The Impacts of Cybersecurity and AI on Businesses and Individuals

Deepanshu Kaushik

Monroe Township High School

ABSTRACT

In today's ever growing technological world, the protection of systems is needed, and cybersecurity does just that. Cyber security is the field of prohibiting unauthorized users from accessing data, networks, and devices and keeping data safeguarded. AI or artificial intelligence plays a major part in this field since they can enhance the activities of humans more efficiently. Therefore, this paper deeply explores the specific positive and negative effects of cyber security and AI on businesses and individuals. This paper also dives deep into some tools of the field: CVE or common vulnerability and exposures and CVSS or common vulnerability scoring system. This leads the paper to discuss two major cyber incidents from JP Morgan and Chase and Microsoft Exchange Data Breach and the attacks used. These incidents displayed the need for more vigorous cyber security. A few of the attacks these companies encountered, and more types of attacks are explained in this paper as well. In addition, this paper informs about the specific effects cyber breaches can have on companies. This paper revealed that cybersecurity can positively affect businesses and individuals through mitigating attacks, securing data, making data accessible to only those who are allowed, and better quality of life and negative effects include high costs, more management, user inconvenience, constant new threats, and human error. The negative effects of AI include analyzing personal information, target vulnerabilities, mislead individuals, impersonate humans, and provide false information and positives include network intrusion detection products, threat hunting, vulnerability management, and data centers.

Introduction

Cyber security or the field of prohibiting unauthorized users from accessing data, networks, and devices and keeping data safeguarded has long been known today (cisa.gov, 2021). This field can protect many electronic assets and can be used to illegally gain access to them, but the real question is what specific effects this field provides to businesses and individuals. AI or artificial intelligence also plays a part in this field by being an aid or an enemy in the protection of systems. AI can provide major effects and expand the field into new depths. This research paper dives into how cybersecurity and AI can positively and negatively affect businesses and individuals.

In 2023, Indian security researchers noticed that a Pakistan-based group also known as APT36 had notoriously cyber attacked the Indian army and the education sector. They posted a malicious file in the army's system to lure army men to click on it. When they do click, malware spreads and exploits any vulnerabilities in the army's systems. They have also conducted a series of attacks targeting India's schools and government like the Indian Institute of Technology and National Institutes of Technology (IANS, 2023).

In 2022, IBM reported that 83% of organizations have incurred at least 1 data breach. There was also a 13% increase in Ransomware attacks recorded in a Verizon Data Breach Investigations Report (Huang et al., 2023).

In 2022, there was a cyber-attack in New Jersey, Somerset in which a ransomware attack affected the emails of many residents and IT systems. This proved disastrous since the residents of the county had to shut off their electronic assets and create temporary Gmail accounts. There was also a disruption in the services in the county's databases which could have altered the history of the county (Lyngaas, 2022). Without the use of proper cyber security measures,

these international, national, and local areas have been negatively affected with major consequences. It is key to understanding the effect of cyber security and AI since these topics could have aided these areas and businesses. Even though there are some negative effects of cyber security and AI, implementing them would have been more useful and worthwhile since their data is important.

Utilizing poor cybersecurity can facilitate many attacks like these to be severely dangerous and have disastrous effects on businesses and people. A hacker can spread malware, steal personal information, and use one's computer to hack other computers without the individual even realizing. They can tap into unidentified vulnerabilities (flaws in software) and exploit them in order to gain access to one's system. Implementation of many types of cyber-attacks can be done in a matter of hours and an individual or business won't even find out. Understanding the implementation of the concepts of Cybersecurity like C.I.A., CVE, and CVSS can save a company from going out of business and individual's work and overall have a positive effect. Understanding the attacks and effects can allow people to become more aware of their information and system. Therefore, this research discusses two major cyber-attacks on two popular companies, the three goals that cyber security teams try to achieve, CVE and CVSS, the different types of attacks done by hackers, and the effects of cyber breaches on businesses and individuals. Without these understandings, an individual's life can be ruined in a matter of seconds and it can take an extremely long time to rebound. Informing the public about the effects both negative and positive allows individuals and businesses to decide for themselves whether they want to implement the necessary security measures.

Effects of Cybersecurity on Businesses and Individuals

First and foremost, cybersecurity can protect technologies and information from illegal access from bad actors, corruption, theft, and damage. C-suites or chiefs of a business lack educational experience regarding cyber risk so without cybersecurity, the business will be left vulnerable and unprepared. Having C-suites and members of a business take cautionary measures through risk management of cyber threats can allow threat mitigation. They can also hire cyber security teams which can facilitate risk assessments through voluntary frameworks.

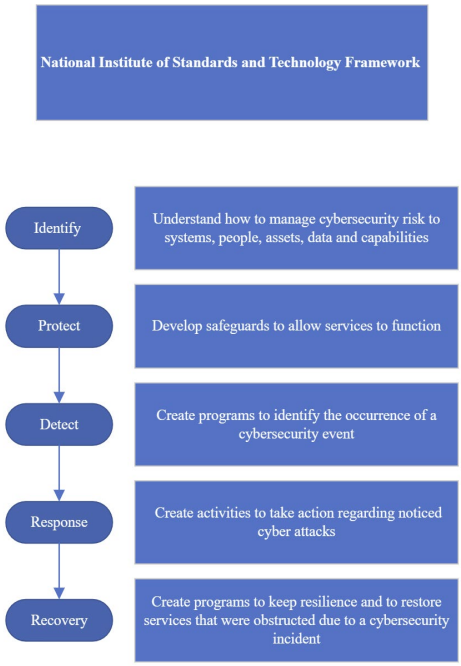

Figure 1. This is one framework made by NIST or National Institute of Standards and Technology which consists of five functions or procedures. These procedures can be taken in order to reduce security risks and implement security activities. Information form "Cybersecurity is Critical for all Organizations - Large and Small" (Ursillo et al., 2019).

From **Figure 1,** this framework can minimize the chances of cyber-attacks occurring in the future and overall allow the growth of a business to grow. Cyber security teams can also have a positive effect through mitigating malicious attacks through firewalls, web proxies, and anti-phishing software. Additionally, Cyber security teams also implement system use policies or rules by which the IT systems can be used and internet use policies. System use policies include passwords being changed regularly, prohibition of copying or removing data without approval, physical security of equipment, and multi factor authentication. Internet use policies include prohibiting the download of executable program files and downloads from safe and reputable websites (Ursillo et al., 2019; Zerlang 2022).

These policies and frameworks can not only mitigate attacks but make sure that the data is secure and accessible to only those who should have access to it. Without these tools, an individual and businesses data can be at high risk of identity fraud or a leakage of personal information. In addition to security, cybersecurity can also provide an overall better quality of life since when access to emails or other websites becomes obstructed, individuals feel stressed. Not only emails but when top secret information has been exposed, this can cause high tension for the one keeping the secret in a system. Through implementing these strong cyber security practices, businesses and individuals can both stay safe from harm (cybersecuritycareer.org, 2022). **Figure 2** exhibits that cybersecurity is rated as top 3rd in a list of 31 worrisome topics of companies. That goes to show how important cyber security is to a company and that taking the necessary measures would reduce this stress and consequently the stress of other topics like bankruptcy that cybersecurity affects.

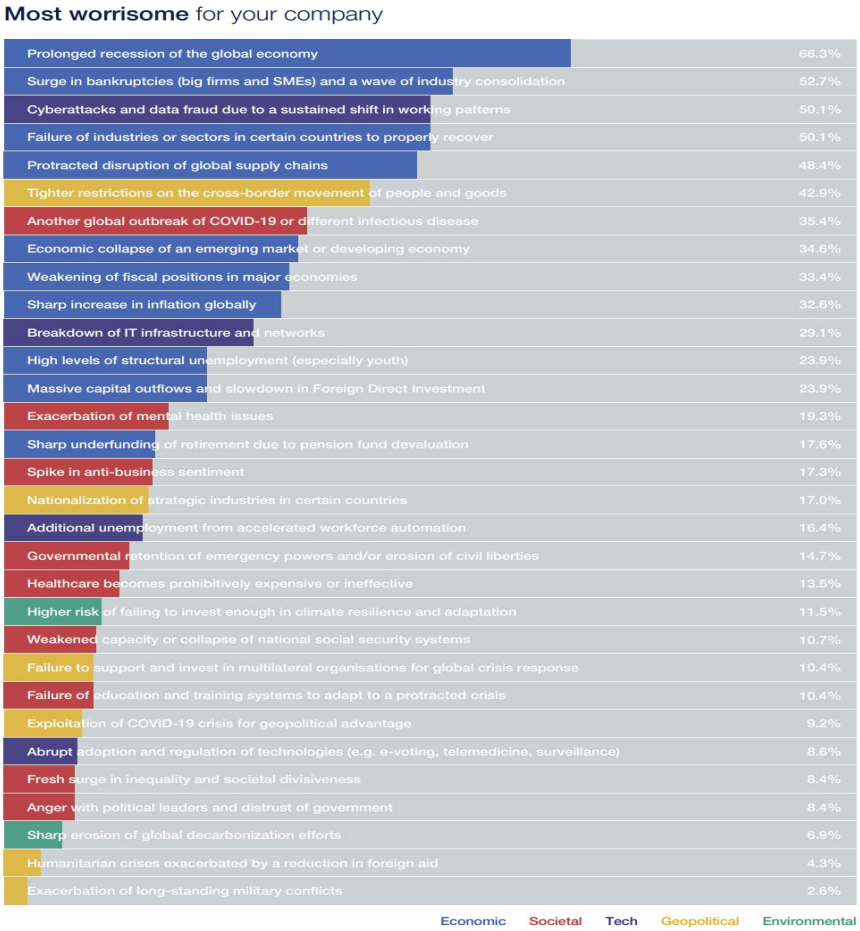

Figure 2. Different issues being placed in a bar graph from least worrisome to most worrisome for a company which was rated by business leaders in which cybersecurity is in the top three. Adapted from "Most Worrisome for your company" by weforum.org (2020).

Even though Cyber security has a surplus of benefits, there are some risks and costs to consider (Aggarwal, 2023).

High Costs	Management	User Inconvenience	Constant New Threats	Human Error
-Small Businesses can find it tough to implement cyber security -Hardware -Software -Skilled professionals need to be hired	-Managing complex cyber security components can take up time -If limited expertise then challenges occur	-Strict protocols can provide as inconvenient to users -Time consuming -Reduced productivity	-continuously update security protocols and rules to adapt to growing cyber threats -Time consuming	-Weak password choice -Poor security engineering -Poor security protocols

Figure 3. Table displaying the costs and risks of implementing cyber security. Adapted from "10 advantages and disadvantages of Cyber Security" by trainings.internshala.com (2023).

These reasons will pose a problem especially to small businesses and require them to spend extra time and money to secure their data. It will take time to secure, constantly update the existing security measures, and manage cyber security software. It will take money to hire specialists, install software, and buy the necessary hardware. It all depends on whether businesses want to take the risk of their data leaking or not weighing in time, money, and security.

Effects of AI on Businesses and Individuals

Ultimately, AI can provide danger to cybersecurity due to how hackers can use them to aid in their evil ventures. AI can analyze data of personal information to create personalized phishing emails with relatable information. This will further convince individuals and businesses to click on their emails and open dangerous links. AI can also target vulnerabilities while being undetected and implementing malware just like bad actors but it saves hackers time to do other malicious activity. One form of AI which can be very dangerous are chatbots because they can impersonate a human and trick the individual into following their orders. Individuals sometimes cannot discern between AI and a human which makes this such a huge problem. The risk of data privacy increases since data collection can be shared with third parties. Other dangers that arise include deceptive trade practices, disinformation, resource depletion, and data sets. Deceptive trade practices denote that AI can mislead individuals to break laws without them even realizing. Disinformation represents that false information can be created at a believable scale which violates the integrity of the data. In addition to these problems, businesses and individuals have to invest their time and money in data and computing power. These extra costs incentivize them to not use AI and keep their original work force in place. Also, AI needs to train on accurate data sets like malicious codes, malware codes, and anomalies which takes too much time and brain power to do. Finally, neural fuzzing or the testing of large amounts of input data to identify vulnerabilities can provide hackers with an upper hand by using this system (Wolf, 2021; Segal, 2023; Anderson, 2023).

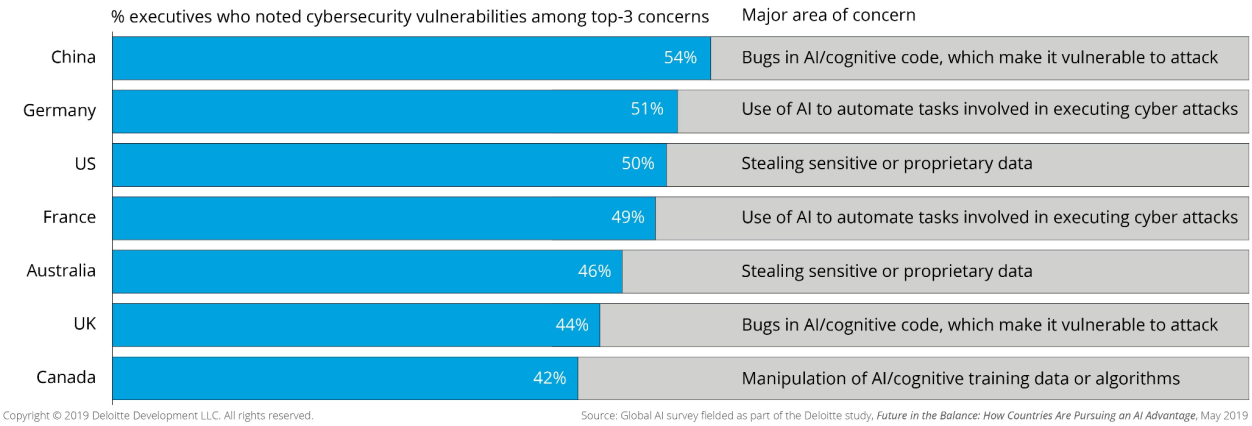

Figure 4. Bar Graph displaying top 3 cybersecurity concerns in a few nations with AI being most prevalent. Adapted from "The idea of AI's threat to nations" by Deloitte.com (2023).

In Figure 5 below**,** AI can also provide many benefits to cyber security specialists through network intrusion detection products, threat hunting, vulnerability management, and data centers.

Network Intrusion Detection products and isolating threats	**Threat Hunting**	**Vulnerability Management**	**Data Centers**
● AI used to find anomalies in user behavior ○ mark higher authority that was given to user ○ Machine Learning (form of AI) that learns and adapts from training data(examples of cyber-attacks) to detect future cyber attacks ○ provide early detection and alert ● Isolate threats before whole networks and systems are destroyed	Threat hunting becomes faster There may be false positives but combining old methods of attack detection and AI can prevent them	Traditional methods include waiting for vulnerabilities to be exploited first and then neutralizing them AI can detect zero-day vulnerabilities(vulnerabilities not known to creator) before they even occur	AI can help monitor and optimize data center's activities calculative abilities of AI can give advice into how to improve security of hardware Reduce the cost of hardware maintenance through notifying the company before hand

Figure 5. Table displaying the different benefits AI can provide (Segal, n.d.; Wolf, 2021)

In addition to these reasons, there are many statistics where businesses use AI to aid them in cybersecurity.

- "51% of businesses use AI primarily for threat detection, 34% heavily for prediction, and 18% for response.
- 62% of enterprises have fully implemented AI for cybersecurity or are exploring additional uses.
- Today, 71% of organizations spend more on AI and machine learning for cybersecurity than two years ago.
- The market for artificial intelligence in cybersecurity is expected to reach USD 133.8 billion by 2030, driven by an increase in the number of cyber-attacks.
- As of 2027, the global market for AI cybersecurity technologies is expected to grow at a compound annual growth rate of 23.6%.
- AI is used for security by more than 80% of telecommunications companies," (Yaqub, 2023).

Types of Cyber Attacks on Businesses and Individuals

There are many cyber-attacks in today's ever growing technology world in which some major ones include denial of service, distributed denial of service, man in the middle, ransomware, phishing, whale-phishing, and trojan horse attacks. The denial of service or DoS attack degrades a network or system through submitting many false requests and overloading the service. It halts all routine and necessary tasks of a user. This costs the user's their time and money to restore the network to its fast-paced self. Distributed denial of service is DoS, but its multiple infected host machines are controlled by an unauthorized user rather than one. In order to protect oneself from this kind of attack, Man in the middle attack or MITM is an attacker who is between the communication line of two parties, computers, or networks and eavesdrops on the data. When the data is sent from an individual or organization, this attacker can alter the data before the receiver of the data receives it. This violates the integrity of the data. To protect a system from this attack, strong encryption or VPN should be used. One attack most commonly used today is ransom. The target's system is held hostage from downloading ransomware from either a website or email attachment. Then, the target must pay a ransom in order to retrieve his system. This cyber-attack can cause a lot of panic to the user and lead them to pay the ransom. In order to avoid this attack, an NGFW or a next-generation firewall should be installed. Phishing attacks on the other hand are done through an email that is sent to a target and disguised as a trusted and legitimate source. The Target presses a link and the bad actor tricks them to reveal sensitive information or the system downloads malware. Whale-Phishing attacks are similar to phishing attacks but the target is a leader of an organization or C-suite hence the name "whale phishing". Another attack with this one being infamous is the trojan horse attack. The trojan implements a malicious program hidden under a legitimate looking one. When the user opens the program or website, malware spreads. The significant aspect is that a backdoor is created and a hacker can access the system and penetrate the network or computer. To avoid this attack, the user is advised to not press on any suspicious links and download a NGFW (fortinet.com, n.d.).

JP Morgan and Chase Data Breach

One of the largest and popular banks in the United States in 2014 incurred a data breach in which 76 million people's personal information and accounts were exposed. This caused panic since these hackers could now easily do identity theft and steal millions. This is significant since bank information holds far more secrets and important information than retail stores. The hackers were able to get into Chase's internal network and breach over 90 servers. Eventually they were able to get full administrative access to all servers when the bank's security team found out about the breach. The attackers gained unauthorized access to customer information, including names, addresses, phone numbers, and email addresses. However, it was later determined that no financial information such as account numbers, passwords, or Social Security numbers were compromised. Although the exact identities of the attackers were never publicly disclosed, law enforcement authorities speculated that the breach was carried out by a group of Russian hackers. There

are many reasons as to how this breach may have occurred but one of the believed reasons was that there was a hole exposed in a server due to a failure to switch two-factor authentication. The technicians failed to update one of their servers and allowed users to enter without a password and a one time code. Even though there was no record of money being stolen, the JPMorgan Chase data breach in 2014 served as a wake-up call for the banking industry and underscored the need for robust cybersecurity measures to protect customer data from cyber threats (Silver-Greenberg, 2014; Leyden, 2014). In this scenario, the implementation of AI could have aided the company by detecting this phishing email early and notifying administration. AI could have been used as a very powerful tool. This would have saved the company a lot of lawsuits, money, stress, and the fear of another attack.

Microsoft Exchange Server Data Breach

Microsoft, famously known for the online tools it provides, incurred a cyber breach in 2021. The suspected actors consisted of ten groups in which included Hafnium (state-sponsored Chinese group), Tick, Lucky Mouse, Calypso, the Winnti group, Tonto team, Mikroceen, Websiic, DLTminer, and one more. The US and other nations believe the cyber actors were affiliated with China's Ministry of State Security, but they denied the accusations. These groups targeted groups and individuals worldwide like the European Banking Authority and the Norwegian Parliament through targeting on premises Microsoft Exchange servers. The methods the hackers implemented was through exploiting multiple zero-day vulnerabilities (vulnerabilities that went unnoticed from the creator of the system) and used certain types of back doors to provide long term access and other tools allowed remote access. Ransomware and crypto-mining malware were also inserted into some systems. The effects of these attacks entail data extraction from the Norwegian Parliament and Acer with Acer also incurring a ransom for fifty million. This led to national responses to be made against the exploits and Microsoft updating its Microsoft Defender antivirus (Chan, 2021).

Cybersecurity Goals and Topics

CVE and CVSS

CVE or common vulnerability and exposures is a program that hosts all common vulnerabilities (weakness in a system) found in systems through identifying them, defining them, and then cataloging them in the MITRE website. Each vulnerability in the catalog has one CVE record. A CVE record entails the description of the vulnerability and a CVE ID. This record is classified into three states: reserved, published, and rejected. A reserved CVE record is when the unique CVE ID is reserved by the CNA(CVE numbering authorities) and is the initial state of the record. A published CVE record is when the CNA populates or inputs information in the record and is accessible to everyone. The information would be a short description of the vulnerability, a CVE ID, and at least one reference. An example of a vulnerability in the CVE is CVE-2022-3465 (VulDB, 2022) in which a critical vulnerability was found in the company Mediabridge. This vulnerability affected some code on the file /index.asp. This affected code could allow manipulation and unauthorized access to a bad actor (cve.mitre.org, n.d.; cve.org, n.d.; cve.org, n.d.; cve.org, 2020)

CVSS or common vulnerability scoring system is used to score numerically how severe a vulnerability is. This numeric number can be transformed into brackets of low, medium, high, and critical severity. In order to use the calculator, the scores are calculated in sequence in three metric groups: base, temporal, and environment. The base group represents the constant qualities of a vulnerability over time. The temporal group represents the qualities that change over time. The environmental group represents the qualities that are unique to a user's environment (cve.mitre.org, n.d.; first.org, n.d.; first.org, 2019).

These tools are important since they allow business and individuals to access these vulnerabilities and make sure that their systems do not replicate them. In addition, the CVSS calculator can calculate the severity of a vulnerability and allow the businesses to decide how much time and money they should spend to fix the vulnerability.

Cyber breach effects on Businesses and Individuals

"Publicly traded companies suffered an average decline of 7.5% in their stock values after a data breach, coupled with a mean market cap loss of $5.4 billion," (Huang et al., 2023). In 2023, a ransomware attack on ION Trading Technologies forced financial institutions to manually confirm trades. Businesses lost their stock value and money due to a cyber breach and not only this but there would have been many more effects. A cyber breach can cause the whole business supply chain to suffer an impact through businesses having less money to spend on products and increasing costs for a company's business ecosystem. These types of breaches can cause economic, reputational, and legal problems. Regarding economic costs, businesses can suffer theft of corporate information, theft of financial information, theft of money, disruption in trading or transactions, and loss in business contracts. Bad actors can alter information on a website and lead the individual business to be portrayed negatively. This can lead to customer loss, sale loss, and profit reduction from customers not buying from the business. Most importantly, if personal information of other individuals is leaked due to a cyber breach, this will lead the business to encounter legal issues with the government and lead the business to go through all sorts of hassles to just clear their name (Huang et al., 2023; nibusinessinfo.co.uk, n.d.; business.gov.au, 2023).

A breach can also lead to an indirect cost where individuals pay a financial cost for taking cyber security measures like antivirus software or they can pay more for stronger cybersecurity. Not only this but an individual's credit card report might be catastrophic. It could take years to restore your credit card score to its original number. This can limit an individual's spending power significantly.

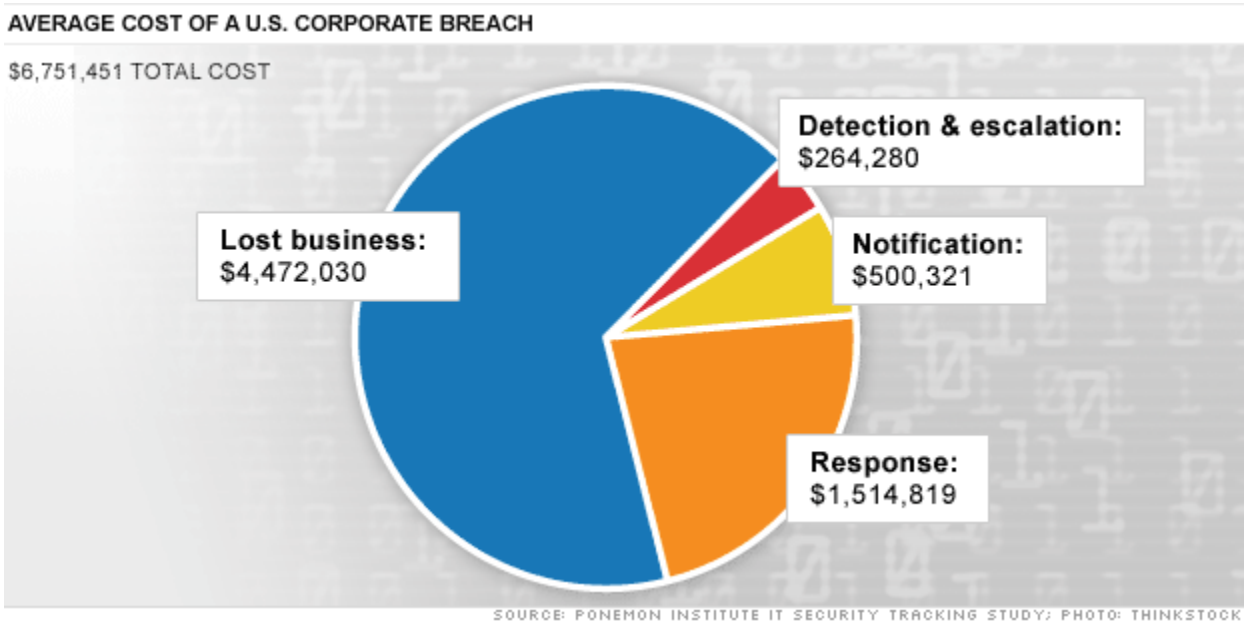

Figure 6. Diagram of a pie chart displaying lost money from a cyber breach in different areas of a company. Adapted from "AVERAGE COST OF A U.S. CORPORATE BREACH" by money.cnn.com (2023).

Conclusion

Cyber security is an ever-growing field with new technology enhancing or endangering the cyber security of many businesses and individuals. The need for it is increasing especially since the major cyber-attacks in JP Morgan and Chase through accessing an unsecured server and in the Microsoft Exchange server data breach through exploiting zero-day vulnerabilities. There are a plethora of benefits this field offers like securing data, mitigating attacks, better

quality of life, and allowing for business growth. These benefits can be achieved through frameworks to facilitate risk assessments, firewalls, two-factor authentication, system use policies, and looking at the CVE database. Even though there are many benefits, there are also many costs like high costs to start, complex management, user inconvenience, constant new threats, and human error. AI has also negatively intertwined in this field through many ways including risk of data privacy, impersonating humans, deceptive trade practices, disinformation, resource depletion, data sets, time, and money. On the other hand, they can provide many positive effects as well like threat hunting, network intrusion detection products, isolating threats, vulnerability management, and data centers. Regarding cyber security and AI, there are both negative and positive aspects about them but understanding the effects of cybersecurity and how cyber-attacks can affect businesses and individuals is necessary in order to comprehend the full scope of effects. Tools like CVE and CVSS are crucial in understanding where to find common vulnerabilities and to determine the severity of a vulnerability so a business can remove possible vulnerabilities from their own systems. Overall, it is important to fully comprehend the effects and tools of cybersecurity and the effects of AI in today's continuously growing technological society and how implementing them can provide benefits and consequences.

Acknowledgements

I would like to thank my family for encouraging me to pursue my passion of Cybersecurity and supporting me for creating this research paper. I would also love to thank Dr. Sarada Prasad for teaching me the fundamentals of Cybersecurity and being an overall supportive teacher. Finally, I would like to thank Coach Jothsna Kethar who has aided me to find what I am truly passionate about and has pushed me to do my very best in this field.

References

Aggarwal, G. (2023). *10 advantages and Disadvantages of Cyber Security*. Internshala Trainings Blog. https://trainings.internshala.com/blog/advantages-and-disadvantages-of-cyber-security/

Ai in cybersecurity: Statistics, example & trends in 2023. BusinessDIT. (2023, May 16). https://www.businessdit.com/ai-in-cybersecurity/

Anderson, M. (2023). *The impact of AI on Cybersecurity*. IEEE Computer Society. https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity

Articles, Iansr. M. (2023). *Pak-based hackers target cyber attacks on Indian Army, Education*. News Karnataka. https://newskarnataka.com/science-technology/technology/pak-based-hackers-target-cyber-attacks-on-indian-army-education/25062023

Breaking down the pros and cons of AI in Cybersecurity. ASIS Homepage. (n.d.). https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2021/april/breaking-down-the-pros-and-cons-of-ai-in-cybersecurity/

Cable News Network. (n.d.). *The cost of Cybercrime*. CNNMoney. https://money.cnn.com/galleries/2011/technology/1107/gallery.cyber_security_costs/2.html

Common vulnerability scoring system SIG. FIRST. (n.d.-a). https://www.first.org/cvss/

CVE Blog "A look at the CVE and CVSS relationship." CVE. (n.d.). https://cve.mitre.org/blog/September112018_A_Look_at_the_CVE_and_CVSS_Relationship.html

CVSS v3.1 user guide. FIRST. (n.d.-b). https://www.first.org/cvss/user-guide

Cyber security and your business. Support for businesses in Australia. (2023, July 5). https://business.gov.au/online/cyber-security/cyber-security-and-your-business

Cyber Security for Business. Impact of cyber attack on your business. (n.d.). https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business

Ursillo, Steve, Jr., C.A. (2019). *Cybersecurity is critical for all organizations – large and small*. IFAC. (n.d.). https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small

The devastating business impacts of a cyber breach. Harvard Business Review. (2023, May 4). https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach#:~:text=.%20.%20.-,Cybersecurity%20risks%20are%20becoming%20more%20systematic%20and%20more%20severe.,increase%20in%20cyber%20insurance%20premiums

Get in touch Jeff Loucks Executive. 614 477 0407. (2020). *Ai and cybersecurity concerns*. Deloitte United States. https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/ai-and-cybersecurity-concerns.html

International cyber law: interactive toolkit. (2021). *Microsoft Exchange Server Data Breach (2021)*. International cyber law: interactive toolkit. https://cyberlaw.ccdcoe.org/wiki/Microsoft_Exchange_Server_data_breach_(2021)

Jessica Silver-Greenberg, M. G. and N. P. (2014). *JPMorgan Chase Hacking affects 76 million households*. The New York Times. https://archive.nytimes.com/dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/

Leyden, J. (2014). *JPMorgan Chase mega-hack was a simple two-factor Auth Fail*. The Register® - Biting the hand that feeds IT. https://www.theregister.com/2014/12/23/jpmorgan_breach_probe_latest/

Lyngaas, S. (2022). *Ransomware attack hits New Jersey County | CNN politics*. CNN. https://www.cnn.com/2022/05/26/politics/new-jersey-somerset-county-ransomware-attack/index.html

Segal, E. (2023). *10 threats that the use of AI poses for companies and organizations*. Forbes. https://www.forbes.com/sites/edwardsegal/2023/03/02/10-threats-that-the-use-of-ai-poses-for-companies-and-organizations/?sh=656858963c7a

Top 20 most common types of cyber attacks. Fortinet. (n.d.-a). https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks

Website. cve. (n.d.-a). https://www.cve.org/ResourcesSupport/AllResources/CNARules

Website. cve. (n.d.-b). https://www.cve.org/CVERecord?id=CVE-2022-3465

Website. cve. (n.d.-c). https://www.cve.org/ResourcesSupport/Glossary?activeTerm=glossaryRecord

Website. cve. (n.d.-d). https://www.cve.org/About/Overview

What impact does cyber security have on our society?. Cyber Security Career. (2022). https://cybersecuritycareer.org/what-impact-does-cyber-security-have-on-our-society/#how-does-cyber-security-affect-our-society

What is cybersecurity?: CISA. Cybersecurity and Infrastructure Security Agency CISA. (2023, August 21). https://www.cisa.gov/news-events/news/what-cybersecurity

World economic forum. (n.d.). https://www3.weforum.org/docs/WEF_COVID_19_Risks_Outlook_Special_Edition_Pages.pdf

Zerlang, J. (2022). *Council post: Why cybersecurity should be part of any business strategy*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2022/11/21/why-cybersecurity-should-be-part-of-any-business-strategy/?sh=656b14d137d6