MODULE: CS1PSA: Professional and Social Aspects of Computing

GROUP: 75

TUTORS: XXXXXXXX

Cybercrime, Artificial Intelligence, and the Impact on Businesses and Consumers

George Hotten (XXXXXX352), XXXXXXXX (XXXXXX904), XXXXXXXX (XXXXXX240), XXXXXXXX (XXXXX028)

March 2024

WORD COUNT: 3964 WORDS

Abstract

George Hotten (XXXXXX352)

With the world of cybercrime becoming evermore advanced, it is important that people are aware of the threats and the consequences of cybercrime, for both businesses and consumers. This report looks to explore the tactics used in cybercrime, from phishing to ransomware, and how people can be educated to spot the warning signs of an attack and prevent attackers gaining access to sensitive information. We further investigate how the recent rise of artificial intelligence impacts the sophistication of malware attacks, the number of AI-powered attacks, and how professionals are leveraging AI to fight back. Finally, we explore the impact on businesses and consumers when they're affected by a cyber-attack, including the potential costs and outcomes. This aims to analyse the power and risks behind modern cyber-attacks, showing how devastating the effects can be on businesses and consumers.

Table of Contents

1. Introduction

XXXXXXXX (XXXXXX240)

Due to the constant advancements and ever-increasing rates of cybercrime, it is crucial to understand how cyber-attacks work in addition to the various contributing factors which work to make cybercrime progressively lethal. Cybercrime refers to any illegal activity involving a network or computer with the objective to cause harm or generate a profit by using malicious tactics and stealing data. Recognising the key components aiding cybercrime in its advance will allow us to significantly lower its success rates and decrease the number of its victims. This would massively benefit users of technology worldwide as statistics from (IBM Security, 2023) state. The global average cost of a data breach in 2023 was 4.45 million dollars, revealing a 15% increase over the previous 3 years, supporting the statement that cybercrime continues to progress. This report will focus specifically on the key topics related to cybercrime such as how it is used, current trends supporting cybercrime and its impacts. The aim of this report is to raise awareness and expand knowledge on cybercrime as a whole, as well as the mentioned topics which will include cybercrime tactics and how to counteract cyber-attacks, followed by how artificial intelligence improves both cybercrime and cybersecurity and the impact of data breaches on businesses and consumers.

2. Tactics Used in Cybercrime

XXXXXXXX (XXXXXX240)

As the world of technology grows, new methods of data manipulation continue to surge which have caused innumerable losses to data due to the multiple tactics available to carry out cybercrime. These attacks have resulted in 39% of businesses in the UK suffering cyber-attacks in 2022, costing them an average of £4,200 in the same year. Cybercrime has increased globally by 125% from 2020 to 2021, threatening both businesses and individuals. (AAG IT Services, 2024). Cybercrime is the primary threat to any online data and with it coming in such a variety of forms, businesses and individuals must be prepared to either drive off or avoid these threats.

2.1 What are Some Common Tactics Used in Cybercrime?

The most common cybercrime tactic is phishing. Phishing is used to reveal personal information such as emails, passwords, and bank account information using fraudulent emails or messages, leaving victims under the impression that these have been sent by reputable companies. Nearly 1 billion emails were exposed in 2021 with 323,972 internet users becoming victims of phishing attacks, meaning phishing was the cause of half of users' data breaches in 2021. Although, phishing is such a commonly used cybercrime tactic, it led to the lowest loss to victims, averaging a loss of 136 dollars per individual. (AAG IT Services, 2024).

Another prevalent cybercrime tactic used today is ransomware which is a type of malicious software (malware) used to hold a victim's data on their device hostage by encrypting it and locking it until a ransom is paid to the attacker by the victim. It is a subset of cyber extortion due to the blackmail and ransom part of the procedure, however, ransomware additionally implements encryption to its tactic. This can further escalate to a double or triple-extortion in which the attacker throws out larger threats after the initial ransom has been paid. According to (IBM Security, 2023), although ransomware negotiators and victims are hesitant to disclose ransom payment amounts, the average cost of a data breach caused by a ransomware attack in 2023 was 5.13

million dollars, with the total expected cost to all victims of ransomware in 2023 being 30 billion dollars.

Furthermore, a distributed denial of service (DDoS) attack is a cybercrime tactic used to disrupt the traffic of a specific server or network by flooding its internet traffic. It is carried out on devices connected through internet that are affected by malware, allowing for remote control with these infected devices being known as bots and a group being called a botnet. Instructions can be relayed remotely from the attacker to each bot to send requests to a target's IP address, overwhelming the server and denying entry to normal traffic. (Cloudflare, 2024) says that in quarter three of 2023, their systems mitigated the most substantial attack they had seen with 201 million requests sent per second which was 8 times larger than their record in the previous year.

To conclude, the wide plethora of cybercrime tactics that attackers have at hand make it exceedingly dangerous for gullible individuals and businesses to use devices online. As the number of methods increase, without any countermeasures it would be impossible to decrease the amount victims and cyber-attacks, hence why it is essential to remain updated on new tactics and what may be done to resist them.

3. Education against Cybercrime Tactics

XXXXXXXX (XXXXXX240)

Due to the continuous advance in cybercrime tactics and cyber threats on a day-to-day basis, it is necessary for methods to anticipate, identify and retaliate against cyber-attacks to be taught and spread among technology users. If the process to ward off cyber threats is too constraining for some, hiring professionals is the quicker route to take which is applied by most businesses to keep both the organisations and their customers' information secure. For example, global spending on cyber security exceeded 1 trillion dollars in 2021 and the cybersecurity market is expected to grow to 300 billion by 2024. (Terranova Security, 2024). This proves that it is becoming

increasingly essential for businesses to employ education against cybercrime tactics into their administration.

3.1 Cyber Security Measures

One cyber security measure includes firewalls which are installable and analyse then filter incoming traffic from unsecure sources to prevent potential attacks, guarding ports where a device's information is exchanged with external devices. Firewalls are very commonly used even by individuals as they are simple to use and offer protection with ease of use. 88% of data breachers are a direct result of human error, according to (WebinarCare, 2024), meaning individuals are at fault for allowing attackers to steal their data. Therefore, firewalls are necessary for users who may not notice malicious traffic.

Additionally, passwords are another cyber security measure where users should be changing their passwords between different accounts. By using the same password for everything, or simple predictable passwords, third parties will have easy access to data by finding one password or even by guessing. Up to 65% of people use the same password for multiple accounts, leaving them at risk of data breaching and poor passwords can be pointed out as the reason for almost 81% of company data breaches. (The Tech Report, 2023). Consequently, it takes a data breach for most users to change their passwords as it is easy to choose a simple password and ignore completing 2 factor authentication.

To sum up, there are plenty of safe cyber security measures that those with no knowledge on cyber security or cybercrime tactics have at their disposal. It is vital that every technology user is aware of these measures and administers them as with increased threats must come increased security.

4. Cybercrime and Artificial Intelligence

XXXXXXXX (XXXXXX904)

In the ever-evolving realm of cybercrime, the fusion of artificial intelligence and illicit activities has ushered in a new era of sophisticated threats. As AI technology becomes more accessible and powerful, malicious entities have exploited this technology to execute a diverse range of cybercrimes, ranging from AI-generated malware to autonomous botnets. This intersection of AI and criminal intent presents unprecedented challenges to cybersecurity professionals and law enforcement agencies worldwide. In this section, we will be looking into how artificial intelligence has contributed to the increase of Cybercrime.

4.2 How is Artificial Intelligence Fuelling the Development of Sophisticated Malware?

As cyber threats continue to evolve, artificial intelligence (AI) has become a double-edged sword, facilitating both defensive and offensive capabilities in the realm of cybersecurity. Malicious actors are increasingly leveraging AI to develop highly sophisticated malware that poses significant challenges to traditional defence mechanisms.

One notable way AI is influencing the development of malware is through its ability to automate the creation of malicious code. By harnessing AI algorithms, cybercriminals can generate malware variants that constantly evolve and adapt to evade detection by traditional antivirus software. This dynamic nature of AI-generated malware makes it particularly challenging for security professionals to detect and mitigate (Symantec, 2023).

Furthermore, AI is being utilized to enhance social engineering tactics, a common method for malware distribution. AI-powered phishing campaigns can generate convincing emails tailored to specific individuals or organizations, increasing the likelihood of successful infiltration. These AI-driven phishing attacks often mimic

legitimate communication from trusted sources, making them difficult to detect (McAfee, 2023).

Additionally, AI algorithms enable cybercriminals to automate the process of identifying and exploiting vulnerabilities in target systems. By analyzing large datasets, AI-powered tools can identify weaknesses in software and networks, allowing attackers to develop targeted exploits with greater efficiency (FireEye, 2022).

In conclusion, the fusion of artificial intelligence and cybercrime is reshaping the threat landscape, with AI-powered malware posing significant challenges to cybersecurity professionals. As AI continues to advance, proactive measures and collaborative efforts are essential to mitigate the evolving threat of sophisticated malware.

4.2.2 Comparison of Traditional Cyber Threats and AI-Powered Cyber Threats

Threat Type	**Characteristics**	**Detection Methods**	**Impact**	**Mitigation Strategies**
Traditional Threats (e.g., Viruses, Phishing)	Known signatures, common attack vectors	Signature-based scanning, behaviour monitoring, network traffic analysis	Data breaches, financial loss, system downtime, disruption of services	Regular software updates, firewalls, antivirus software
AI-Powered Threats (e.g., AI-generated Malware, AI-driven Social Engineering)	Dynamic code generation, evasion techniques	Anomaly detection, machine learning models, behavioural analysis	Targeted attacks, sophisticated malware, increased risk of data theft, system compromise	AI-driven threat intelligence platforms, AI-based malware detection systems, security awareness training

4.3 How are Cybersecurity Professionals Leveraging Artificial Intelligence to Defend Against Evolving Cyber Threats?

In response to the ever-evolving landscape of cyber threats, cybersecurity professionals are increasingly turning to advanced technologies, including artificial intelligence (AI), to fortify their defence mechanisms. AI offers a suite of capabilities that enhance threat detection, response, and mitigation, empowering security teams to stay ahead of emerging threats.

One of the primary applications of AI in cybersecurity is anomaly detection. By leveraging AI algorithms, security systems can identify deviations from normal behaviour patterns within networks, enabling early detection of potential security breaches. This proactive approach, as observed in various studies, has proven instrumental in mitigating the impact of cyberattacks (Gartner, 2023).

Additionally, AI-driven threat intelligence platforms play a pivotal role in proactively identifying and prioritizing emerging threats. These platforms aggregate and analyse data from multiple sources, including dark web forums and social media channels, to provide actionable insights into evolving cyber threats. By harnessing AI capabilities, security professionals can anticipate and mitigate potential risks before they escalate (Darktrace, 2022).

Another significant application of AI in cybersecurity is malware detection and mitigation. AI-based malware detection systems analyse code patterns and behaviours to identify previously unseen malware variants. This proactive approach enables security teams to quarantine malicious files before they can execute and cause damage, as highlighted in studies conducted by leading research organizations (MITRE Corporation, 2021).

Furthermore, AI-powered security orchestration and automation platforms streamline incident response processes by automating routine tasks such as alert triage and investigation. By reducing response times and alleviating the burden on human

analysts, these platforms enable security teams to respond effectively to cyber threats (IBM Security, 2023).

In conclusion, artificial intelligence is revolutionizing the cybersecurity landscape, empowering professionals to defend against evolving cyber threats more effectively. By leveraging AI capabilities for threat detection, intelligence, and automation, security teams can enhance their resilience in the face of an ever-changing threat landscape.

4.4 How is Artificial Intelligence Enhancing Social Engineering Tactics in Cyber Attacks?

In the ever-evolving landscape of cybersecurity, the integration of artificial intelligence (AI) into social engineering tactics has emerged as a significant threat vector, exploiting the vulnerabilities inherent in human behaviour. Cybercriminals are leveraging AI-driven techniques to manipulate individuals into divulging sensitive information or performing actions that compromise security.

According to a study conducted by IBM Security, AI-powered social engineering attacks have become increasingly prevalent, with cybercriminals using AI algorithms to craft highly convincing phishing emails (IBM Security, 2023). These phishing emails often mimic legitimate communication from trusted sources, making them difficult for users to discern from genuine correspondence.

Moreover, AI-driven social engineering attacks can exploit psychological vulnerabilities to elicit specific responses from targets. By analysing vast amounts of data on individual behaviour and preferences, AI algorithms can tailor social engineering tactics to exploit inherent biases or emotional triggers, increasing the likelihood of success (McAfee, 2023).

Furthermore, AI-powered chatbots and virtual assistants are being utilized to impersonate trusted individuals or entities in social engineering attacks. These AI-driven agents can engage in interactive conversations with users, persuading them to disclose sensitive information or perform actions that facilitate unauthorized access to systems or data (Darktrace, 2022).

A notable case study involving the use of AI in social engineering attacks is the breach of a prominent financial institution, as detailed in the Internet Organised Crime Threat Assessment (IOCTA) by Europol (2018). The attackers employed AI algorithms to analyse publicly available data on employees and customers, enabling them to craft highly targeted phishing emails that bypassed traditional security measures.

In another instance, an AI-driven social engineering attack targeted a leading technology company, resulting in the compromise of employee credentials and sensitive data. The incident underscores the growing threat posed by AI-driven social engineering tactics in the cybersecurity landscape.

In conclusion, the integration of artificial intelligence into social engineering tactics represents a significant evolution in cyber threats, posing formidable challenges to organizations and individuals alike. As AI-driven social engineering attacks continue to evolve, vigilance and proactive measures are essential to mitigate the risks posed by these sophisticated tactics.

5. Impact of Data Breaches on businesses and consumers

George Hotten (XXXXXX352)

Due to the ever-increasing sophistication of cybercrimes, more and more organisations are facing attacks and data breaches. SurfShark (2024) found that in 2023, over 40 million user account data was exposed worldwide. In this section, I will research the impact that data breaches have on businesses and the people who use their services.

5.2 How do data breaches occur?

The weakest point in all security applications is the end user themselves. Proofpoint (2024) found that over 71% of working adults took risky action online, and 96% of them knew that it was risky. This led to 69% of organisations being infected by ransomware.

As the human factor is often the easiest to exploit, this leads to most attackers attempting to gain access to a business' network and data via phishing, most commonly via email. Proofpoint (2024) further found that in 2023, 76% of businesses attacked worldwide were compromised by bulk phishing attacks. Attacks complete this by creating fraudulent e-mails aiming to be mistaken as from a legitimate source, such as your businesses IT department or a business partner. These e-mails typically contain links to fake login portals which attackers use to steal credentials, or the e-mails contain seemingly innocent attachments which contain malware.

In 2023, the popular YouTube channel Linus Tech Tips were a victim to phishing. In an article by Jay Peters (2023) regarding the incident, it was noted that a member of the YouTuber's team downloaded "what appeared to be a sponsorship offer from a potential partner". The offer sent was malware disguised as a PDF that was able to steal tokens and credentials from the team member's browsers. This allowed them to completely take over the YouTuber's channel, costing them days' worth of revenue.

5.3 The impact on businesses

Data breaches can have a huge financial impact on businesses, as well as severely damaging the trust of the people who use their services. IBM (2023) found that since 2020, the average cost of a data breach has risen by 15.3% from 3.86 million dollars to 4.45 million dollars in 2023. These costs often continue to impact the business for years after the breach occurred.

Research conducted into a breach of a US Health Insurer by Deloitte Advisory (2016) showed that the loss of contract revenue and the loss of customer relations contributed to 75% of the 1.679 billion dollars lost by the company. This cost was accumulated over 5 years after the attack occurred. It took the company 3 years to reach pre-breach member enrollment levels, however due to the story being kept fresh in the news, the company was forced to lower their insurance premiums costing them a further 40 million dollars.

This research shows the devastating effects that data breaches can cause to businesses. They have a huge financial penalty, costing billions of dollars in legal fees, fines by regulatory bodies, and in the loss of customers. Data breaches also risk exposing thousands of records of sensitive data. This data often has a knock-on effect on consumers, who could become victim of identity theft and fraud. With 69% of large businesses in the UK experiencing a data breach between April 2022 and April 2023 (Cyber Security Breaches Survey, 2023), it is more important than ever to invest in the proper cybersecurity tools and resource to prevent large financial penalties and customer loss.

5.4 The impact on consumers

Data breaches don’t always contain consumer information, however when they do the effects can be severe for the consumers who use a business’ service. Action Fraud (2021), the UK's national reporting centre for fraud and cybercrime, received over 336,000 reports of fraud via banking related attacks which costed UK citizens £184 million. In 2023, 744 financial companies were breached, exposing thousands of user’s bank card information (Identity Theft Resource Centre, 2023).

This can be devastating for affected consumers, costing them thousands of pounds that banks are often unable to reimburse. Leaked information can also lead to identity theft, especially when sensitive data such as addresses, medical records and national insurance numbers are part of the breach. With the fraud caused by data breaches costing each affected person on average £547, this can be life altering as people may have to choose between essentials such as food and heating. This could even put some people into homelessness if they couldn’t pay their rent as they had to pay to fix the results of fraud.

5.5 Conclusion

To conclude, data breaches can have a severe impact on both businesses and consumers. Data breaches can damage a business’ reputation for years after the initial breach, costing them a large financial penalty. This is in part due to losing the customer’s trust and to legal fees and recovery from the breach. For consumers it can cost them hundreds of pounds, and it vastly increases the risk of being a victim of identity theft. With the high cost of being a victim of a data breach, it could force them to decide between life essentials, such as food and heating.

6. Conclusion

XXXXXXXX (XXXXXX904)

In conclusion, it's evident that cybercrime, especially through data breaches, poses a significant threat that demands serious attention to cybersecurity. The evolving tactics, including those driven by artificial intelligence, present formidable challenges for both businesses and individuals. For instance, the use of AI in crafting convincing phishing emails has led to a surge in successful attacks, as noted by IBM Security (2023). The financial fallout for businesses is substantial, often extending into the millions of dollars and lingering long after the breach, as seen in research by Deloitte Advisory (2016). Meanwhile, consumers face profound risks, such as identity theft and financial fraud, underscored by the rise in banking-related attacks reported by Action Fraud (2021). Given these realities, it's crucial for us to invest proactively in cybersecurity measures and raise awareness among all technology users. This is essential to mitigate the grave consequences of cybercrime and ensure the protection of sensitive data in our increasingly digital world.

6. References

Action Fraud. (2021). *Fraud Crime Trends 2021 – 21.* Available at: https://data.actionfraud.police.uk/cms/wp-content/uploads/2021/07/2020-21-Annual-Assessment-Fraud-Crime-Trends.pdf (Accessed: March 19, 2024)

AAG IT Services. (2024). *The Latest 2024 Cyber Crime Statistics (updated March 2024).* Available at: https://aag-it.com/the-latest-cyber-crime-statistics/ (Accessed: March 19, 2024)

Cloudflare. (2024*). DDoS threat report for 2023 Q4.* Available at: https://blog.cloudflare.com/ddos-threat-report-2023-q4/ (Accessed: March 20, 2024)

Cloudflare. (2024). *What is a distributed denial of service (DDoS) attack?* Available at: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (Accessed: March 20, 2024)

Cyber Security Breaches Survey. (2023). *Cyber security breaches survey 2023.* Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023 (Accessed: March 18, 2024)

Darktrace. (2022). *Cyber AI Platform.* Available at: https://www.darktrace.com/en/technology/ (Accessed: March 18, 2024)

Deloitte Advisory. (2016). *Beneath the surface of a cyberattack.* Available at: https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html (Accessed: March 07, 2024)

Europol. (2018). *Internet Organised Crime Threat Assessment (IOCTA).* Available at: https://www.europol.europa.eu/iocta (Accessed: March 19, 2024)

FireEye. (2022). *Adversary Tactics, Techniques & Common Knowledge*. Available at: https://www.fireeye.com/ (Accessed: March 13, 2024)

Gartner. (2023). *Gartner Top Strategic Technology Trends for 2023*. Available at: https://www.gartner.com/en/conferences/na/technology-symposium-us/agenda/tech-trends (Accessed: March 08, 2024)

IBM Security. (2023). *Cost of a Data Breach Report*. Available at: https://www.ibm.com/downloads/cas/E3G5JMBP (Accessed: March 07, 2024; March 19, 2024)

IBM Security. (2023). *IBM Security Orchestration, Automation, and Response.* Available at: https://www.ibm.com/security/what-is-security-orchestration-automation-response (Accessed: March 18, 2024)

IBM Security. (2023). *IBM X-Force Threat Intelligence Index*. Available at: https://www.ibm.com/security/data-breach/threat-intelligence-index (Accessed: March 18, 2024)

Identity Theft Resource Centre. (2023). *2023 Data Breach Report*. Available at: https://www.idtheftcenter.org/publication/2023-data-breach-report/ (Accessed: March 19, 2023)

McAfee. (2023). *Threats Report*. Available at: https://www.mcafee.com/enterprise/en-us/threat-center/threat-report.html (Accessed: March 10, 2024)

MITRE Corporation. (2021). *AI and Machine Learning for Cyber Defence*. Available at: https://www.mitre.org/publications/project-stories/ai-and-machine-learning-for-cyber-defense (Accessed: March 19, 2024)

Proofpoint. (2024). *State of the Phish*. Available at: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2024.pdf (Accessed: March 06, 2024)

Peters, J. (2023). *How hackers took over Linus Tech Tips*. Available at: https://www.theverge.com/2023/3/24/23654996/linus-tech-tips-channel-hack-session-token-elon-musk-crypto-scam (Accessed: March 06, 2024)

SurfShark. (2024). *Number of user accounts exposed worldwide from 1st quarter 2020 to 4th quarter 2023 (in millions).* Available at: https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/ (Accessed: March 06, 2024)

Symantec. (2023). *Internet Security Threat Report*. Available at: https://www.symantec.com/security-center/threat-report (Accessed: March 10, 2024)

Terranova Security. (2024). *131 Cyber Security Statistics: 2024 Trends and Data*. Available at: https://www.terranovasecurity.com/blog/cyber-security-statistics#:~:text=95%25%20of%20data%20breaches%20are,by%20the%20cybersecurity%20skills%20shortage/ (Accessed: March 21, 2024)

The Tech Report. (2023). *Password Reuse Statistics: Over 60% Have a Password Problem*. Available at: https://techreport.com/statistics/password-reuse-statistics/ (Accessed: March 21, 2024)

WebinarCare. (2024). *Firewall Statistics 2024 – Everything You Need to Know*. Available at: https://webinarcare.com/best-firewall-software/firewall-statistics/ (Accessed: March 21, 2024)