INTERNET FINANCIAL CRIME SECURITY PREVENTION AND CRIMINAL LAW REGULATION OPTIMIZATION PATH

[1]MAO XINXIN, [2]HANNA AMBARAS KHAN, [3]SUHAIMI AB RAHMAN

[1]School of Business and Economics, Universiti Putra Malaysia, Jalan Universiti 1, 43400 Serdang, Selangor, Malaysia.gs64631@student.upm.edu.my

[2]Senior Lecturer, School of Business and Economics, Universiti Putra Malaysia, Jalan Universiti 1, 43400 Serdang, Selangor, Malaysia. hanna@upm.edu.my

[3]Associate Professor, Department of Management and Marketing, Faculty of Economics and Management, Universiti Putra Malaysia, Jalan Universiti 1, 43400 Serdang, Selangor, Malaysia. suhaimiabrahman@upm.edu.my

Abstract: *Since the advent of the Internet, Internet and finance are becoming more and more closely integrated. In 2014, the banking industry paid around $65 billion in regulatory penalties, with misbehavior and anti-financial crime failures acting as key prosecution justifications. Many financial institutions are finding that it is difficult to properly handle growing requirements with their current processes and infrastructure, leading to significant increases in associated operational expenses. Recent improvements in data analytics, which allow a speedier analysis of larger, more thorough, and more diversified data sets, appear to have the potential to ease some of the key pain points in this context. This paper investigates the rise of Big Data in this sector, concentrating on use cases where advanced analytics is presently being applied, as well as its long-term potential.*

Keywords: *Cybercrime, Internet Financial Crime, Legislation, Criminal Law, Big Data*

INTRODUCTION

Cybercrime is a crime in which a computer is used to commit a crime such as hacking, spamming, phishing. Cybercriminals use the internet and other forms of computer technology to get access to people's private information, whether it be financial, personal, or otherwise. Criminals that commit these activities over the internet are known as "hackers." Many people have fallen victim to identity theft, hacking, and malicious software, and despite attempts by law enforcement to stop its spread, the problem persists. Inscrutable security, which uses a unified system of software and hardware to authenticate all information accessible through the Internet, is one of the most successful strategies for deterring burglars and securing critical information. Security software is used by many people and companies to prevent hackers from accessing their systems.[1] Even more concerning is the fact that many countries seeking to enact e-crime laws imperil society and individuals. This is because getting electrical devices has never been easier thanks to advances in IT.[2]

Factors that Lead to Cybercrime: When it comes to making money, cybercriminals are always on the lookout for the quickest and easiest route possible. They hack into the systems of the affluent or the institutions that handle big quantities of money, such as banks, casinos, and financial organisations. Such criminals are difficult to arrest. The outcome is a worldwide increase in cybercrime. Computers are vulnerable, thus rules must be put in place to keep them safe from hackers. Some potential causes of computer insecurity include[3]:

[1] ACLU (American Civil Liberties Union) (2016) Statement of Concern About Predictive Policing by ACLU and 16 Civil Rights Privacy, Racial Justice, and Technology Organizations, 31 August. URL (accessed 4 September 2019): https://www.aclu.org/other/statement-concern-about-predictive-policing-aclu-and-16-civil-rights-privacy-racial-justice.

[2] Perakslis ED. Cybersecurity in health care. N Engl J Med. 2014 Jul 31;371(5):395–7. doi: 10.1056/NEJMp1404358.

[3] Claunch D, McMillan M. Determining the right level for your IT security investment. Healthc Financ Manage. 2013 May;67(5):100–3.

Simple to access : The complexity of today's technologies makes it difficult to ensure that unauthorised users cannot access a computer system. In order to bypass biometric security and penetrate firewalls, hackers may obtain access codes, retinal images, and high-tech voice recorders.

Capability to store data in a relatively small area : The computer is remarkable in that it can store data in a very little area. This facilitates the process of stealing information from other storage systems for the benefit of criminals.

Complicated : Computers rely on operating systems, which consist of millions of lines of code. Errors may happen at any time since the human intellect is fallible. Intruders in the cyber world take advantage of these weaknesses.

Evidence loss : Information related to the crime can be removed easily. Because of this, the process underpinning cyber-crime investigation has been paralysed by the pervasive and obvious problem of evidence loss.

Classifications of Cyber Crime[4]

Hacking: It's a simple term for sending malicious code to another device or system. To get access to private or sensitive information, hackers break into a user's computer. The thief uses a variety of programmes to break into a victim's computer, and the victim may not even realise that his system has been breached. In order to gain notoriety, which is then fuelled by hostile media attention, hackers often attack government websites. Many businesses use what's called "ethical hacking" to ensure their own network is secure.

Internet stalking: This is a kind of cyberbullying in which the target repeatedly receives unwanted texts or emails. In many cases, these stalkers are familiar with their targets yet prefer to conduct their harassment online. If they see that their cyberstalking isn't having any effect, they may resort to traditional stalking methods to further complicate their targets' lives.[5]

Digital vandalism: The term "computer vandalism" refers to acts of destruction committed against computers and data, which may have an impact on businesses. Computer vandalism often entails the creation of harmful software with the express purpose of causing damage, such as erasing data from a hard drive or stealing login credentials. While computer vandalism does not modify already-running programmes in any way, viruses do.

Infectious Programs: These are pieces of code that are designed to cause havoc on an online network. The software is used to break into a computer in order to steal data or information or to damage the system's programming.

Scam emails and phone calls: You've undoubtedly heard quite a bit about this crime, and you may have even received a fake phone call yourself. Vishing is short for "voice phishing," which describes this kind of attack. The perpetrator of this crime will contact you by email, text message, or phone call, pretending to be from your bank and asking about your cards or accounts. He either asks you to click on a link he provides or for sensitive information (such your ATM PIN, one-time password, or login details). You risk losing all the money in your account if you give them the details by mistake and trust them. Remember that your bank will never ask for personal information, and that you should never provide account details online or with a stranger.

The spread of false information through social media: It's not uncommon for hackers to utilise social media just to distribute false information concerning sensitive societal, religious, and government matters. People on social media are so fascinated by this that they accidentally spread the link or post of total strangers. Considering that sharing any anything that violates the law on social media is also considered cybercrime, this action may lead to serious legal repercussions for the user. Don't conduct any work on social media while pretending to be someone else; doing so might ruin your whole existence.

[4] Cyber Security Ventures, (2018). https://cybersecurityventures.com/hackerpocalypsecybercrime-report-2016/.

[5] Global Cybersecurity Index 2017, (2017). International Telecommunication Union (ITU), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

Internet marketplace for illegal goods (the "Dark Web"): When a criminal offers a person illicit firearms, drugs, contraband goods, or access to private information through an illegitimate internet marketplace, they may use bitcoin to execute the deal. It promotes terrorism and smuggling, both of which it discourages. Darknets and networks host content from the World Wide Web known as the Dark Web, which is inaccessible without special software, configuration, or authorization. For unlawful content, use this online search engine. If it were legal, everyone would avoid using it, but you'd be mistaken. Millions of people all across the globe use it, and that figure rises daily.

Constantly shifting policies and additional regulations are testing conventional methods of ensuring compliance:-

In 2014, Western banks were hit with over $65 billion in regulatory penalties, a 40% increase from 2013. While this may be a record fine, authorities have made it clear that they expect a dramatic change in industry behaviour and will have zero tolerance for any further compliance management lapses. Financial institutions are now expected to take a proactive and risk-based strategy to compliance rather than a checklist or just procedural one as a result of increased enforcement and supporting criteria quickly rising in severity and reach. Regulators are working to alter the company's culture and attitude toward compliance, but this is mostly a human resources issue at the execution level. However, it is causing substantial increases in operational overheads as organisations are compelled to cultivate enabling business activities and technical capabilities, boost process performance, and drive compliance-led decision making throughout the organisation.[6]

The standards for AML, CTF, and penalties are changing toward risk-based methods and outcome-based obligations:-

Those working in finance have always been responsible for combating financial crime. The earliest coordinated intergovernmental policy standards date back to 1990, with the first Financial Action Task Force (FATF) report addressing money laundering, and the bulk of developed markets have had their own laws in place for even longer. It is true that laws like the Bank Secrecy Act (1970) and the Money Laundering Control Act (1986) are still very relevant today.

Even while a sense of responsibility has always existed, the actual expectations placed on people have increased considerably in recent decades, and this trend is likely to persist rather than regress. During the 1980s and 1990s, narcotics and organised crime were the primary drivers of anti-money-laundering (AML) laws. The USA PATRIOT Act of 2001 was pivotal in this expansion in the fight against terrorist funding (CTF) in the 2000s. (The key difference is that here, legal funds are being used to bolster unlawful activity, as opposed to the opposite strategy of trying to legalise illegally obtained funds.) BNP Paribas' record $8.9 billion penalty in 2014 for breaches of US sanctions on Iran is indicative of current tolerance levels, highlighting the regulatory emphasis on maintaining adherence to financial and trade sanctions in recent years.[7]Among the changes introduced by the Fourth Money Laundering Directive (MLD4), published in June 2015, are stricter requirements for conducting Customer Due Diligence, a more explicit reference to tax offences, and new rules for dealing with politically exposed persons (PEPs).

However, subsequent regulations (such as MLD3, and expanded with MLD4) have shifted implementation attention to a risk-based rather than rule-based strategy to combating financial crime, which is expected to increase in both intensity and breadth. One could say that this represents a major change. This means that compliance or money laundering officers do not have the default stance of deferring to the 'rulebook' when executing policies, even though institutions do have more discretion in some areas of decision-making (for example, they are not required to immediately dismiss hazardous customers). Instead, businesses must recognise risks, learn how to deal with them, document their efforts, and accept responsibility for the outcomes of their decisions. It also suggests

[6] Aimee O'Driscoll (October 2, 2018), 100+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2018 EDITION], https://www.comparitech.com/vpn/cybersecurity-cybercrime-statistics-facts-trends/#Global.

[7] Kruse C, Frederick B, Jacobson T, Monticone D. Cybersecurity in healthcare: a systematic review of modern threats and trends. Technol Health Care. 2017;25(1):1–10.

that actual outcomes are more important than a company's compliance with detailed rules (although these remain critical as well). Therefore, compliance is now an inherent part of day-to-day operational operations and decision making, rather than a supervisory role relegated to the back office and driven by checkboxes. While the methods for striking a balance between risk and laws vary from country to country, a more outcome-based approach to regulation is gaining traction. The same holds true for the administration of financial crimes and compliance regulations, whether they pertain to consumer protection (like UDAAP in the US or TCF in the UK) or to more systemic conduct risk issues like the Libor rate-fixing scandal.[8]Because of this, controls-enabling technology platforms and solid management reporting are essential.

Technology solutions are a vital enabler of effective compliance management, even if many of these requirements are related to people, rules, and procedures. Case management and analytics solutions help operations staff with work prioritisation and volume/quality management, both of which fall within the purview of the compliance position. Notably, this is shown in the creation of "appropriate controls" as part of larger compliance programmes' implementation. Examples of such systems include those that impose information-gathering requirements (such as during origination procedures) or those that use automated monitoring and analytics to spot potentially suspicious activities and halt them in their tracks (by, for example, restricting transactions that violate risk-defined policies). More infrastructure is needed to develop "robust management reporting," which allows for the measurement and monitoring of risk/performance metrics at both the aggregated and granular levels, is up-to-date thanks to automated data collation/processing, is accessible, for example, through dynamic, business intelligence tools, and is traceable, for example, through the ability to track underlying supporting data and preparation workings.[9]

The need for ongoing checks and balances and regular evaluation of the success of the program suggests that the creation of accompanying technology platforms is an ongoing process. There is a growing need to use non-traditional data sources to improve the efficiency of detection and due diligence procedures; this is especially true for high-risk clients requiring deeper investigations. In addition to traditional internal bank transaction datasets (which lie at the core of most existing methods). These can increase the efficiency with which organizations identify and analyze identified hazards, while also allowing them to identify previously unknown threats.[10]

The rising price of operations is placing stress on conventional, piecemeal methods of problem solving. The impact of ever-increasing regulations has been enormous. Due to the need for a larger number of people to work in compliance and anti-financial crime roles, direct costs have increased. There have also been large outlays in areas like staff education and time away from other projects to deal with compliance issues. As an example, in 2014, HSBC said that it had hired 24,300 people specifically for risk and compliance, or around 10% of its overall staff. It was acknowledged that this had contributed significantly to the overall rise in operating expenses over the preceding three years, having climbed by a sixth during that time period (with most other functions conversely reducing costs). It was expected that this trend would go on throughout the year 2015. Although HSBC was subject to extensive regulatory oversight as a globally systemically important bank, it is not alone in facing difficulties of this kind; other financial institutions have faced similar situations.

There has also been and will continue to be a major investment in the necessary IT infrastructure to ensure compliance. More than half of the 500+ banks questioned aim to increase investment in the major compliance and anti-financial crime sectors in 2016, according to Ovum's ICT Enterprise Insights programme (a global primary research study undertaken in Q3 2015 with senior IT executives on IT expenditure intentions). As seen in Figure 1. Even yet, over 20% are still counting on a sizable (i.e.,

[8] Riazul Islam SM, Daehan K, Humaun Kabir M, Hossain M, Kyung-Sup K. The internet of things for health care: a comprehensive survey. IEEE Access. 2015;3:678–708.

[9] Brookman J. Protecting privacy in an era of weakening regulation. Harv Law Policy Rev. 2015;9:355–74.

[10] Angst CE, Block Es, D'Arcy J, Kelley K. When do IT security investments matter? accounting for the influence of institutional factors in the context of healthcare data breaches. MISQ. 2017 Mar 3;41(3):893–916.

over 6% spending) growth in this sector. Despite a significant rise in compliance spending after the 2008 financial crisis.

For many financial institutions, required investments like this have become a significant chunk of their IT budgets' potential game-changers. Therefore, effectively managing escalating compliance costs has emerged as a pressing business need. As a result, organisations are shifting their focus from managing compliance requirements one by one (i.e., treating each regulation as a separate project) to adopting a platform approach. Banks need to find methods that allow infrastructure to be utilised across existing and future needs since many of these demands have substantial commonalities across data sources, collation and preparation, analysis, and reporting requirements.[11]

Traditional data warehousing and BI approaches can't keep up with the need for rapidity, efficiency, and low cost:

Banks have extensive information demands spanning risk, compliance, finance, and business operations, therefore they are already familiar with traditional SQL-based analytic approaches. To create an analytical SQL database, typically a specialised data mart or a more general data warehouse, data must be extracted, converted, and loaded (ETL) from its source systems. This processed data is then queried for further analysis, report generation, or model construction to aid in operational decision making. Business intelligence tools like dashboards and visualisation engines have made the produced information more accessible across the firm via self-service and interactive portals; formerly, this would have been handled by a professional analyst. This technique is helpful in a wide range of situations, particularly when dealing with structured data, such as that found in most financial source systems (which tend to be transaction-centric). Risk, compliance, and financial operations all rely heavily on the accuracy and reliability of analytical results, which are often provided via this method. It is crucial to many risk management, fraud prevention, and compliance processes and will remain so.[12]

SQL data warehousing does have its challenges, however. As most institutions digitise their client interaction and business processes, they are faced with an increasing influx of data that is changeable in structure, yet these systems were not designed to handle such information. This includes the following:

Information created by machines, such as web and mobile activity logs, phone call detail records (CDRs), and network events.

Data that is less organised inside an organisation but is nevertheless important, such as contracts, emails, documents, speech, images, and videos; and Data collected through social media platforms and the internet (e.g., from Twitter, Facebook, or Google). There is a wealth of new data waiting to be mined from a wide variety of sources, but traditional SQL databases aren't well-suited to handling this data since their structure isn't fixed and often undergoes frequent updates. Extremely dynamic, differently organised data sources are increasingly critical for piecing together a complete picture of risk, and static ETL solutions would have a hard time keeping up. In practise, this means that analysts have only had access to a small fraction of these data sets in the past. Besides, data visibility (e.g., the ability to drill-down into lower levels) is often lost, since aggregated processed data is typically used to save processing time when querying large data sets, and underlying raw data is often discarded.

Larger data quantities or more intricate analyses will result in longer batch processing run times, illustrating the non-linearity of processing scalability. This means that users of analytics applications are frequently forced to make a trade-off between depth and breadth when using the usual SQL method. Analytics may be conducted more rapidly with larger data sets if tasks are kept basic,

[11] Namoğlu N, Ulgen Y. Network security vulnerabilities and personal privacy issues in Healthcare Information Systems: a case study in a private hospital in Turkey. Stud Health Technol Inform. 2013;190:126–8. [PubMed] [Google Scholar]

[12] Zarei J, Sadoughi F. Information security risk management for computerized health information systems in hospitals: a case study of Iran. Risk Manag Healthc Policy. 2016;9:75–85. doi: 10.2147/RMHP.S99908. doi: 10.2147/RMHP.S99908.

whereas rich, complex analytics can be performed if data amount is limited (or a long batch window is employed).[13]

Adapting to new data management practises and applying learnings into operations:-

The explosion of data from machine-generated and Internet-connected sources over the last five years has sparked a revolution in analytics, necessitating the development of new approaches to supplement or replace SQL-based query and analytics. These new technologies, frequently referred to as "Big Data," increase the breadth of data that can be covered and make possible other ways to storing and analysing data, such as programmed methods using languages like Java, Python, or R. These have the potential to expand analytics' scope to include all data, rather than just a part of it, and to provide better, more well-rounded insights at a lower cost. Real-time analytics, made possible by recent innovations like the Spark computing engine, has far-reaching consequences for how institutions may operationalize information.

More importantly, this time period has seen the development of cutting-edge analytics methods for use in business. Because of the flexibility with which institutions may combine new programming and SQL approaches, the process of implementation has become more manageable and convenient (with latter also evolving in response). Further, it is critical for financial institutions that best practises in data governance have finally caught up to meet legal and organisational requirements. It's still a young discipline, but it's maturing to the point where it can be used in large corporations to address pressing issues for companies.[14]

Compared to traditional methods, data lakes provide a more comprehensive framework for storing and using information.

Data storage and manipulation have been revolutionised by newer methods. Hadoop is the most well-known technology for allowing this use case, and the concept of a "data lake" is a great example of it in action. Businesses who have already gained Hadoop expertise, understand how to handle large data, and know what data should be kept might consider adopting the data lake implementation approach. The raw data is loaded into the platform and then stored using a highly scalable, open source distributed file system across large clusters of commodity servers, allowing for massively parallel computation (again, using commodity computing power) and supporting multiple access methods (e.g., batch, real-time, in-memory, streaming)(Figure 1) . There are several upsides to this:

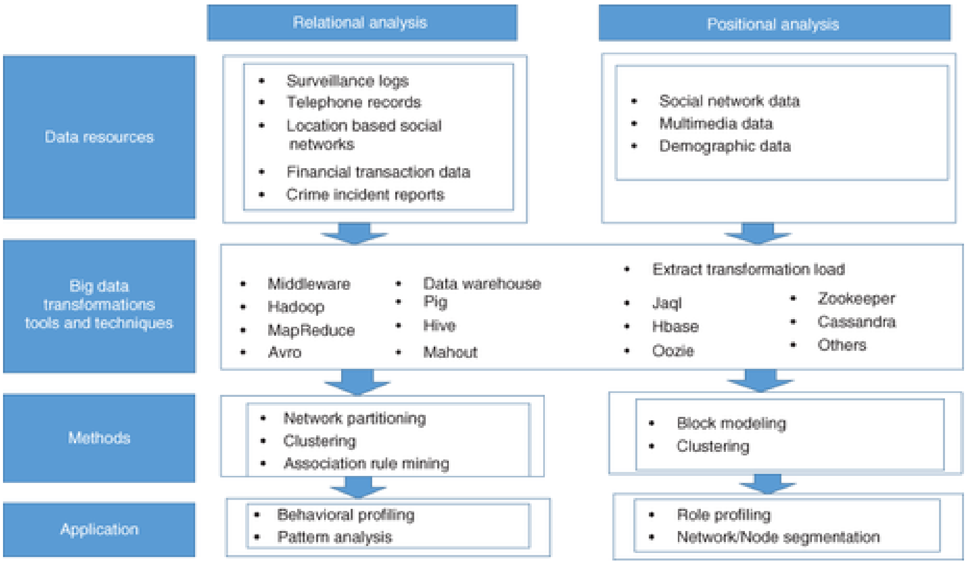

Figure 1: A big data management framework for security and criminal investigation.

[13] Laabes EP, Nyango DD, Ayedima MM, Ladep NG. Physician use of updated anti-virus software in a tertiary Nigerian hospital. Niger J Med. 2010;19(3):289–94.

[14] Humaidi N, Balakrishnan V. Indirect effect of management support on users' compliance behaviour towards information security policies. Health Inf Manag. 2018 Jan;47(1):17–27.

Cost savings in processing and storing data:

Storage costs are many orders of magnitude cheaper than those associated with high-end Storage Area Networks or Massively Parallel Processing architectures, which are typically used in data warehouses. This is because of the flexibility to employ commodity servers and directly connected commodity high-capacity drives.

Keeping all information safe:

Raw data, along with any processed or aggregated data, may be maintained since it is feasible due to the low cost and high scalability. Since raw data isn't always preserved using the SQL method, this approach simplifies data lineage dialogues while providing the most leeway for future studies.The capacity to store a wide variety of information -It is not necessary to organise data until it is being assessed or searched.Fresh data storage that can be adjusted on the go -Since there is no hard and fast storage format, data may be organised in any way necessary.By letting the data dictate the questions asked, businesses may be able to see correlations, trends, and patterns that might have otherwise gone undetected. It helps banks and other financial institutions spot and evaluate emerging risks in novel ways.[15]

Using a standardised system:

Hadoop is now more than just a MapReduce batch processing cluster. The current second version of the platform was designed to logically segregate clusters to enable different workloads to run concurrently, including batch, interactive, and real-time applications. A financial institution, for instance, may use analytics to react to incoming transactions in real time, with compliance/fraud operations teams doing interactive processing all day long and batch-oriented processing being used for more exploratory research at other times. Many batch modelling jobs may be run on the same cluster at once while you sleep. In this scenario, integrating new data is a considerably easier process than in the usual data warehouse and operational application approach, where the 'closed loop' between systems, if there is one at all, may be time-consuming.[16]

Data lineage and utility are the focus of new developments in data governance and user tools:

There are positives and negatives to the Hadoop data lake method. Internet companies like Google, Yahoo, and Facebook were the driving forces behind much of the early development of the Hadoop ecosystem. The focus was on capability rather than usability, manageability, or security; the focus was on running extremely data-intensive studies on log files for improving search indexes or ad placement, which required a high level of IT and technical expertise. Complex knowledge was required to create MapReduce applications. It was also deemed unnecessary to implement processes such regulating security, access, privacy, and audit duties since the platform was only known to a select group of experts and the analyses were conducted on somewhat irrelevant data.

While these concerns have always been important, they have taken on a greater urgency as Big Data has grown more commonplace in the workplace over the last five years, especially in highly regulated sectors like banking. Limiting access, selectively hiding or encrypting data, organising data transformation operations, and tracing provenance are all becoming possible with the help of new open source and commercial tools and capabilities. They're laying the groundwork for financial institutions to implement governed data lakes that support privacy (e.g., managing the protection of sensitive items of data, like account numbers, to ensure they're automatically masked) in order to uphold internal policies and comply with regulatory mandates.[17]

Hadoop may now function in tandem with the data warehouse, despite the fact that SQL and classic

[15] Sittig DF, Singh H. A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. Appl Clin Inform. 2016;7(2):624–32.

[16] Jalali M, Siegel M, Madnick S. Arxiv. 2017. [2018-05-07]. Decision making and biases in cybersecurity capability development: evidence from a simulation game experiment https://arxiv.org/abs/1707.01031 webcite.

[17] Jalali M, Kaiser J, Siegel M, Madnick S. SSRN. 2017. [2018-05-07]. The internet of things (IoT) promises new benefits—and risks: a systematic analysis of adoption dynamics of IoT products https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022111 webcite.

MapReduce-style programmatic analytics originated in different universes. Hadoop can now execute SQL queries against relational databases, and analytics conducted using MapReduce or Spark may provide output that can be placed into data warehouses for additional analysis. For instance, using Oracle Big Data SQL, users may write SQL queries in Oracle and have them executed on Hadoop, where the data is shown in virtual Oracle tables. Additionally, Hadoop's Oracle Loader for Hadoop allows for basic analysis of trends in real-time events to be undertaken, with the resulting data sets being able to be loaded into Oracle. This is made possible by the use of techniques like Spark Streaming. Using either method, businesses may take use of Hadoop's powerful processing capabilities and inexpensive, scalable storage in addition to the familiar query and analytic environments of data warehouses.

The impact of Big Data in fighting financial crime and maintaining regulatory compliance:

Many banks and other financial firms have already reaped the benefits of Big Data.Having been a "trend to observe" at the turn of the decade, then a "trend to experiment with," and finally a "trend to pilot," the adoption maturity of Big Data in banking has altered drastically over the previous five years. It is presently in production use at a number of financial institutions. Although progress toward full potential is still in its infancy, advantages are already being observed in practical applications.

It is becoming more common for banks to use sophisticated analytics for financial crime and compliance purposes. Despite significant developments in analytics over the last five years, adoption in the banking sector is still in its infancy. But it has progressed rapidly, and now most organisations are either using it or planning to start. Figure 3 depicts this trend, which is supported by data from Ovum's ICT Enterprise Insights programme indicating a substantial interest in advanced analytics for both anti-financial crime and compliance management purposes. About 20% of banks throughout the world have already invested in the manufacturing sector, led by the largest US banks but with significant representation across all three regions. An further 50% of financial institutions are now involved, split evenly between those in the most advanced testing phase and those actively planning for it. Interest in advanced analytics is high generally, with just 10–15% of banks worldwide and in the areas of financial crime and compliance showing little enthusiasm for the field. The regulatory pressure to adopt best practises in this field is reflected in this fact.

METHODOLOGY

More than 4478 interviews with CIOs and other high-level IT decision-makers are presented in ICT Enterprise Insights. More than 44 countries were represented in the survey, with research focusing on financial services, media and communications, government, and energy sector technological developments. Data was rigorously examined at a standard far above the norm in the industry. CIOs and other senior IT decision-makers who answered the Ovum survey were selected from pre-qualified panels. Where English was not widely spoken, interviews were conducted via the respondent's native language and completed online or over the phone. Ovum's primary research analysts and our sector experts reviewed the resulting data using Ovum's proprietary quality assurance tools.

Using alternative data sources to strengthen anti-fraud and cyber-security measures:-

Several financial institutions are putting Big Data analysis to use, such as by using new data sources to improve fraud detection and cyber-security, particularly in relation to online banking. Data collected throughout a user's time online is used to create a profile of their typical behaviour. Together with other anti-fraud methods (such checking whether the payee for the current payment instruction fits past patterns), this helps the bank spot suspicious activities and imposes extra security validation checks. This method uses machine-generated log data and message transmission from online sessions to learn about the paths users travel when navigating websites (i.e., clickstream data). All sorts of structured information, such user and page request details, make it challenging to assess using SQL methods because of the time and effort required to join the data together. However, when the Spark computing engine is used with Hadoop, doing a path analysis is straightforward, and it can even be done in real-time, enabling deployment even while work is in progress. Institutions might therefore proactively avoid problems rather than only responding to them.[18]

Institutions can now respond more quickly to regulators' demands thanks to the data lake concept:

A major financial institution in the United States is using the data lake concept to create a data platform to manage requests for information from regulators, particularly those requests associated with regulatory Matters Requiring Attention (MRA). In the past, such demands were dealt with on an as-needed basis, with relevant information being found, collected, reviewed, and reported for each demand. However, due to legal obligations for disclosing data provenance, providing granularity, and ensuring consistency across all requests, the effort became more time intensive and costly as the volume increased dramatically. Using Hadoop (and SQL) and an analytical workflow orchestration layer to manage data quality, processing, model execution, and reporting, the institution has created a data-as-a-service platform that can hold all relevant data. By taking this route, the institution may provide the regulator with reporting in the manner of business intelligence while also responding rapidly to questions regarding data lineage and modelling, making the process of responding to MRA-related information requests quicker, cheaper, and more controlled.

Working with full datasets in analyzing potential credit card fraud

Hadoop has also improved analytical performance in another domain: the detection of credit card fraud. Most financial institutions do basic real-time checks on transactions using predefined criteria, and then conduct more in-depth overnight batch analysis using sophisticated algorithms. These models will zero in on specific types of transactions (e.g., high-value transactions) and/or use a sample of data over time to find trends due to the large credit card volumes at top-tier banks, the need to control batch processing times (which may be long), and the cost. Since fraud is a rare event detection problem from a statistical modelling perspective (the number of fraud events is small relative to total transaction volumes), missing positive fraud instances may have a significant negative impact on model quality. It also suggests that some forms of fraud and/or trends in fraud may be missed.

Hadoop is being used by a major bank to analyse all of the daily transaction data, not just the transactions that occur in the front office. This has the benefit of reducing computing costs and analysing time while enhancing detection efficiency.

Committing fraud by professionals who are aware of and prepared to exploit fraud detection systems is another major obstacle to eradicating the problem. Therefore, financial institutions need to be aware of and adapt their behavioural models to low-latency events. A few financial institutions are looking into using Spark to enable real-time streaming of transactions with more sophisticated models, with the ability for models in the background to be continuously updated via machine learning.

As the need to mitigate insider malfeasance risks grows, the ability to integrate disparate data sets will become more important:

An important challenge for banks in ensuring compliance is that to various degrees employees will be aware of an institution’s controls and compliance processes. Given this knowledge, this means there is a danger that employees may be able to circumvent controlling systems to allow them to undertake undesirable activity, such as deliberate insider fraud or wider potential misconduct (which may be or may not be deliberately malicious). Banks can try to impose more stringent controls, but there alwaysneeds to be a balancing act between rigor of controls and ensuring that employee can actually conduct their core business activities as well.[19]

To address this, banks need to conduct analysis at multiple levels, to identify compliance or risk flags that might not be triggered at an individual transaction level. For example, analysis of sales activities might find that a financial advisor might sell a disproportionate amount of business in one product

[18] Jalali M, Rahmandad H, Bullock S, Ammerman A. Dynamics of implementation and maintenance of organizational health interventions. IJERPH. 2017 Aug 15;14(8):917. doi: 10.3390/ijerph14080917.

[19] Jarrett MP. Cybersecurity—a serious patient care concern. JAMA. 2017 Oct 10;318(14):1319.

set compared to an institution's average, which might suggest potential mis-selling activity even if individual compliance file-checks for the sold activity are passed. The challenge here is that an outlier in itself is no evidence that misconduct has actually occurred, and as misconduct is a relatively rare event, identifying and calibrating appropriate key risk indicators (KRIs) is problematic. This is particularly as any ensuing investigation may cause changes the flagged behavior, for example, the advisor may adjust their sales balance, without necessarily addressing the fundamental misconduct issue.

In this situation, being able work across multiple data types, rather than rely on pre-identified KRIs canbe highly effective for tackling misconduct risk. In particular, this includes being able to move beyond transaction data (of which insiders may have more knowledge) to include machine generated and unstructured data. This may include system access logs, phone call data, email, or chat data. These are often investigated post-event, to substantiate details of known misconduct, but use of Hadoop- based system provides the ability to store, link, and analyze across the data sets (along with KRIs) to provides a far more effective analysis to identify potential misconduct upfront (Figure 2).

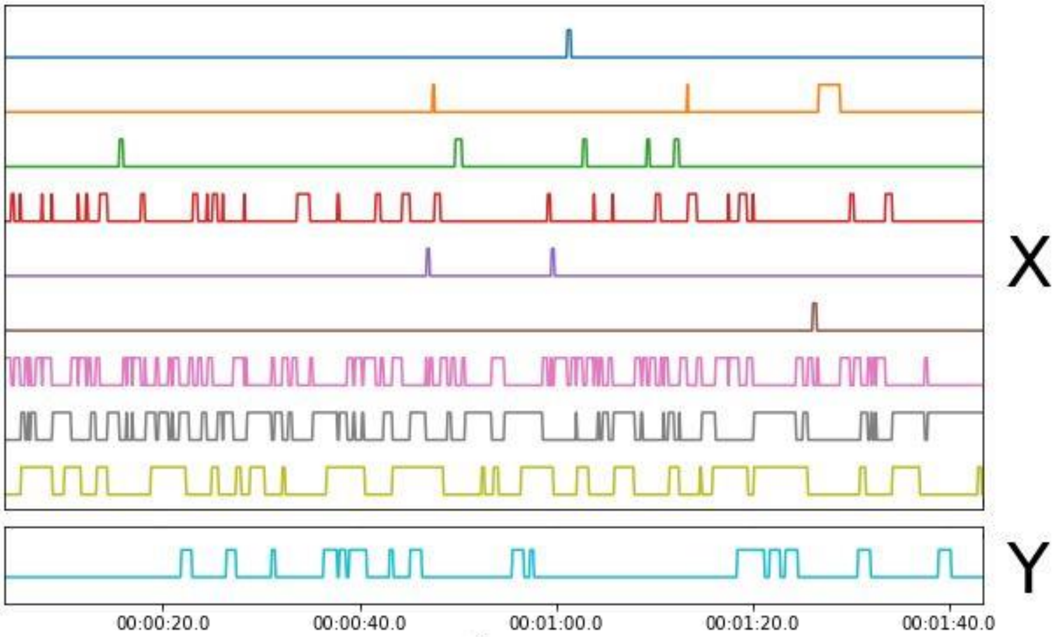

Figure 2: Binary visualisation

Reducing AML/fraud false positives through correlating activity across datasources

Similarly, the ability to combine multiple data sources and types offers significant advantages for reducing false positive levels in identifying suspect AML/fraud cases. Figure two in the first section ofthe paper highlighted the value of this, being a key driver of IT investment already to minimize the customer inconvenience it can cause. More effective detection also has major benefits from an operational cost perspective as reduces investigation time spent on genuine/legitimate activity.

It is also beneficial for regulators and anti-crime authorities; for example, it enhances the quality of Suspicious Activity Reports (SAR) that institutions have to submit when dealing with suspect cases. This has been a major pain-point for many countries with SAR volumes increasing significantly as regulators have reinforced requirements, particularly when a more rule-based approach has been adopted. Institutions have generally taking highly risk-adverse approach to avoid potential compliancebreaches, resulting in a high number of SARs for what is actually legitimate activity, with high volumesreducing their effective value to law enforcement agencies.

Use of new data sets, such as social network data or location data allows institutions to obtain additional correlating data to facilitate automated validation/analysis of identified suspect activity through transaction-based detection models. Such data can either be fed as extra inputs into initial monitoring processes, or used as a second detection layer where activity receiving certain risk scores can be re-screened using enriched datasets. Examples here include use social link analysis to understand any associations that may affect risk assessment, or location data from social networks/digital banking sessions to help assess whether a transaction is genuine. With this approach institutions can validate activity that would fall below the bar set for internal investigation, providing greater protection against potential undetected activity.[20]

External unstructured data becomes key for enhanced customer-due-diligence:-

Another key area where the Hadoop ecosystem will be beneficial is in meeting Know-Your-Customer requirements (KYC), particularly for clients where banks have identified the need for enhanced customer-due-diligence (CDD). This is typically required for clients identified as higher-risk based on factors such as size of funds, potentially suspect activity, location, or being a politically exposed person (PEP). Here banks having a greater duty of care to verify identify, establish source of funds, monitor transactions/activity, and track the customer/entity to ensure that CDD information is kept upto date. This may include both the client, and their family and known close associates (such as is required for PEPs).

While commercial supporting services do exist in this space, these are generally not regarded as sufficient by regulators, and banks need to ensure that they maintain current information on such clients, as well as react to negative events. This means that banks need to track news/media reports (potentially involving text, photos and video), social media, and relevant authority information (e.g., arrest warrants, criminal charges, or bankruptcy). Currently, this requires a high degree of manual KYC activity given much of this information is unstructured, potentially with inferred rather than directassociation to the client.

With the ability to work with unstructured data, using Hadoop as a platform will significantly improve both the efficiency and effectiveness of enhanced CDD operations. Institutions will be able to automate a far higher proportion of the required monitoring and analysis, allowing them to incorporateadditional external information sources and react faster to events. It also supports tools that allow patterns to be found and tracked across data types and relationships, such as social link analysis, which means that institutions can be more effective in identifying and understanding implications ofassociates.[21]

Legal safeguards:

The primary goals of preventive law are regulation and risk reduction. Preventive legislation in the context of cybercrime aims to either prevent cybercrime or, at the very least, mitigate the damage caused by the commission of a cybercrime (UNODC, 2013, 55). Cybersecurity laws (such as The Law of Ukraine on the Basic Principles Ensuring the Cyber Security of Ukraine, 2017) and data protection laws (such as the EU General Data Protection Regulation of 2016 and the African Union Convention on Cyber Security and Personal Data Protection of 2014, both of which are discussed in Cybercrime Module 10 on Privacy and Data Protection) aim to mitigate the effects of data breaches caused by criminals. The infrastructure of telecommunications and electronic communications service providers, for example, is such that it enables wiretapping and data preservation, thanks to the provisions of other laws that make it easier for law enforcement to detect, investigate, and prosecute cybercrime. Telecommunications service providers and equipment manufacturers in the United States are obligated by the Communications Assistance for Law Enforcement Act (CALEA) of 1994 (47 U.S.C. 1001-1010) to ensure that their services and products allow government agencies with lawful authorization (i.e., with the appropriate legal order) to access communications.

Proposed artificial neural network model (3-10-1) Neural network weight vectors are initially generated randomly at infinite values between -10 and +10. The total number of weights according

[20] Angwin J, Larson J, Mattu S, Kirchner L (2016) Machine bias: There’s software used across the country to predict future criminals. And it’s biased against blacks. ProPublica, 23 May. URL (accessed 4 September 2019): https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[21] Barabas C, Dinakar K, Ito J, Virza M, Zittrain J (2017) Interventions over predictions: Reframing the ethical debate for actuarial risk assessment. Cornell University. arXiv:1712.08238 [cs, stat].

to the parts of the neural network are given in the equation numbered (4). Training Regression and Test Regression performance values in 3-10-1 hidden layer numbers have come up more successfully when compared to other layer numbers (Figure 3).

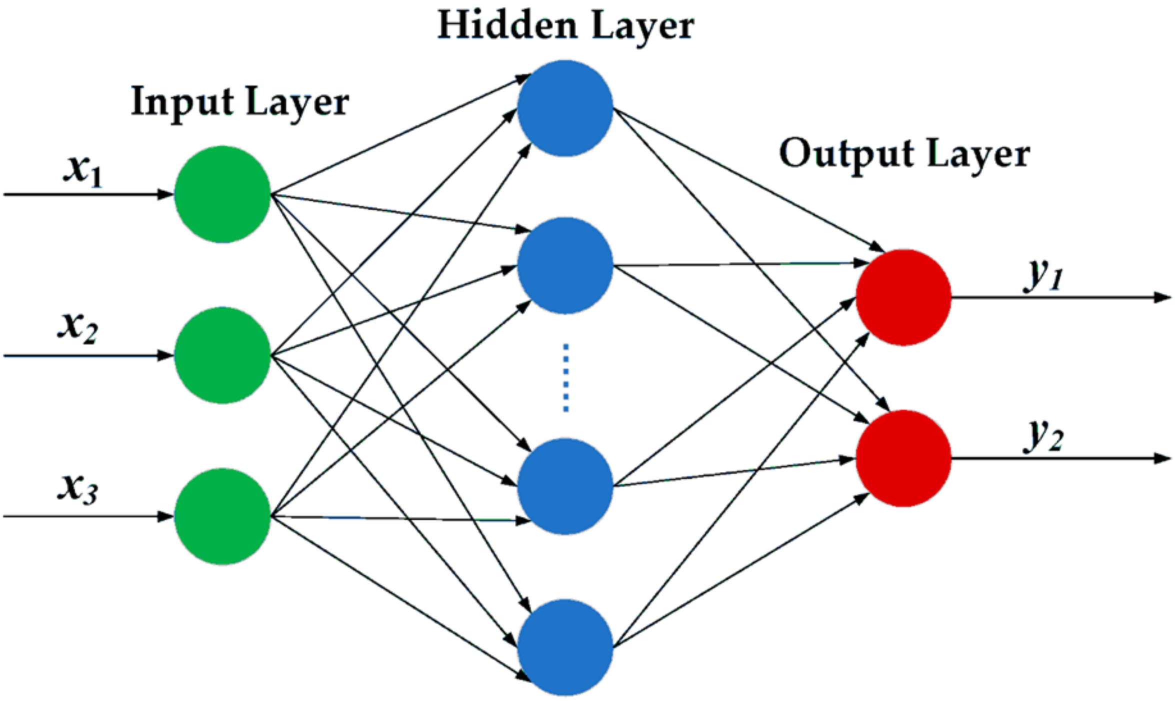

Figure 3: Training Regression and Test Regression performance values in hidden layer numbers

Thus, when the ANN model is being developed, a 3-10-1 network structure has been selected. The network designed in the 3-10-1 architecture has a total of 51 weight values. The weight number is calculated as follows: Total Number of Weights = (Number of Input Number of Hidden Layer Neurons) + (Number of Hidden Layer Neurons Number of Outputs) + (Number of Bias Number of Hidden Layer Neurons) + (Number of Outputs) (4) Total Weight = (3 10) + (10 1) + (1 10) + (1 1) = 30 + 10 + 10 + 1 = 51 (Figure 4). The ANN model is defveloped to determine the learning method for the purpose of determining anomaly or normality of the HTTP requests within the web application. The WAF software is developed on the .NET Framework platform using Microsoft Visual Studio 2015 toolkit, with the use of the C# ASP.NET programming language. The feedforward backpropagation algorithm is used in the training of the specified weights. The recursive algorithm is the most appropriate shape insertion technique designed to minimize a target function. The most commonly used target function is the MSE.s.[22]

[22] Birkhold MH (2018) Why do so many judges cite Jane Austen in legal decisions? Electric Literature, 24 April.

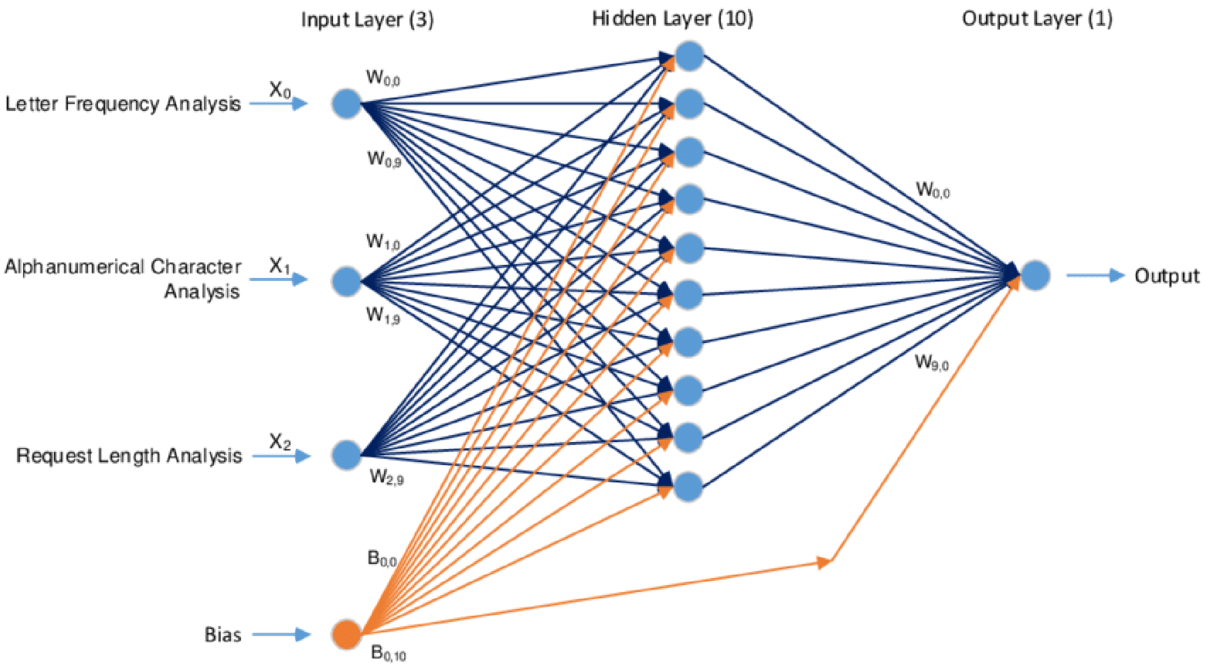

Figure 4: Calculation and assessmnet of weights

RESULTS AND DISCUSSION

A Strategy for Countering Cybercrime

Establishing multi-faceted public-private cooperation involving law enforcement, the IT sector, information security groups, internet providers, and financial institutions is crucial for efficiently combating cybercrime. Cybercriminals, unlike their real-world counterparts, don't engage in constant warfare to establish who's at the top of the criminal food chain. Instead, they support one another in their pursuit of professional growth and even assist one another in pursuing new possibilities as they arise. That's why conventional crime-fighting strategies are useless against cybercriminals.

Cross-Domain Solutions offers the optimal approach. Organizations may now use a single system, consisting of software and hardware, to verify the transmission and access of information across varying levels of security. This enables for unhindered communication and access to data inside a certain security classification, without risk of interception or accidental disclosure to users outside of that classification. This helps to maintain the security of the network and any connected systems.[23]

Visualization of Sorting data, Abstract processing of information flow. Vector database background. Filtering machine algorithms (Figure 5). To keep your accounts secure, it is recommended that you use unique passwords and user names for each one, and that you never write them down. Weak passwords are readily broken by techniques such as the Brute force assault, the Rainbow table attack, and others. Here are some measures you may take to keep your password safe from hackers.

[23] Brkan M (2017) Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond. SSRN Scholarly Paper, 1 August

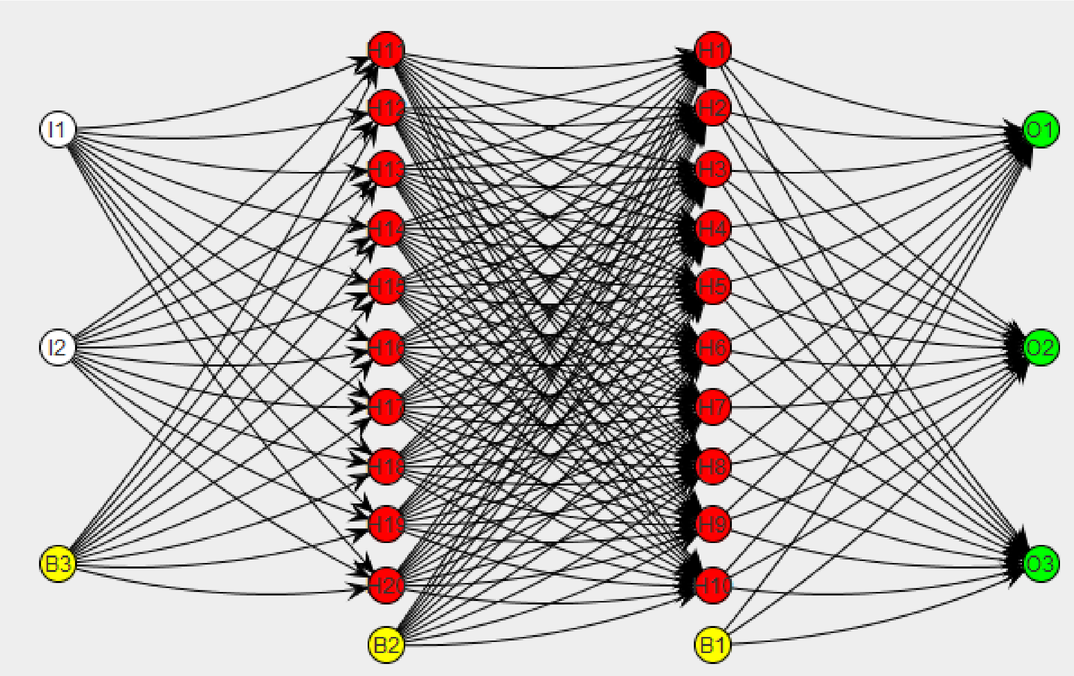

Figure 5: Visulaization of sorting data

Passwords that use keyboard patterns are becoming common. Examples: qwertyui

Applying simple permutations. Such as: Raju1990, February1990. Passwords are being left at their factory settings. e.g., "Welcome123," "Ravi123," etc. By using the same string of characters for both the password and the user name. Instances of the name Raju and its variants are provided as an example. Maintaining your Facebook, Twitter, YouTube, etc., accounts as private as possible shows that you're tech savvy and aware of the potential risks of public sharing. Verify that your safety measures are all set to the appropriate levels. Take caution with any personal details you provide online. The Internet is a permanent repository for information.

Be sure to keep your mobile devices safe: However, many people still don't realise that mobile devices can be infected with malware just like their desktop or laptop computers. Always use reputable sources to acquire software. Maintaining a current OS is also essential. Get anti-virus software and use a password to protect your screen. If not, if you lose your phone, or even if you just put it down for a second, anyone can access all of your private data. And if someone were to install malicious software on your device, they could monitor your every move using the GPS coordinates.[24]

Maintain data security: Encryption should be used to safeguard your most sensitive files, including tax returns and bank statements. A person can stay ahead of a hacker by learning about common scams and hacking techniques from the Internet. Well-known as a method of hacking, "fishing" can be avoided by learning about the most recent fishing attacks online. Maintain a secure environment by informing your community about these scams.

[24] Courtland R (2018) Bias detectives: The researchers striving to make algorithms fair. Nature 558(7710): 357 – 360.

Preserve Your Privacy When Using the Internet: It's better to err on the side of caution than to risk having your identity stolen online. You must exercise extreme caution before divulging any personally identifiable information online, including your name, address, phone number, and/or bank account details. When conducting financial transactions, etc., online, you should always check the site's security settings. Make sure you've got your social media privacy settings turned on.[25]

Update your system regularly: Implementing security updates and patches as soon as they are released is a great way to keep hackers at bay. By keeping your computer up-to-date, you reduce the likelihood that an attacker will be able to exploit security holes (vulnerabilities) in the programme.

Safeguard your computer with anti-virus and firewall programmes; these are just the bare minimums for keeping your data safe online. Firewalls and anti-virus software are two of the most important pieces of security software you can have. Typically, a firewall is the first line of defence for a computer. It regulates the kinds of programmes and people who can access your computer remotely. Imagine a firewall as a "policeman" who monitors all the data trying to enter and leave your computer over the Internet, only letting in communications that it has determined to be safe while preventing malicious attacks and other potentially harmful traffic.

CONCLUSION

In the modern, internet-based world, we simply cannot function without the aid of technological devices. Despite the fact that technology has many positive applications, it now poses serious risks to human safety. It's important to be cautious whenever using technology now, in case it leads you into the hands of cybercriminals. Since many nations do not have laws specifically addressing ecrimes, it is crucial that new laws be enacted to combat this global plague.

In light of this, it aimed to carry out the following in the near future: Construct new models for gauging the impact of population and technology on the main causes of e-crime in local and global political, cultural, economic, and sexual spheres. Make educated guesses about the relationships between variables by formulating hypotheses about them. To put the constructed models and hypotheses to the test, it's necessary to amass data from representative sample sources on a regional and national scale. Analyzing data with the right statistical tools.Do talk about the results and aims of the study. Finding a final verdict and settling on a course of action for further research. Taking all appropriate and required precautions to ensure the security of digital systems.

REFERENCES

[1] ACLU (American Civil Liberties Union) (2016) Statement of Concern About Predictive Policing by ACLU and 16 Civil Rights Privacy, Racial Justice, and Technology Organizations, 31 August. URL (accessed 4 September 2019): https://www.aclu.org/other/statement-concern-about-predictive-policing-aclu-and-16-civil-rights-privacy-racial-justice.

[25] Ferguson AG (2017) The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. New York: NYU Press.

[2] Perakslis ED. Cybersecurity in health care. *N Engl J Med.* 2014 Jul 31;371(5):395-7. doi: 10.1056/NEJMp1404358.

[3] Claunch D, McMillan M. Determining the right level for your IT security investment. *Healthc Financ Manage*. 2013 May;67(5):100–3.

[4] Cyber Security Ventures, (2018). https://cybersecurityventures.com/hackerpocalypsecybercrime-report-2016/.

[5] Global Cybersecurity Index 2017, (2017). International Telecommunication Union (ITU), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

[6] Aimee O'Driscoll (October 2, 2018), 100+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2018 EDITION], https://www.comparitech.com/vpn/cybersecurity-cybercrime-statistics-facts-trends/#Global.

[7] Kruse C, Frederick B, Jacobson T, Monticone D. Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technol Health Care*. 2017;25(1):1–10.

[8] Riazul Islam SM, Daehan K, Humaun Kabir M, Hossain M, Kyung-Sup K. The internet of things for health care: a comprehensive survey. *IEEE Access*. 2015;3:678–708.

[9] Brookman J. Protecting privacy in an era of weakening regulation. *Harv Law Policy Rev*. 2015;9:355–74.

[10]Angst CE, Block Es, D’Arcy J, Kelley K. When do IT security investments matter? accounting for the influence of institutional factors in the context of healthcare data breaches. *MISQ*. 2017 Mar 3;41(3):893–916.

[11]Namoğlu N, Ulgen Y. Network security vulnerabilities and personal privacy issues in Healthcare Information Systems: a case study in a private hospital in Turkey. *Stud Health Technol Inform*. 2013;190:126–8. [PubMed] [Google Scholar]

[12]Zarei J, Sadoughi F. Information security risk management for computerized health information systems in hospitals: a case study of Iran. *Risk Manag Healthc Policy*. 2016;9:75–85. doi: 10.2147/RMHP.S99908. doi: 10.2147/RMHP.S99908.

[13]Laabes EP, Nyango DD, Ayedima MM, Ladep NG. Physician use of updated anti-virus software in a tertiary Nigerian hospital. *Niger J Med*. 2010;19(3):289-94.

[14]Humaidi N, Balakrishnan V. Indirect effect of management support on users' compliance behaviour towards information security policies. *Health Inf Manag*. 2018 Jan;47(1):17–27.

[15]Sittig DF, Singh H. A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Appl Clin Inform*. 2016;7(2):624–32.

[16]Jalali M, Siegel M, Madnick S. *Arxiv*. 2017. [2018-05-07]. Decision making and biases in cybersecurity capability development: evidence from a simulation game experiment https://arxiv.org/abs/1707.01031 *webcite*.

[17]Jalali M, Kaiser J, Siegel M, Madnick S. *SSRN*. 2017. [2018-05-07]. The internet of things (IoT) promises new benefits—and risks: a systematic analysis of adoption dynamics of IoT products https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022111 *webcite*.

[18]Jalali M, Rahmandad H, Bullock S, Ammerman A. Dynamics of implementation and maintenance of organizational health interventions. *IJERPH*. 2017 Aug 15;14(8):917. doi: 10.3390/ijerph14080917.

[19]Jarrett MP. Cybersecurity—a serious patient care concern. *JAMA*. 2017 Oct 10;318(14):1319.

[20]Angwin J, Larson J, Mattu S, Kirchner L (2016) Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks. *ProPublica*, 23 May. URL (accessed 4 September 2019): https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[21]Barabas C, Dinakar K, Ito J, Virza M, Zittrain J (2017) Interventions over predictions: Reframing the ethical debate for actuarial risk assessment. *Cornell University*. arXiv:1712.08238 [cs, stat].

[22]Birkhold MH (2018) Why do so many judges cite Jane Austen in legal decisions? *Electric Literature*, 24 April.

[23]Brkan M (2017) Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond. *SSRN Scholarly Paper*, 1 August

[24]Courtland R (2018) Bias detectives: The researchers striving to make algorithms fair. *Nature* 558(7710): 357–360.

[25]Ferguson AG (2017) *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: NYU Press.