Academic Paper

Grayson Dunaway

Porcher

CPD494

4/21/2023

Introduction

The convenience and utility of mobile devices for everyday tasks, including communication, entertainment, and information gathering, have made them indispensable. Increases in mobile device usage correlate with increases in the prevalence of security threats. Information that might be used to steal someone's identity, money, or intellectual property is called "sensitive information," It is breached when it is accessed, stolen, or made public by those who shouldn't have access to it (Edwards et al., 2016). Data breaches increasingly focus on mobile devices because they store so much personal information and are easy prey for hackers due to their portability and constant connectivity. Concern over mobile data breaches is on the rise among consumers, businesses, and governments. McAfee predicts a 50% increase in mobile malware attacks in 2020, with the average data breach cost reaching $3.86 million at that time (IBM Security, 2020). The massive expense of data breaches affects a company's ability to function financially and the public's perception of that company.

This article aims to propose Purge, a mobile security application that will protect mobile devices from data breaches. This article will summarize Purge, its capabilities, and its operation to secure mobile devices. This article will also highlight the relevance of Purge as a breakthrough in mobile security that might help individuals and businesses alike avoid data breaches on mobile devices.

Overview of Purge, the mobile security application

Purge is a mobile security app that provides a foolproof defense against any data intrusion on your mobile device. Personal information, financial data, and intellectual property are among the types of data that this application safeguards on mobile devices by employing cutting-edge encryption algorithms and security measures. Apple and Google's mobile operating systems (iOS and Android) are supported. Thus, the app may be installed on just about any portable device.

Remote wiping, anti-malware protection, phishing prevention, and storage for sensitive information are just a few functions Purge offers to keep mobile devices safe. Users may safely save their passwords, credit card information, and other important data in the vault. Features like anti-phishing and anti-malware protect mobile devices from malicious attacks like phishing emails and malware downloads. If a user's mobile device is stolen or lost, the user can use the remote wipe feature to erase all data from the device.

Importance of the innovation

To prevent data breaches on mobile devices, Purge provides a comprehensive solution, making it a significant advancement in mobile security. Customers are protected in more ways than usual because of the program's robust security features, which are not standard on most smartphones. The ability of Purge to encrypt passwords, financial data, and intellectual property can help individuals and businesses avoid the pitfalls of identity theft and financial loss.

Safeguarding mobile devices against attacks that might compromise sensitive information is an absolute need, and Purge's anti-phishing and anti-malware technologies play a crucial role in this. With the increase of malware and phishing attacks on mobile devices, Purge fills a much-needed gap in security. And with Purge's remote wipe feature, you can rest easy knowing that if your mobile device ever gets lost or stolen, you may erase all of the sensitive information stored on it to prevent unauthorized access and data breaches.

Review of Literature

Definition and types of mobile data breaches

When confidential data stored on mobile devices like smartphones and tablets is accessed or exposed by unauthorized parties, this is known as a mobile data breach. Security may be breached in several ways, including the environment, apps, and network. Sensitive data stored on a mobile device is vulnerable if the device is lost, stolen, or accessed by an unauthorized party. Data like usernames, passwords, and phone numbers fall into this category. A poorly designed or programmed mobile app leaves itself vulnerable to unauthorized access or manipulation, a situation known as an "app-based security breach." With these vulnerabilities, hackers can access the app and steal data such as user login credentials, credit card numbers, and personal details (Seh et al., 2020). Hackers can snoop on a mobile device's data transmissions if they get unauthorized access to its network connection (through Wi-Fi or cellular network, for example). Login credentials, social security numbers, and credit card details are all examples.

Impact of mobile data breaches on Individuals and Businesses

Impact on individuals

Direct costs. Exposure to private information due to data breaches can cause serious harm to both individuals and businesses. This article explores the effects of mobile data breaches on individuals. Mobile data breaches can result in serious consequences for victims, including financial loss, identity theft, and invasion of privacy. For many people, data breaches can result in direct costs, such as legal fees, financial theft, and even extortion payments to attackers (Wang et al., 2019). Additionally, when the company's stock price declines following a data leak, customers who are stockholders could suffer immediate financial losses. Affected individuals could be forced to pay for credit monitoring on their dime if the breached organization does not provide adequate services.

Indirect costs. In addition to these direct costs, mobile data breaches can have several indirect costs for individuals. Data breaches can result in various negative consequences for individuals, including loss of time, wages, convenience, credit, increased prices, and emotional stress. Such incidents can be particularly inconvenient for consumers, often leading to switching services and consumer accounts. In a survey study by Wang et al. (2019), the median estimated cost of inconvenience resulting from a data breach was $500 per person. Moreover, individuals may suffer from credit loss or damage to their credit rating due to identity theft and fraudulent transactions that stem from stolen sensitive personal data. This can result in lost employment opportunities and financial income. The psychological impact of a data breach can also be significant, causing confusion, frustration, anxiety, depression, loss of self-confidence, and negative changes in perception. Such incidents can increase affected individuals' perception of vulnerability and harm, leading to negative outcomes.

Impact on businesses

Businesses in the present day depend heavily on technological advancements to help them function. However, this trust comes with the risk of inadequate security measures and commercial procedures, which may lead to significant monetary losses, damage to a company's brand, and legal repercussions (Wang et al., 2019). With each passing year, cyberattacks become more frequent and costly. Moreover, the global pandemic has caused changes in business operations, which has led to alterations in organizations' attack and risk profiles.

Financial loss. Cyberattacks frequently result in financial losses for businesses. Real costs associated with cyberattacks are easier to quantify (such as direct monetary expenditures). In contrast, intangible costs (such as damage to employee morale, customer goodwill, and the company's reputation) can be more difficult to pin down. Should this occur, it may be possible to assign a monetary value to intangible expenses that have not yet been assigned a market value. According to research by Perera et al. (2022), this can have far-reaching effects on a business's competitiveness in both the social and economic arenas. Data breaches, ransomware, persistent assaults, and lapses in computer security are just a few examples of cyber risks that can affect an organization. Equipment damage or theft results in repair or replacement costs, legal fees, and lost revenue that must be made up for during the downtime.

Reputation damage. Damage to a company's reputation, an intangible asset affecting all its stakeholders, is one of the most obvious effects of cyberattacks. Trust from customers and investors, as well as general perceptions of reliability and credibility, all play a role in an organization's overall reputation. A company's reputation and ability to compete can take a hit from a cyberattack, say Wang et al. (2019). Unfortunately, many businesses need more time to deal with these risks. Research conducted in the United Kingdom by Perera et al. (2022) found that more than 58% of businesses underestimated the potential damage a data breach may do to their operations. In addition, a survey of 599 businesses that had suffered a data breach found that 81% felt it had harmed their brand.

Legal consequences. Cyberattacks have consequences for businesses in the courtroom as well. In many countries, it is a legal need for businesses to protect the privacy of their clients and employees. Fines, lawsuits, and disciplinary action from regulators may come from failing to comply. In addition, companies may be held liable for disclosing customer and employee information, which might lead to costly litigation. Companies that do not take enough measures to protect their customers' and employees' personal data from cyberattacks may face severe legal consequences. Several countries have passed regulations and laws mandating businesses to protect private information. You might face fines, lawsuits, and other regulatory punishment if you don't follow the rules.

Furthermore, companies that suffer data breaches may be liable for losing customers' and employees' personal information. Legal costs, and those for hiring lawyers and settling disputes, can quickly add up when this happens. If businesses fail to protect private information, they may face criminal penalties.

Current mobile security solutions

Mobile antivirus software

Antivirus software for mobile devices, like those for computers, can detect and eliminate viruses from your smartphone or tablet. Antivirus software for mobile devices combines signature-based detection with behavioral analysis to identify and block malware before it can damage the device, providing real-time protection against existing threats and those that have yet to be discovered. Anti-theft features, which let users remotely lock or erase their device if lost or stolen, are one example of the supplementary features that mobile antivirus software may offer (Telo, 2019). Protect your online privacy and anonymity while using a virtual private network (VPN) service that is included with certain mobile antivirus packages. Similar to traditional antivirus software, mobile antivirus has its limitations. Limitations include a lack of protection against zero-day attacks and the use of system resources, among others. In addition, mobile antivirus software is prone to false positives and missing infections due to its signature-based detection approach.

In recent years, malware has become increasingly concerning due to the widespread use of cell phones for communication and internet activity. Mobile antivirus software, such as Purge, is essential in safeguarding mobile devices from this danger. While iOS has seen its fair share of malware attacks, Android is where the action is. Besides stealing sensitive information, malware may remotely control the device and impose unauthorized expenses on the user. The widespread usage of traditional signature-based antivirus software masks the fact that it cannot detect threats that have yet to be discovered. As Chen et al. (2015) suggested, one solution may lie in behavior-based detection methods. Companies operating online must establish safe mobile and wireless networks to protect their data from theft. This includes corporate and personal information such as text messages, addresses, photos, and GPS coordinates. Purge is a mobile antivirus application that offers comprehensive protection from current and emerging threats and features like anti-theft safeguards and virtual private network access.

Mobile device management solutions

Since more and more employees depend on their mobile phones and tablets to gain access to sensitive company data, MDM solutions are indispensable. Organizations may benefit from MDM (Mobile Device Management) solutions that help them monitor and secure their employees' Android phones, which are now the market leaders. Mobile device management (MDM) solutions allow enterprises to centrally control mobile phone policies and prohibit certain functions from preventing misuse and keeping GDPR compliance for data protection. Glowinski et al. (2020) estimate that the MDM market will be worth $3.94 billion by the end of 2019. Despite the advantages of MDM systems, finding the proper one might be difficult due to the wide variety of suppliers and descriptions of available features. To help with this, Gartner Inc. produced a magic quadrant study on mobile device management software, classifying vendors into "leaders," "visionaries," "challengers," and "niche" categories. While it provides some context, it may not consider the special needs of smaller and medium-sized businesses. Mobile device management (MDM) solutions are essential for businesses since mobile devices, compared to stationary equipment, cannot be monitored by the company or local administrators. Because of their limited security features, mobile devices are easier to hack. Using an MDM solution, you can control and protect your company's mobile devices, keeping sensitive information safe and preventing unauthorized users from accessing internal networks.

Successful mobile device management (MDM) systems safeguard sensitive company data and stop unauthorized users from accessing the internal network. Enrollment/configuration, distribution, authentication, instruction, and control/reporting are only a few of the essential procedures that make up the MDM architecture and must be carried out regularly to meet operational needs (Barthwal, 2016). Easy software updates, remote device management and monitoring, data backup and restoration, and password-protected logging and reporting to guarantee compliance are just a few of the many advantages offered by MDM solutions. Organizational data must be protected, and security risks associated with MDM systems must be managed. Data loss, software corruption, virus infection, manipulation, and natural disasters are all examples of such dangers. Purge solves these problems by providing a safe place to store sensitive information, safeguards against phishing and malware, and the ability to delete data remotely in the event of theft or loss. Implementing MDM solutions like Purge may help businesses better manage and secure their mobile devices and protect their most important data.

Two-factor authentication (2FA)

The use of two different authentication methods to gain entry to a protected account or network is known as two-factor authentication (2FA), and it is a reliable security solution. With this extra safeguard in place, hackers and data thieves will have a harder time getting through than they would with only a login and password. Two-factor authentication (2FA) options include text message verification, email verification, and authentication software that generates a one-time code. In addition to a username and password, many login processes now need a secondary authentication factor, often a device-generated unique code. An extra layer of security is provided because this code will become invalid after a certain time. Two-factor authentication (2FA) is becoming increasingly important as more and more people rely on online accounts and digital services. The Verizon 2021 Data Breach Investigations Report found that the most common type of cybercrime was the theft of credentials such as usernames and passwords (61% of all data breaches). Two-factor authentication (2FA) adds an extra layer of protection for access to accounts and other sensitive data that may be used to thwart assaults like these.

The Purge software provides many layers of protection on mobile devices. Features include two-factor authentication (2FA) to thwart phishing attacks and remote wipes so that data may be erased from a lost or stolen device. Organizations that must follow regulations like GDPR, HIPAA, and PCI-DSS will find this feature very useful. Two-factor authentication (2FA) can add an extra layer of security when securing highly sensitive information is needed. Two-factor authentication (2FA) has many advantages but involves extra steps, which may annoy certain users. The use of push notifications and biometric authentication has helped many organizations streamline their 2FA options. That two-factor authentication (2FA) is not foolproof is one of its flaws (Telo, 2019). The risk of hacking and data breaches is reduced significantly, but it is still possible for hackers to get access to user accounts through social engineering, phishing, or other techniques. We've included anti-phishing technology in Purge as an additional safeguard against scams.

Private vault and Remote wipe functionality

The frequency of mobile data breaches is raising the importance of mobile security. Protecting consumers and businesses from the fallout of mobile data breaches will become increasingly vital as mobile technology evolves. Purge's remote delete and safe vault are two examples of cutting-edge technology created in response to the increasing danger posed by mobile data breaches. The encrypted vault in Purge is a great way to protect sensitive data from hackers. It uses robust encryption techniques and security procedures to safeguard information from unauthorized access. Purge's remote delete features are another helpful tool for avoiding data breaches (Di Leom et al., 2016). In the event of a lost or stolen mobile device, the user can remotely delete any data stored on the device. This prevents sensitive information from falling into the wrong hands.

These cutting-edge tools are essential for reducing the harm of mobile data breaches, both to consumers and businesses. Direct effects of mobile data breaches include monetary loss and privacy violations, while indirect effects include missed time at work, income, and emotional stress. Businesses may suffer significant monetary loss, reputational damage, and legal repercussions due to data breaches. Improvements in mobile security are urgently needed to protect individuals and businesses from the fallout of lost or stolen mobile data. A mobile data leak may be avoided with the help of Purge's remote delete and encrypted vault. These products provide comprehensive protection for mobile devices, ensuring the safety of sensitive data and blocking unauthorized access. As mobile technology advances, there will be a growing need for cutting-edge mobile security solutions to protect sensitive information.

The Relation of the Innovation and Problem to Classes Outside of the Major

Some of the courses I have taken outside of my major have impacted the way I approached addressing the problem of data breaches as well as creating the innovation Purge. One course that was particularly helpful was Interdisciplinary Theory and Concepts (IDS 300W). This course focused on interdisciplinary research around a topic that involves your major. I chose to research "the most effective technologies to protect mobile devices from data breaches in 2023", which sparked the creation of Purge to address the issue of data breaches. The course emphasized the importance of solving problems using different perspectives from various disciplines. This is an important tool to have in the world of cybersecurity. It also showed me how to approach a situation that requires several solutions. IDS 300W played a big role in helping me address the complex issue of data breaches on mobile devices. While developing Purge, I incorporated different disciplines such as law, computer science, and cybersecurity. The discipline of law helped with the legal aspects of the application, computer science helped develop the code, and cybersecurity helped in creating the procedures and solutions to protect mobile devices from data breaches. The IDS 300W course taught me how to solve the complex issue of data breaches by integrating different disciplines into my innovation.

Another course that assisted with the innovation and the problem is Introduction to Interpersonal Communication (COMM 112R). This class taught me about different communication theories that helped with the development and promotion of Purge. One of the theories we discussed was about the importance of studying an audience. The skills I learned from this course allowed me to identify our target audience and understand their needs in order to make sure Purge is effective. Additionally, I learned about effective persuasive communication techniques in the course. This will be important in the promotion and marketing of Purge. The skills and knowledge I gained through taking COMM 112R have been quite useful in contributing to the success of Purge as a tool for protecting mobile devices from data breaches.

The other course that played an important role in this process was Introduction to Contemporary Business (BUSN 110). In this course, I learned about the business environment and how companies successfully function in the current economy. It made it easier for me to see the significance of Purge and how to maintain an edge over the competition. It was crucial to make sure Purge stood out from the competition and could add unique value to the market. My BUSN 110 course helped me understand how to identify if a business is successful and how to create a product that will meet the needs of consumers. The course also emphasized the importance of effective marketing and creating a strong brand identity, which is something I tried to implement in my idea for Purge. These are crucial aspects to make sure Purge is successful. BUSN 110 also played a significant role in shaping my understanding of business as a whole and provided me with the tools to address the problem of data breaches and develop the innovation Purge.

Elementary Statistics (STAT 130M) played an important role in developing the innovation Purge. The course taught me the skills to analyze data and draw insights from that data. This helped in identifying the prevalence of data breaches in mobile devices. I was able to gather data to confirm the necessity for an application like Purge using the tools and methodologies I learned from the course. Additionally, the course taught me how to make informed decisions based on data analysis, which has been very helpful throughout the developmental process of Purge. Additionally, I gained a strong foundation in probability theory which was crucial for me to understand the likelihood of a data breach happening and how Purge could reduce the risks of data breaches. In summary, my STAT 130M course played an important role in shaping my decision-making for Purge. Even though all of these courses are outside of the Cyber Security major, they still helped with the development and the process of innovation for the lack of security for mobile devices against data breaches.

Evaluating the Effectiveness of Purge

Regarding our innovation, there are multiple things that will help determine the effectiveness of the Purge. The first thing we will need to do is take a count of the number of users who have downloaded and used Purge. A lot of downloads indicate that our application is being accepted by users. We can evaluate Purge’s effectiveness by looking at our user engagement rates. We can measure this by tracking how often our users use Purge. What we will be looking at in order to track the effectiveness of Purge is the number of logins we have daily, how many people are using our two-factor authentication, as well as the number of active subscriptions. If our users are using Purge frequently, it will indicate that the users are actively using our security features to protect their mobile devices. Which shows that our application is successful.

I believe another way we can evaluate whether Purge is effective or not is by comparing the number of data breaches that have occurred on devices with Purge installed versus mobile devices that don't have Purge installed. If it shows that a lower number of data breaches occurred on devices with Purge installed, then this can show Purge's effectiveness in protecting mobile devices from data breaches. Customer satisfaction is another important thing that can be used to determine the effectiveness of Purge. This can be measured by conducting user surveys or analyzing our user's reviews. If our reviews are overwhelmingly positive, then that can indicate that Purge is successful in providing effective protection against data breaches.

Once Purge launches and is up for a few months we can use our revenue to determine the effectiveness of Purge. By looking at the revenue generated by Purge we can determine whether our application is successful or whether there is a need for it in the market. We can also determine whether we are meeting the needs of our customers by looking at whether were making a profit.

By looking at Purge's downloads, the user engagement rate, the data breach rate of devices with and without Purge, customer reviews, and our revenue we can determine the effectiveness of Purge. This can also be used to determine Purge's effectiveness in protecting mobile devices from data breaches. By looking at all the mentioned ways we will be able to make informed decisions on how to improve Purge to better provide effective protection against data breaches and make sure it is a successful business venture.

Turning the Innovation into a Reality

Turning Purge into a reality requires a plan that covers several steps. My group created an application called Purge. Purge plans to be the solution to the important issue of data breaches on mobile devices. The first step in turning Purge into a reality is by conducting research on whether there is a need for Purge. This will be done by looking at the market and identifying whether there is a demand for Purge. This is crucial because if no one needs Purge then it is a wasted venture. In addition, market research helps in identifying Purge's competition and we can use this research to create unique features that can differentiate Purge from our competitors. Market research can also help identify the pricing strategy for the application. We will need to ensure that the price of Purge is competitive and affordable to our targeted audience.

Next, is to develop a business plan that outlines our objectives, strategies, and tactics that are required for us to launch and promote Purge to the public. The business plan will define our target audience, Purge's features and the benefits of the application, as well as our pricing strategy, and marketing plan.

After developing our business plan, next we will need to try and get the necessary funding to develop and launch Purge. Creating applications is expensive and Purge is no exception to this. Therefore, we will need to seek investors or crowdfunding to be able to afford the developmental process of the Purge. We will be using the funding to cover development costs as well as ongoing maintenance costs to maintain Purge and ensure it is successful. We plan on creating a pitch to show the benefits that Purge provides, how Purge will fix the issue of data breaches on mobile devices, and how in demand is this security. We plan on providing this information in hopes they will invest in our business. This is a crucial step in turning Purge into a reality.

Once we get our funding secured from investors, we can use the investments to assemble a development team that will consist of various experienced app developers, some cybersecurity experts, and user experience designers. Our team will work together on designing and building Purge. We will ensure the team incorporates the features and benefits we identified in our business plan. This is a very important step as we want Purge to be the best application we can create. We plan on hiring some of the best in their fields to make sure that Purge turns into the great success we envision it to be.

Once the Purge has been built, it is important to monitor it and make sure it stays up to date. We can do this by testing the application before releasing it to ensure that no problems occur during launch. Availability is crucial to having successful security for mobile devices. We will ensure availability by conducting user testing to identify any possible bugs or issues that need to be fixed. The application should be user-friendly and effective in protecting mobile devices from data breaches. If the app is too complicated, then users won't want to implement Purge onto their devices. Therefore, making sure the application user friendly is very important. The testing phase is critical as it helps ensure that the application meets the needs of the target audience and is effective in protecting against data breaches.

After testing and refining, Purge will be launched and promoted to our target audience. We will do this by using different marketing strategies. We will promote Purge via social media, emails, and online advertising. Our marketing strategy will focus on the unique features and benefits of Purge. We will do this to show that Purge is different from our competitors and is the future of mobile device security. To ensure we keep our promise to our users we will maintain constant maintenance of Purge and if any issues occur, we will have a fast-responding support team. We plan on doing this to ensure that Purge stays up to and will also be able to address the evolving strategies of cyber-attacks.

We must take into consideration of everything when creating Purge. One important thing to consider while creating Purge is the possible barriers that could occur while developing Purge. These possible barriers are competition, lack of funding, or various technical challenges. Although these are possible barriers I believe with a well-planned approach and a dedicated team we can overcome these obstacles and turn Purge into a successful mobile device security application.

Summary of Next Steps

The next steps will involve turning Purge from an idea into a reality. We can begin with the development process next. We will do this by working with the programmers, designers, and cybersecurity specialists we hired. This is necessary to make sure the application follows the various rules and regulations revolving around Purge. In order to make sure that Purge is bug-free, we will need to carry out constant testing and quality assurance. As well as keeping ahead of the competition and satisfying our consumer's expectations, we will be constantly implementing new features and technologies that will address the ever-changing issue surrounding data breaches.

Following the development phase, we must build and implement a marketing strategy to advertise Purge and raise its profile in the marketplace. This can entail using social media sites, developing a website, and forming a partnership with companies that make mobile devices or work in cybersecurity to offer packaged services. To increase our credibility and win the market's trust, we also need to form connections with associations and organizations within the sector.

In conclusion, the next stages for Purge will be to make it a reality and release it on the market. This would be done by gathering market data, working with experts, developing the application, and putting a marketing plan into action. Through this project, I've learned the significance of collaborations between different disciplines, and the importance of innovation in solving real word issues. I also picked up useful project management principles, such as how crucial it is to set clear objectives, do deep research, as well as to adjust to criticism. Looking back, I see that before creating the concept of Purge, I should have spent more time studying the market and other possible applications. I believe because of this; we missed out on opportunities to stand out from the competition. The other issue is we could have changed our strategy to better suit the needs of the market. In the future, I will be sure to perform better research and analysis to make sure that Purge and its services are satisfying our consumer demands. It is important in the future for us to distinguish ourselves from the competition.

References

Barthwal, D. (2016). Mobile Device Management (MDM) in Organizations. *Eastern Institute of Technology*. https://www.researchgate.net/publication/305380830_Mobile_Device_Management_MDM_in_Organizations

Chen, P. S., Lin, S., & Sun, C. (2015). Simple and effective method for detecting abnormal internet behaviors of mobile devices. *Information Sciences*, *321*, 193–204. https://doi.org/10.1016/j.ins.2015.04.035

Data Breach Investigations Report (DBIR). (2022). *DBIR Data Breach Investigations Report 2022*. https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf

Di Leom, M., Choo, K. R., & Hunt, R. (2016). Remote Wiping and Secure Deletion on Mobile Devices: A Review. *Journal of Forensic Sciences*, *61*(6), 1473–1492. https://doi.org/10.1111/1556-4029.13203

Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity*, *2*(1), 3–14. https://doi.org/10.1093/cybsec/tyw003

Glowinski, K., Gossmann, C., & Strümpf, D. (2020). Analysis of a cloud-based mobile device management solution on android phones: technological and organizational aspects. *SN Applied Sciences*. https://doi.org/10.1007/s42452-019-1819-z

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

IBM Security. (2020). *Cost of a Data Breach Report 2022* (3R8N1DZJ). IBM. https://www.ibm.com/downloads/cas/3R8N1DZJ

Perera, S., Jin, X., Maurushat, A., & Opoku, D. J. (2022). Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. *Informatics (Basel)*, *9*(1), 28. https://doi.org/10.3390/informatics9010028

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, *8*(2), 133. https://doi.org/10.3390/healthcare8020133

Telo, J. (2019). A Comparative Analysis of Network Security Technologies for Small and Large Enterprises. *International Journal of Business Intelligence and Big Data Analytics*. https://orcid.org/0009-0004-5101-8064

Wang, P., Morris, R., & Wood, D. F. (2019). ECONOMIC COSTS AND IMPACTS OF BUSINESS DATA BREACHES. *Issues in Information Systems*. https://doi.org/10.48009/2_iis_2019_162-171