, 'Why businesses don't report cybercrimes to law enforcement' Computer Security Online, 30 May 2019 <https://www.csoonline.com/article/567307/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html> on 2 February 2024.
[151] Bidgoli M, Grossklags J, End user cybercrime reporting: what we know and what we can do to improve it, 5.
[152] -< https://www.idx.us/knowledge-center/why-many-cyberattacks-are-never-reported> on 3 February 2024.

victim.[153] In such instances, organizations targeted in these attacks, likely based on factual assessment or counsel, may conclude that these incidents do not qualify as data breaches.[154] Also some companies would prefer dealing with the incident internally that is by paying the extortion.[155] As a result, they may not feel the need to report such incidents.

Reluctance in reporting may also arise from differing priorities between companies and law enforcement bodies. A company's priority when a data breach occurs is to remedy the situation at hand, cater for the internal deficiencies caused, notify the affected parties and ensure such a data breach does not reoccur.[156] On the other hand, the law enforcer's priority is to identify the perpetrator and bring them to justice.[157] Additionally, they may find one-off minor incidents not worth their time making companies reluctant to report such incidents as they may not see the need in involving the authorities.[158]

Another perspective that victims base their decision is from the lens of expected cost versus the benefit of each alternative.[159] An expected benefit could be financial compensation whereas an expected cost could be time or expenses incurred. It is therefore obvious that individuals may choose to report a cybercrime where the benefits override the costs. As a result, companies end up not getting law enforcement involved but resolving the issue internally.

3.3.2 Barriers faced by Small and medium enterprises

Small and medium sized enterprises (SMEs) are also reluctant towards reporting cybercrime incidences.[160] They are facing significant challenges when it comes to identifying and

[153] -<https://www.cisa.gov/stopransomware> on 3 February 2024.
[154] -< https://www.idx.us/knowledge-center/why-many-cyberattacks-are-never-reported> on 3 February 2024.
[155] -< https://www.idx.us/knowledge-center/why-many-cyberattacks-are-never-reported> on 3 February 2024.
[156] Swinhoe D, 'Why businesses don't report cybercrimes to law enforcement' Computer Security Online, 30 May 2019 <https://www.csoonline.com/article/567307/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html> on 2 February 2024.
[157] Swinhoe D, 'Why businesses don't report cybercrimes to law enforcement' Computer Security Online, 30 May 2019 <https://www.csoonline.com/article/567307/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html> on 2 February 2024.
[158] Swinhoe D, 'Why businesses don't report cybercrimes to law enforcement' Computer Security Online, 30 May 2019 <https://www.csoonline.com/article/567307/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html> on 2 February 2024.
[159] Weijer V *et al*, Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking, 487.
[160] Bougaardt G, Kyobe M, Investigating the factors inhibiting SMEs from recognizing and measuring losses from cybercrime in South Africa, 169.

quantifying damages in relation to cybercrime incidents.[161] They lack the necessary skills and resources for proper risk management together with inadequate infrastructure for information security systems.[162] This reluctance could be attributed to concerns about maintaining confidentiality, potential disruptions to business operations and the fear of reputational damage. They are unaware of the awareness that could be raised with reporting such incidences.

There also exists a perception that cybercriminals are more interested with larger organizations with valuable data. However, SMEs are mostly targeted by cybercriminals precisely because they are an easier target and less protected.[163] These attacks may result in increased financial losses or even closure of businesses underscoring the urgent need for cybersecurity measures such as reporting of cybercrime.[164]

3.4 Assessing the current reporting framework in Kenya

3.4.1 Computer Misuse and Cybercrimes Act of 2018

The Computer Misuse and Cybercrimes Act (CMCA) provides for offences relating to computer systems. It enables timely and effective detection, prohibition, prevention, response, investigation and prosecution of cybercrimes. It establishes the National Computer and Cybercrimes Coordination Committee (NC4), under the National Security Council, whose mandate is to ensure coordination of cyber security concerns to ensure effective prevention and detection.[165]

The Act of Parliament mandates any person who operates a computer system or network whether in the public or private sphere to inform the Committee of any attack, disruption or intrusion

[161] Bougaardt G, Kyobe M, Investigating the factors inhibiting SMEs from recognizing and measuring losses from cybercrime in South Africa, 167.
[162] Bougaardt G, Kyobe M, 'Investigating the factors inhibiting SMEs from recognizing and measuring losses from cybercrime in South Africa', Proceedings of the 2nd International Conference on Information Management and Evaluation, Toronto, Canada, 2011, 169.
[163] Gallant B, 'Why do SMBs neglect cyber security'? LinkedIn, 8 October 2023, - <https://www.linkedin.com/pulse/why-do-smbs-neglect-cyber-security-brett-gallant#:~:text=Misconception%20of%20Not%20Being%20a,easier%20and%20less%20protected%20targets> on 10 February 2024.
[164] Dinha F, 'The effects of cybercrime on small businesses' Forbes, 11 May 2023 - <https://www.forbes.com/sites/forbestechcouncil/2023/05/11/the-effects-of-cybercrime-on-small-businesses/?sh=7ee16cfb2f68> on 10 February 2024.
[165] Section 4, *Computer Misuse and Cybercrimes Act* (Act No 5 of 2018).

within 24 hours of such attack, disruption or intrusion.[166] The section goes ahead and spells out the content of the report which includes information about the breach, including a summary of any information that the agency knows on how the breach occurred, an estimate of the number of people affected by the breach, an assessment of the risk of harm to the affected individuals, and an explanation of any circumstances that would delay or prevent the affected persons from being informed of the breach.[167] Finally the section imposes a fine not exceeding two hundred thousand shillings or imprisonment for a term not exceeding two years or both.[168]

3.4.2 Trend in the cyber-threat landscape

The years 2019 and 2020 were marked by an increase in cyber-attacks across different key sectors such as the government and financial services among others.[169] Over the last three years from 2021, the number of cyber threats detected in Kenya has significantly increased from 4,589 in July-September 2017 to 143,040,599 in July-September 2021.[170] The National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC) revealed that from July to September 2022, there was a 10.08 percent drop in cyber threats over the October-December 2022 timeframe.[171] In comparison to the threat events detected in the preceding period, October-December 2022, the National KE-CIRT/CC detected a 24.89 percent drop in January-March 2023.[172] The National KE-CIRT/CC detected 139,775,123 cyber threat events between April and June 2023, a drop of 25.6 percent from the 187,757,659 threat events discovered between January and March 2023.[173] With systems attacks being the most common, the National KE-CIRT/CC detected almost 1.2 billion cyber threat occurrences between October

[166] Section 40, *Computer Misuse and Cybercrimes Act* (Act No 5 of 2018).
[167] Section 40, *Computer Misuse and Cybercrimes Act* (Act No 5 of 2018).
[168] Section 40(4), *Computer Misuse and Cybercrimes Act* (Act No 5 of 2018).
[169] Serianu, *Local perspective on data protection and privacy laws*, 2020, 13.
[170] National Computer and Cybercrimes Coordination Committee Secretariat, *National cybersecurity strategy*, 2022, 3.
[171] National Kenya Computer Incident Response Team – Coordination Centre, October -December cybersecurity report, 2022, 10.
[172] National Kenya Computer Incident Response Team – Coordination Centre, January- March cyber security Report, 2023, 7.
[173] National Kenya Computer Incident Response Team – Coordination Centre, April- June cyber security report, 2023, 11.

and December 2023, a 943.01 percent increase over the 123 million threats recorded in the previous period from July to September 2023.[174]

Kenya has experienced a record high of 860 million cyber-attacks in 2023, marking a significant increase in both frequency and sophistication of cyber-threats.[175] The Communications Authority reports that over the past year, the number of attacks has surged dramatically, with 79 percent of these attacks attributed to cyber criminals exploiting weaknesses and vulnerabilities in organizations' internal controls and information systems to gain unauthorized access to computer systems.[176] This figure represents a stark contrast to six years ago when cyber-attacks in Kenya were reported to be at 7.7 million annually.[177]

3.4.3 Addressing cyber security policies in Kenya

Kenya continues to face cyber threats increasingly.[178] These cyber threats include data breaches, cyber espionage, and cyber sabotage among others. Cyber security is a major problem with the main cause being the existing gaps in existing cyber security laws.[179] In light of the Cybersecurity Strategy, there is need to enhance cyber security policies and laws for efficacy and coherency[180] as there has been an acknowledgement of a cyber-security gap.[181] Cyber security involves measures put in place to deter and control cybercrime. Reporting of cybercrime is a cyber-security measure that has not been adequately practiced and enforced. Statistically, 88

[174] National Kenya Computer Incident Response Team – Coordination Centre, October -December cyber security Report, 2023, 5.
[175] Musau D, 'Kenya hit by record 860 million cyber-attacks in 2023' Citizen Digital, 4 October 2023 -<https://www.citizen.digital/news/kenya-hit-by-record-860-million-cyber-attacks-in-2023-n328649> on 11 February 2024.
[176] Musau D, 'Kenya hit by record 860 million cyber-attacks in 2023' Citizen Digital, 4 October 2023 -<https://www.citizen.digital/news/kenya-hit-by-record-860-million-cyber-attacks-in-2023-n328649> on 11 February 2024.
[177] Musau D, 'Kenya hit by record 860 million cyber-attacks in 2023' Citizen Digital, 4 October 2023 -<https://www.citizen.digital/news/kenya-hit-by-record-860-million-cyber-attacks-in-2023-n328649> on 11 February 2024.
[178] National Computer and Cybercrimes Coordination Committee Secretariat, *National cybersecurity strategy*, 2022, 3.
[179] Serianu, Achieving cyber security resilience: enhancing visibility and increasing awareness, 2016, 19.
[180] National Computer and Cybercrimes Coordination Committee Secretariat, *National cybersecurity strategy*, 2022, 9.
[181] Serianu, Achieving cyber security resilience: enhancing visibility and increasing awareness, 2016, 30.

percent of cybercrime has gone unreported[182] and those that are reported, very few are followed through to prosecution.[183]

In light of the trend in the cyber-threat landscape in Kenya, we see a decrease of 10.08 percent in cybercrime within the 2022 timeframe then a drastic increase in 2023. This shows the dynamic and evolving nature of threats. It is evident that cybercriminals are adapting their strategies in order to circumvent the defenses put in place. Therefore, there is a need to take proactive approaches to stay ahead and with implementation of robust cyber security policies, there is potential for improvement in the overall cyber security posture in the country.

3.5 Conclusion

The evaluation of cyber-incident reporting has shown its significance within the cybersecurity realm. The Computer Misuse and Cybercrimes Act (CMCA) mandates reporting of cyber-attacks within a specified timeframe, but it is evident that this measures have not proven effective due to the drastic increase in cyber threats faced in the country, highlighting the need to review and amend the existing regulations surrounding cyber security. While cyber-incident reporting is undeniably important, the barriers in existence hinder its efficacy in addressing the growing cyber threat landscape. Addressing these barriers may be effective in fortifying resilience against cyber threats.

[182] Serianu, Achieving cyber security resilience: enhancing visibility and increasing awareness, 2016, 23.
[183] Serianu, Achieving cyber security resilience: enhancing visibility and increasing awareness, 2016, 30.

4.0 The implications of a limited liability clause: Fostering reporting behavior in the private sector

4.1 Introduction

This chapter seeks to contribute valuable insights to the ongoing discourse surrounding legal incentives, liability protection, and the limitations posed by the concept of limited liability. Legal incentives act as a catalyst for desired behavior. They prompt organizations to align their actions with the set legislation or norms. Understanding legal incentives and its nuances will shed more light on the need for a liability protection clause. While also scrutinizing the potential drawbacks associated with a limited liability clause, the double-edged sword that grants protection, the chapter aims to offer insights that contribute to a balanced understanding of the limitations and implications inherent in this adopted legal construct.

4.2 Assessing the implication of legal incentives

Legal incentives are considered a powerful concept in legal analysis and regulatory design.[184] They may be defined as interventions that are utilized to mitigate deterrents and enhance motivations for individuals to act in a certain way.[185] They are established within the confines of the law and are designed to influence behavior positively as they are curated around factors that influence specific actions. An example is tax breaks or financial aid issued by the government to companies investing in renewable energy in order to encourage cleaner and sustainable use of energy sources.

The focus is on predicting and managing the outcomes of individual choices through incentives. The law is portrayed as a tool for creating incentives to compensate for the inadequacies of natural instincts, with a shift from cultivating civic virtue to designing institutions that function effectively in its absence.[186] Incentives acknowledge that human behavior is influenced by desires for various rewards and aversions to sanctions. These incentives can range from

[184] Emad A, Why motives matter: reframing the crowding out effect of legal incentives, 123 *The Yale Law Journal* 4, 2014, 862.
[185] https://www.law.cornell.edu/wex/incentive#:~:text=An%20incentive%20is%20a%20reason,financial%20subsidies%2C%20or%20tax%20provisions on 16 November 2023.
[186] Emad A, Why motives matter: reframing the crowding out effect of legal incentives, 123 *The Yale Law Journal* 4, 2014, 862.

monetary rewards to considerations of job security, promotion, esteem, and the altruistic value of serving the public interest.[187]

The United Nations Convention on Corruption categorizes incentives as either hard or soft. It makes a distinction where soft incentives involve non-tangible recognition whereas hard incentives involve tangible rewards.[188] Liability protection fits within the confines of soft incentives.

While legal incentives try to encourage legal compliance it also has its downsides. The crowding-out effect refers to the harm that can arise when external incentives or rewards diminish intrinsic motivations.[189] It is a phenomenon where external motivations may diminish individuals' intrinsic motivations for certain activities.[190] It suggests that incentives can alter motivations by redirecting attention away from intrinsic considerations, rendering intrinsic motives vulnerable.[191] The traditional view of the crowding out effect questions the efficacy of legal incentives, suggesting that the decline in intrinsic motivation may make individuals less likely to engage in desired behavior.[192] Intrinsic motivation is viewed as valuable because it leads to better behavioral outcomes, such as compliance with the law or positive social norms.[193]

There's an assumption that people perform better when promised incentives, however these incentives typically secure only temporary compliance rather than fostering lasting change in attitudes and behavior.[194] Studies across different settings show that rewards do not create enduring commitments or induce sustained changes in behavior. Instead, they temporarily alter

[187] Boyne G, Hood C, Incentives: new research on an old problem, 20 *Journal of Public Administration Research and theory* 2, 2010, 177.
[188] Rahman K, Legal incentives for compliance in the private sector, U4 Anti-Corruption Resource Centre, June 2020 https://www.u4.no/publications/legal-incentives-for-compliance-in-the-private-sector on 2 January 2024.
[189] Emad A, Why motives matter: reframing the crowding out effect of legal incentives, 123 *The Yale Law Journal* 4, 2014, 862.
[190] Promberger M, Marteau T, When do financial incentives reduce intrinsic motivation? Comparing behaviors studied in psychological and economic literatures, 32 *Health Psychology* 9, 2013, 951.
[191] Promberger M, Marteau T, When do financial incentives reduce intrinsic motivation? Comparing behaviors studied in psychological and economic literatures, 2013, 952.
[192] Emad A, Why motives matter: reframing the crowding out effect of legal incentives, 123 *The Yale Law Journal* 4, 2014, 862.
[193] Emad A, Why motives matter: reframing the crowding out effect of legal incentives, 862.
[194] Folmer C, 'Crowding-out effects of laws, policies and incentives on compliant behavior' *Cambridge Handbook of Compliance*, 2021, 5, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4138087 on 15 January 2024.

actions without fundamentally impacting underlying attitudes.[195] This reliance on behavioral manipulation doesn't inherently address motivation and often perpetuates the cycle of reliance on rewards.[196]

4.3 Understanding liability protection and its significance

Liability protection refers to safeguarding institutions and individuals from facing punitive measures or additional penalties when they voluntarily share information to enhance trust and collectively combat threats or breaches.[197] The emphasis is on establishing mechanisms that ensure institutions can freely exchange information without fear of retribution or facing harsh repercussions, such as hefty fines or penalties.

As a form of incentive, they are considered more conducive to fostering cooperation and reporting among organizations that have fallen victim to cyber-attacks.[198] It aims to build mutual trust and collaboration thereby contributing to national resilience. Therefore, organizations should be granted extensive liability safeguards when reporting cyber incidents.

Reporting entities must be confident that they won't encounter legal repercussions due to submitting a cyber-incident report. This confidence should encompass protection from both civil and criminal liability, as well as safeguarding against any form of regulatory enforcement stemming from the act of reporting or the content of the report. This is not only a matter of equity but also crucial for upholding the reporting's quality and credibility which is what liability protections try to do. It ensures that reporting entities can wholly concentrate on delivering the most comprehensive and detailed information available, rather than diverting their focus to shield themselves from potential legal consequences. The absence of liability assurance may deter organizations from reporting candidly and could lead to information restriction or bias while still meeting the minimum reporting requirements.

[195] Folmer C, 'Crowding-out effects of laws, policies and incentives on compliant behavior' *Cambridge Handbook of Compliance*, 2021, 5, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4138087 on 15 January 2024.
[196] Folmer C, 'Crowding-out effects of laws, policies and incentives on compliant behavior' *Cambridge Handbook of Compliance*, 2021, 5, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4138087 on 15 January 2024.
[197] https://www.fsb.org/wp-content/uploads/FSSCC-1.pdf on 22 September 2023.
[198] https://www.confidentialitycoalition.org/about/cyber-incident-reporting-principles/ on 23 September 2023.

4.4 Assessing the reporting framework in the United States

The Critical Infrastructure Act of 2022 is a step forward for voluntary disclosures by companies that have experienced cyber-attacks. It is a breathing example of incorporation of a limited liability clause. The Act requires companies to report significant cyber incidents while offering protections thereby incentivizing them to report.[199] This liability protection limits the dissemination of any personal or identifiable information collected in conjunction with the reporting requirements.[200] The provision states that no legal action can be initiated in any court by any individual or entity against another party solely based on the submission of a cyber-incident report in accordance with the law and associated rules.[201] The scope of this liability protections is however limited to litigation directly related to the submission of a cyber-incident report or a report on ransom payments to the relevant agency. It specifies that no report submitted or any related communication, document, or record created for the sole purpose of preparing and submitting such a report can be used as evidence, subject to discovery, or presented in any legal proceedings at the federal, state, or local level, except when unrelated materials are concerned.[202] In essence, this provision aims to protect those who comply with the reporting requirements from legal action tied specifically to the act of reporting.

Another piece of legislation is the Cybersecurity Information Sharing Act of 2015 which was enacted to improve cybersecurity in the United States through enhanced sharing of information in relation to cybersecurity threats. The section of law protects private entities from liability in relation to sharing or receipt of cyber threat indicators.[203] It establishes that private entities conducting information system monitoring with the law will be shielded from legal action and any such action brought against the party shall be dismissed.[204] In addition to this, private entities that share or receive cyber threat indicators or defensive measures are protected from legal action provided that institutions comply with the federal government and, if sharing with the federal government, to do so in accordance with the specific guidelines set forth.[205] Lastly, the section

[199] Section 2245 (c), *The Cyber Incident Reporting for Critical Infrastructure Act,* 2022.
[200] https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/cyber-breach-reporting-legislation.html on 24 September 2023.
[201] Section 2245 (c), *The Cyber Incident Reporting for Critical Infrastructure Act*, 2022.
[202] Section 2245 (c), *The Cyber Incident Reporting for Critical Infrastructure Act*, 2022.
[203] Section 106, *Cybersecurity Information Sharing Act*, 2015.
[204] Section 106, *Cybersecurity Information Sharing Act*, 2015.
[205] Section 106, *Cybersecurity Information Sharing Act*, 2015.

clarifies that the law doesn't create an obligation for entities to disclose such information or take specific actions based on it.[206]

4.5 Determining the potential drawbacks to a limited liability clause

Implementing a limited liability clause to incentivize companies to report cyber-attacks comes with potential drawbacks that need careful consideration. One of the concerns is the possibility of underreporting or selective reporting, where companies may disclose only certain incidents to avoid significant legal consequences.[207] This could lead to incomplete and inaccurate reporting, undermining the effectiveness of cybersecurity measures.[208]

Furthermore, a limited liability clause may inadvertently lead to reduced investments in robust cybersecurity measures.[209] If companies perceive that their financial liability is capped, they might be less motivated to allocate resources to comprehensive cybersecurity defenses, potentially leaving their systems more vulnerable to cyber-attacks.

Additionally, victims of cyber-attacks, such as customers and clients, may face adverse consequences if companies are not held fully accountable for security breaches. This could lead to a negative impact on individuals whose data is compromised. The legal and regulatory challenges associated with implementing a limited liability clause are also significant. Determining the appropriate cap on liability, defining the scope of covered incidents, and addressing potential conflicts with existing laws would require careful consideration. Nonetheless, a limited liability clause may increase the burden on law enforcement agencies if companies, feeling less compelled to invest in cyber security, contribute to a higher number of cybercrime incidents. This strain on resources could hinder effective response efforts.

Ultimately, unintended consequences, such as companies exploiting loopholes or engaging in unethical practices, are potential risks associated with implementing limited liability clauses.

---

[206] Section 106, *Cybersecurity Information Sharing Act*, 2015.
[207] Daniel M, 'Reporting cyber-attacks will soon be mandatory. Is your company ready'? Harvard Business Review, 19 April 2023 https://hbr.org/2023/04/reporting-cyberattacks-will-soon-be-mandatory-is-your-company-ready on 23 September 2023.
[208] Daniel M, 'Reporting cyber-attacks will soon be mandatory. Is your company ready'? Harvard Business Review, 19 April 2023 https://hbr.org/2023/04/reporting-cyberattacks-will-soon-be-mandatory-is-your-company-ready on 23 September 2023.
[209] Daniel M, 'Reporting cyber-attacks will soon be mandatory. Is your company ready'? Harvard Business Review, 19 April 2023 https://hbr.org/2023/04/reporting-cyberattacks-will-soon-be-mandatory-is-your-company-ready on 23 September 2023.

Striking a balance between incentivizing reporting and maintaining a strong cybersecurity posture is crucial, requiring thoughtful design and implementation to mitigate these drawbacks efficiently.

4.5.1 Possible solutions

To counter argue on the points of under-reporting or selective reporting, strict and exhaustive required standards of reporting with very little scope for ambiguity should be implemented. Performance-based liability caps evolving as per the severity and impact of the cyber incidents may be introduced and implemented to encourage accurate reporting while discouraging intentional under-reporting.

Continuous monitoring and compliance checks could also maintain an important driver to help cushion the perceived decline of motivation towards robustness of cybersecurity measures.[210] This is to assure organizations actively invest and uphold comprehensive cybersecurity defenses, in light of the possible outcomes for failing to do so.

Collaboration with regulatory bodies also helps take care of legal and regulatory challenges associated with the limited liability clauses.[211] Regular dialogues can make them refine regulations up to a point where they can easily align with the evolving cybersecurity needs such that there is a balance in legal framework.[212]

At the same time, transparency and accountability measures play a pivotal role, with companies benefiting from limited liability be required to publish aggregated reports on cyber incident reporting.[213] This will build trust among stakeholders and prove attempts at being responsible for such actions.

---

[210] Daniel M, 'Reporting cyber-attacks will soon be mandatory. Is your company ready'? Harvard Business Review, 19 April 2023 https://hbr.org/2023/04/reporting-cyberattacks-will-soon-be-mandatory-is-your-company-ready on 23 September 2023.

[211] Barrachin M, Pipikaite A, We need a global standard for reporting cyber-attacks, Harvard Business Review, 6 November 2019, https://hbr.org/2019/11/we-need-a-global-standard-for-reporting-cyber-attacks on 15 November 2023.

[212] Barrachin M, Pipikaite A, We need a global standard for reporting cyber-attacks, Harvard Business Review, 6 November 2019, https://hbr.org/2019/11/we-need-a-global-standard-for-reporting-cyber-attacks on 15 November 2023.

[213] Daniel M, 'Reporting cyber-attacks will soon be mandatory. Is your company ready?' Harvard Business Review, 19 April 2023 https://hbr.org/2023/04/reporting-cyberattacks-will-soon-be-mandatory-is-your-company-ready on 23 September 2023.

Public awareness campaigns could be very instrumental in influencing responsible cybersecurity practices by teaching the consumers about the measures in place and the role that limited liability plays towards honest reportage.[214] Public-private partnerships could also be implemented to encourage collaboration of companies, law enforcement, and cybersecurity experts thereby promoting information sharing and strong cybersecurity measures.[215]

By tailoring these solutions, lawmakers and industry stakeholders can strike a balance between incentivizing reporting and maintaining a strong cybersecurity posture thereby fostering a culture of responsibility, accountability and trust in the cybersecurity environment.

4.6 Conclusion

What the interaction of legal incentives, limited liability, and possible disadvantages of limited liability communicates is the need for and importance of a clause on liability protection that provides an inducement towards reporting cybercrimes. These are legal incentives recognized as potent instruments in the analysis of law and structure of regulation which try to promote positive action within a legal framework. However, the cons such as the temporary duration of compliance caused by incentives reflect the requirement of an improved approach. The comprehension of liability protection and the importance that it bears in general points out a critical necessity for a mechanism that voluntarily protects institutions in sharing information on the occurrence of cyber incidents. Liability protections as an incentive, fosters cooperation and reporting in several organizations targeted for various cyber-attacks. Confidence of broad liability protections when reporting cyber incidents would be significant to building mutual confidence and cooperation as a key building block of national resilience. Examining existing legislation such as the Critical Infrastructure Act of 2022 and the Cybersecurity Information Sharing Act of 2015 evidences the incorporation of a liability protection clause. Such a clause provides an important protective layer to the reporting entities as they are strictly prohibited from any sorts of legal actions in a direct connection with the act of reporting about the facts conveyed to them and proper disclosure. The potential drawbacks including underreporting, decreased investment on cybersecurity with regard to the limited liability clause necessitate careful

[214] Bidgoli M, Grossklags J, 'End user cybercrime reporting: what we know and what we can do to improve it', IEEE International Conference on Cybercrime and Computer Forensics, Vancouver, Canada, 2016, 6.
[215] Barrachin M, Pipikaite A, We need a global standard for reporting cyber-attacks, Harvard Business Review, 6 November 2019 https://hbr.org/2019/11/we-need-a-global-standard-for-reporting-cyber-attacks on 15 November 2023.

consideration. There should be a primary focus on maintaining a fine balance between incentivizing reporting and at the same time assuring a strong cybersecurity posture. While a limited liability clause could mitigate some of the risks, thoughtful design and implementation are required to address potential unintended consequences. A well-crafted liability protection clause is not just called for but also an indispensable provision that will help foster a culture of open and honest reporting of the same. It provides a vital element for a balanced and effective approach to cyber threat, which promotes the sharing of information without fear of overburdening legal recourse, adding to collective resilience against cyber threats.

5.0 Conclusion

5.1 Assessing the viability and efficacy of a limited liability clause in Kenya

The efficacy of the limited liability clause hinges on its ability to strike a balance between incentivizing cyber incident reporting and maintaining accountability and transparency within the cyber security realm. By providing legal protections and incentives for organizations to report cyber threats promptly and transparently, the clause can play a pivotal role in enhancing cyber incident response capabilities and fortifying the country's cyber security posture.

In framing a limited liability clause within the legislative framework, several key considerations must be addressed. The clause should clearly define the scope of liability limitations applicable to organizations reporting cyber incidents, outlining the types of incidents covered and the extent to which liability is restricted. This definition should be comprehensive yet precise to avoid ambiguity and ensure consistent interpretation and application.

Moreover, the clause should incorporate provisions for incentivizing cyber incident reporting, such as offering immunity from certain civil or for organizations that adhere to reporting requirements in good faith. This incentive mechanism is crucial for fostering a culture of transparency and cooperation among stakeholders, encouraging proactive engagement in cyber security efforts.

Furthermore, the limited liability clause should incorporate safeguards to prevent abuse or misuse of immunity privileges like selective reporting. It should include mechanisms for verifying the authenticity and severity of reported incidents, as well as penalties for organisations found to have submitted false or misleading information.

A limited liability clause is beneficial for both businesses and the overall cyber security ecosystem. With effective enforcement, stakeholder engagement and continuous evaluation there may be improved incident response and ultimately enhanced cyber security resilience. A limited liability clause provides legal protection to organizations that promptly report cyber incidents, thereby encouraging transparency and collaboration in addressing cyber security threats. This protection can alleviate concerns about the financial risks associated with cyber incidents, encouraging organizations to invest in robust cyber security measures. . Implementing a limited liability clause also helps safeguard critical infrastructure by encouraging proactive risk

management and incident response practices among infrastructure operators and service providers. This ultimately enhances the overall cyber resilience of critical infrastructure, businesses, and individuals within the country.

5.2 Summary of findings

There are various tactics utilized by cybercriminals to carry out cyber-crime. With the evolving and adaptive nature of cyber threats, cybercrime has experienced a notable increase. This rise has been attributed to cyber security gaps and inefficient cyber security policies, among other reasons. The cyber security gaps include the reluctance of individuals and organisations to report cyber-crime due to fear of negative publicity and lack of awareness. While these barriers hinder organizations from reporting cyber threats, there are benefits that could accrue, such as early threat mitigation or even building of trust with customers, investors and partners. In order to encourage reporting and improve the country's overall cyber security posture, a limited liability clause could be incorporated into the CMCA to incentivize reporting by organisations. With the implementation of a limited liability clause there's the possibility of drawbacks like selective reporting. However, with a well-crafted provision and effective enforcement, a culture of accountability and transparency may be promoted.

5.3 Recommendations

In light of the increasing frequency and severity of cyber-attacks in the country, it is imperative to take proactive measure to bolster our defenses in cyber security. As such, the study sets out to provide recommendations to the legislature, courts, researchers and the National Computer and Cybercrimes Coordination Committee to address the urgent need for cyber-incident reporting.

This study recommends that the legislature initiates the amendment of a comprehensive provision, with regards to the relevant Act (CMCA), incorporating a limited liability clause. This provision ought to provide clear guidelines as to the application of the liability protection in the event of reporting of cyber incidents by organisations.

At the same time, courts ought to be prepared to apply and enforce the relevant provision and Act in its entirety in consistently and judiciously. This way courts are able to establish precedents thereby contributing to the growth and development of cyber security jurisprudence.

The National Computer and Cybercrimes Coordination Committee should take a proactive role in ensuring the inclusion of a limited liability clause in the cyber security legislation. This could be by providing technical expertise. Additionally, the Committee could organize training and capacity building sessions for the judiciary, law enforcement agencies, members of the public and other relevant stakeholders in order to enhance their understanding on cyber security issues and the law surrounding cyber-incident reporting among other cyber security measures.

Lastly, this study recommends researchers to conduct studies to assess the possible impact of a limited liability clause on cyber incident reporting rates in Kenya. This could be by carrying out an analysis of the surveys, reports, case studies and interviews with stakeholders.

BIBLIOGRAPHY

Books

March J and Simon H, 'Organizations' John Wiley and Sons, New York, 1958.

Book Chapters

Davis J, 'Expected Utility Theory' in Mongin P (ed) *The handbook of economic methodology*, Edward Elgar Publishing, Cheltenham England, 1998.

Shinder D, 'Understanding network intrusions and attacks' in Tittel E (ed) *Scene of the cybercrime*, 1ed, Syngress Publishing, Massachusetts, 2002.

Journal Articles

Amitai E, 'The private sector: a reluctant partner in cyber security' *Georgetown Journal of International Affairs, 2014, International Engagement on Cyber IV*, 2014, https://www.jstor.org/stable/43773650 on 26 December 2022.

Amitai E, 'The bankruptcy of Liberalism and Conservatism' 128 *Political science quarterly* 1, 2013.

Healey J, 'Who's in control: balance in cyber's public-private sector partnerships' 18(3) *Georgetown Journal of International affairs*, 2017.

Swinhoe D, 'Why businesses don't report cybercrimes to law enforcement' Computer Security Online, 20 May 2019 https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html on 20 February 2023.

Friedman M and Savage L, 'The Utility analysis of choices involving risks' 56(4) *Journal of Political Economy*, 1948.

Tversky A, 'Additivity analysis of risky choices' 75(1) *Journal of Experimental Psychology*, 1967.

Tversky A, 'A critique of expected utility theory: Descriptive and Normative considerations' 9(1) *Erkenntnis Journal*, 1975.

Harrison G, 'Expected utility theory and the experimentalists' *Physica-Verlag HD*, 1994, https://link.springer.com/chapter/10.1007/978-3-642-51179-0_ on 3 March 2023.

Mosteller F and Nogee P, 'An experimental measurement of utility' 59(5) *Journal of Political Economy,* 1951.

Tversky A, 'The intrasivity of preferences' 76(1) *Psychological Review*, 1969.

Amitai E, 'Cyber security in the private sector' 28 *Issues in Science and Technology* 1, 2011.

Yadron D, 'Companies wrestle with the cost of cyber security' *The Wall Street Journal*, 2014 https://www.wsj.com/articles/no-headline-available-1393371844 on 8 March 2023.

Gordon L, Loeb M and Lucyshyn W, 'Cyber security Investments in the private sector: The Role of Governments' *Georgetown Journal of International Affairs,* 2014 https://www.jstor.org/stable/43773651 on 7 March 2023.

[1] Robinson N, 'Information sharing for Cyber-Security: Evidence from Europe' *Asan Institute for Policy* studies, 2013 https://www.jstor.org/stable/resrep08108 on 7 March 2023.

Huang K, Siegel M, Madnick S, 'Systematically understanding the cyber-attack business: A survey' 51 *Association for Computing Machinery Surveys* 4, 2018.

Hynds L, 'Hacker cracker' 149 *Royal Society of Arts Journal* 5500, 2002.

Bossler A, Berenblum T, 'New directions in cybercrime research' 42 *Journal of crime and justice* 5, 2019.

Katyal N, 'Criminal law in cyberspace' 149 *The University of Pennsylvania* 4, 2001.

Nurse J, 'Cybercrime and you: how criminals attack and the human factors that they seek to exploit', The Oxford Handbook of Cyberpsychology, 2018 https://arxiv.org/abs/1811.06624v1 on 9 September 2023.

Katyal N, 'Criminal law in cyberspace' 149 *The University of Pennsylvania* 4, 2001.

Agrafiotis I, Nurse J, Goldsmith M, Creese Sadie, Upton D, 'A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate' 4 *Journal of Cybersecurity* 1, 2018.

Buchanan T, Whitty T, 'The online dating romance scam: causes and consequences of victimhood' 20 *Psychology, Crime & Law* 3, 2013.

Craigen D, Diakun-Thibault N and Purse R, Defining cybersecurity, 4 *Technology Innovation Management Review* 10, 2014.

Peslak A, Hunsinger S, What is cybersecurity and what cybersecurity skills are employers seeking? 20 *Issues in Information Systems* 2, 2019.

Barrachin M, Pipikaite A, We need a global standard for reporting cyber-attacks, Harvard Business Review, 6 November 2019 https://hbr.org/2019/11/we-need-a-global-standard-for-reporting-cyber-attacks on 15 November 2023.

Emad A, Why motives matter: reframing the crowding out effect of legal incentives, 123 *The Yale Law Journal* 4, 2014.

Promberger M, Marteau T, When do financial incentives reduce intrinsic motivation? Comparing behaviors studied in psychological and economic literatures, 32 *Health Psychology* 9, 2013.

Boyne G, Hood C, Incentives: new research on an old problem, 20 *Journal of Public Administration Research and theory* 2, 2010.

Daniel M, 'Reporting cyber-attacks will soon be mandatory. Is your company ready'? Harvard Business Review, 19 April 2023 https://hbr.org/2023/04/reporting-cyberattacks-will-soon-be-mandatory-is-your-company-ready on 23 September 2023.

Internet Sources

https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/reporting-cybercrime.html on 20 February 2023.

https://www.fsb.org/wp-content/uploads/FSSCC-1.pdf on 20 August 2023.

https://www.idx.us/knowledge-center/why-many-cyberattacks-are-never-reported> on 3 February 2024.

-<https://www.cisa.gov/stopransomware> on 3 February 2024.

https://www.techtarget.com/searchsecurity/definition/password-cracker on 2 January 2024.

Mackay J, 'The importance of security incident reporting' Metacompliance, https://www.metacompliance.com/blog/cyber-security-awareness/the-importance-of-security-incident-reporting on 17 September 2023.

Gallant B, 'Why do SMBs neglect cyber security'? LinkedIn, 8 October 2023, -<https://www.linkedin.com/pulse/why-do-smbs-neglect-cyber-security-brett-gallant#:~:text=Misconception%20of%20Not%20Being%20a,easier%20and%20less%20protected%20targets> on 10 February 2024.

Dinha F, 'The effects of cybercrime on small businesses' Forbes, 11 May 2023 - <https://www.forbes.com/sites/forbestechcouncil/2023/05/11/the-effects-of-cybercrime-on-small-businesses/?sh=7ee16cfb2f68> on 10 February 2024.

https://www.law.cornell.edu/wex/incentive#:~:text=An%20incentive%20is%20a%20reason,financial%20subsidies%2C%20or%20tax%20provisions on 16 November 2023.

https://www.fsb.org/wp-content/uploads/FSSCC-1.pdf on 22 September 2023.

https://www.confidentialitycoalition.org/about/cyber-incident-reporting-principles/ on 23 September 2023.

Reports

Communications Authority Kenya, *Cyber security report* 2022.

Serianu, *Kenya cyber security report*, 2015.

National computer and cybercrimes co-ordination committee, *Kenya Cyber security strategy*, 2022.

National Collaborating Centre for Mental Health, *Self-harm: the short-term physical and psychological management and secondary prevention of self-harm in primary and secondary care*, 2004.

Serianu, *Local perspective on data protection and privacy laws*, 2020.

National Kenya Computer Incident Response Team – Coordination Centre, October -December cybersecurity report, 2022.

National Kenya Computer Incident Response Team – Coordination Centre, January- March cyber security Report, 2023.

National Kenya Computer Incident Response Team – Coordination Centre, April- June cyber security report, 2023.

National Kenya Computer Incident Response Team – Coordination Centre, October -December cyber security Report, 2023.

Serianu, Achieving cyber security resilience: enhancing visibility and increasing awareness, 2016.

Newspapers

Obura F, 'Kenya worst hit in East Africa by cybercrime,' The Standard, 2017, https://www.standardmedia.co.ke/article/2001235820/kenya-worst-hit-in-eastafrica-by-cyber-crime 2017.

Cierra P, 'Silent threat; FBI warns against trend of not reporting cyber attacks' WTHR, 11 August 2022 https://www.wthr.com/article/news/investigations/13-investigates/silent-threat-fbi-warns-against-trend-of-not-reporting-cyberattacks-ransomware/531-6cbee4c4-c23a-4d13-af20-ffb2fe6aa3a4 on 2 January 2023.

Frankline S, 'This is why Kenyan firms are vulnerable to cyber-attacks' The Standard, 23 May 2017 https://www.standardmedia.co.ke/business/sci-tech/article/2001240803/this-is-why-kenyan-firms-are-vulnerable-to-cyber-attacks on 13 January 2023.

Karabus J, 'JP Morgan must face suit from ray-ban maker after crooks drained $272m from accounts' The Register, 6 January 2023 https://www.theregister.com/2023/01/06/jp_morgan_lawsuit_essilor/ on 14 January 2024.

Musau D, 'Kenya hit by record 860 million cyber-attacks in 2023' Citizen Digital, 4 October 2023 -<https://www.citizen.digital/news/kenya-hit-by-record-860-million-cyber-attacks-in-2023-n328649> on 11 February 2024.

James K, 'How legal loopholes are hurting Kenya's cybercrime fight' Business Daily Africa on 24 February 2022 How legal loopholes are hurting Kenya's cybercrime fight - Business Daily (businessdailyafrica.com) on 20 August 2023.

VT OMNES
VNVM SINT