Vertical Institute

CAPSTONE PROJECT

Guardians of the Vault: AI-Based Cybersecurity in Finance

Mohammad Sopfian

`

Table of Content

01 Executive Summary 2

02 The Surge in Phishing Attempts in Singapore 2022 3

03 AI in cybersecurity: An overview 5

04 Risk and The Challenges 6

05 Future Of AI in Financial Sector 7

06 Key Areas of Focus 9

07 CIA Triad 10

08 Five Essential Pillars 11

09 How can security AI and automation solutions solve the new upcoming cyber-attacks such as generative AI and other forms of AI? 13

10 Significance of AI adhering to specific cybersecurity policies and procedures 15

11 Real-world example of financial institutions successfully utilizing AI 16

12 Documentation 18

13 Conclusion 20

14 Reference 21

`

Executive Summary:

In today's digital age, the financial sector is increasingly reliant on technology and data-driven operations. While this transformation has brought unprecedented convenience and efficiency, it has also opened the doors to sophisticated cyber threats. Financial institutions are entrusted with safeguarding vast amounts of sensitive data and assets, making them prime targets for cybercriminals. As a result, the need for robust cybersecurity measures is paramount.

This executive summary provides an overview of our comprehensive capstone project, **"Guardians of the Vault: AI-Based Cybersecurity in Finance,"** which delves into the critical intersection of artificial intelligence (AI), cybersecurity, and the finance sector. In this project, we explore the transformative role of AI in bolstering the security posture of financial institutions, ensuring the safety and integrity of financial systems.

The modern financial landscape is characterized by rapid digitization, making it increasingly dependent on technology and data-driven operations. While this transformation has brought numerous benefits, it has also exposed the financial sector to evolving and sophisticated cyber threats. Safeguarding the integrity, confidentiality, and availability of financial systems and sensitive data has never been more critical. In response to this ever-growing challenge, this capstone project, titled "Guardians of the Vault: AI-Based Cybersecurity in Finance," explores the transformative role of Artificial Intelligence (AI) in bolstering the security posture of financial institutions.

This project delves into the integration of AI technologies, including machine learning, natural language processing, and anomaly detection, to create AI-driven cybersecurity solutions tailored to the unique requirements of the finance sector. By harnessing AI's predictive capabilities, automation, and real-time threat detection, financial institutions can better protect their data, assets, and reputation while ensuring compliance with industry regulations.

`

The Surge in Phishing Attempts in Singapore 2022

PHISHING Attempts reported to the Singapore Cyber Emergency Response Team nearly trebled to about 8,500 in 2022 from 3,100 in 2021, with the top three spoofed sectors being banking and financial services, the government and logistics.

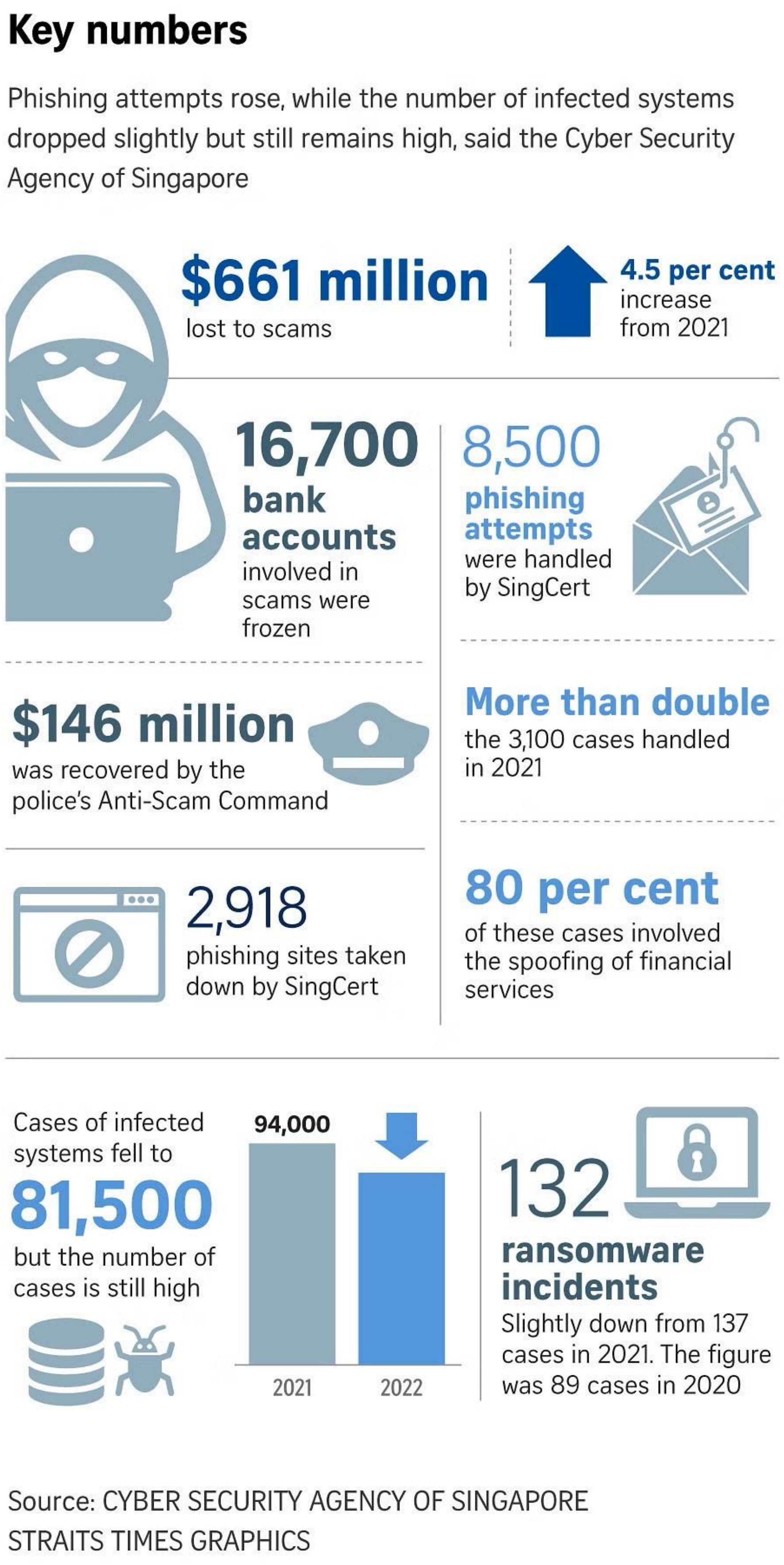
The average cost of a cybersecurity attack here is approximately SGD 1.7 million (USD 1.3 million) per breach, the highest in Asia-Pacific[1]. The Singapore Cybersecurity Market is valued at USD1.96 billion in 2023 and this is expected to grow to USD4.15billion in 2028[2], making this industry one of the most resilient and fast growing industry post Covid.

More than 80 per cent of reported phishing sites in 2022 masqueraded as banking and financial institutions, the *Singapore Cyber Landscape 2022* report published on Friday (Jun 23) showed on The Strait Times.

Since 2016, the sector has been among the top three with the highest number of phishing attempts, said the publication by the Cyber Security Agency of Singapore (CSA). CSA maintains oversight of national cybersecurity functions and works with sector leads to protect Singapore's critical information infrastructure.

Banking and financial institutions are often targeted by phishing attacks as they are trusted organisations which hold sensitive and valuable information such as personal details and login credentials.

`



Key numbers

Phishing attempts rose, while the number of infected systems dropped slightly but still remains high, said the Cyber Security Agency of Singapore

$661 million lost to scams

4.5 per cent increase from 2021

16,700 bank accounts involved in scams were frozen

8,500 **phishing attempts** were handled by SingCert

$146 million was recovered by the police's Anti-Scam Command

More than double the 3,100 cases handled in 2021

2,918 phishing sites taken down by SingCert

80 per cent of these cases involved the spoofing of financial services

Cases of infected systems fell to **81,500** but the number of cases is still high

132 **ransomware incidents** Slightly down from 137 cases in 2021. The figure was 89 cases in 2020

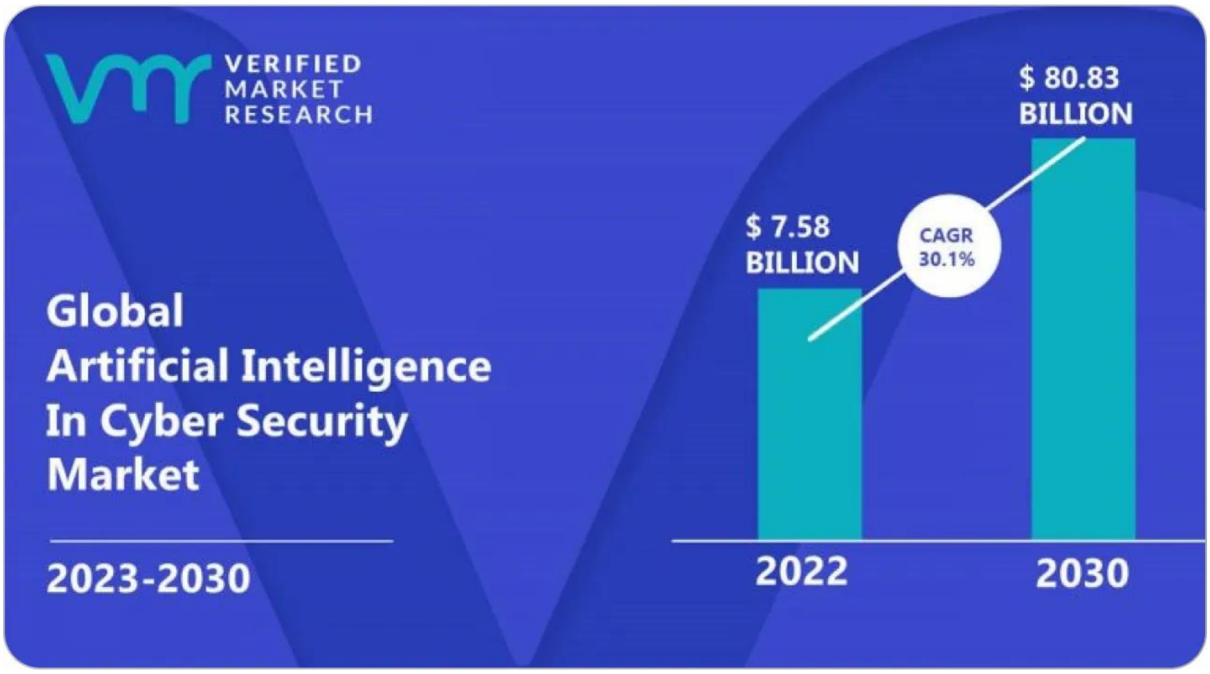
Source: CYBER SECURITY AGENCY OF SINGAPORE
STRAITS TIMES GRAPHICS

`

AI in cybersecurity: An overview

AI in cybersecurity has been gaining traction over the past years. The idea of mitigating cybersecurity risks before they occur has been bringing in investments to develop and improve AI-powered cybersecurity systems.

The latest report by Verified Market Research suggests that the market size for Artificial Intelligence in cybersecurity stood at 7.58 billion dollars in 2022 and is expected to reach 80.83 billion by 2030.



AI in cybersecurity market size 2022-2030 (source)

These growing numbers are not surprising since hackers also get access to new technologies.

For instance, about 93.67% of malware observed in 2019 could modify its source, which made it nearly impossible to detect. Moreover, reportedly 53% of consumer PCs and 50% of commercial computers were re-infected with malware after a brief recovery period.

The increasing number of cyber-attacks has brought the international community's attention toward the possible use of artificial intelligence in cybersecurity. According to a survey by The Economist Intelligence Unit, 48.9% of global executives and leading security experts believe that AI and machine learning are best equipped for countering modern cyber threats.

Moreover, a report by Pillsbury, a global law firm focusing on technology, asserted that 44% of global organizations already implement AI to detect security intrusions.

`

Risk and The Challenges:

Financial institutions face an ever-evolving threat landscape characterized by advanced, persistent cyber threats. Traditional security approaches, while necessary, are no longer sufficient to counteract the agility and sophistication of modern adversaries. To address this challenge, AI has emerged as a powerful ally, offering predictive capabilities, automation, and real-time threat detection.

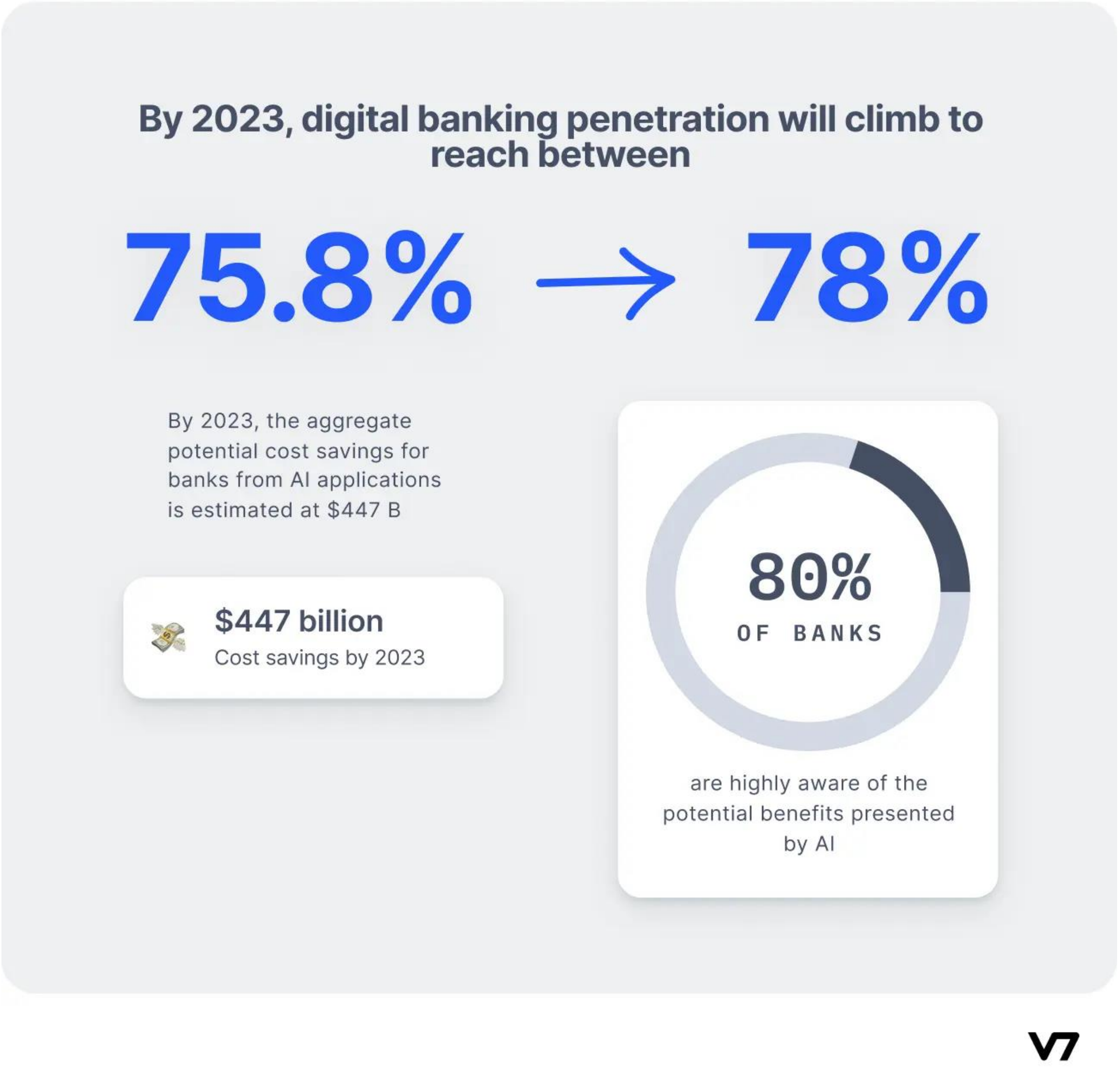
Machine learning systems have done wonders for modern-day businesses by providing critical insights, aiding decision-making, and automating everyday cumbersome tasks. However, there are still many risks and challenges that need to be taken into consideration. Gaurav Keerthi, Deputy Chief Executive Officer at Cyber Security Agency of Singapore says that “AI holds great promise to provide solutions for mankind, yet from a cybersecurity perspective, AI can be both a blessing and a curse.”

Integrating AI in cybersecurity systems poses a number of challenges, such as:

- **Data manipulation**. AI systems use data to understand historical patterns. Hackers can gain access to the training data, alter it to include biases and damage the efficiency of the models. Furthermore, data can be altered to benefit the hacker more.
- **AI-powered cyber-attacks:** Hackers can use AI techniques to develop intelligent malware that can modify itself to avoid detection from even the most advanced cybersecurity software.
- **Data unavailability:** The performance of AI models depends on the volume and quality of data. If sufficient high-quality training data is not provided or the data contains bias issues, the AI system will not be as accurate as expected. Based on this data, an inadequately trained model will result in false positives and a false sense of security. Any threats will go undetected and lead to substantial losses.
- **Privacy concerns:** To properly understand user patterns, AI models are fed real world user data. Without adequate sensitive data masking or encryption, user data is prone to privacy and security issues, favoring malicious actors.
- **Attacks on the AI systems:** AI systems, like any other software product, are susceptible to cyber-attacks. Hackers can feed these models with poisonous data to alter their behavior according to their desired malicious intent.

`

Future Of AI in Financial Sector



By 2023, digital banking penetration will climb to reach between

75.8% → 78%

By 2023, the aggregate potential cost savings for banks from AI applications is estimated at $447 B

$447 billion
Cost savings by 2023

80%
OF BANKS

are highly aware of the potential benefits presented by AI

Future of Artificial Intelligence in the financial sector.
[Source]

The finance industry has always seen the potential benefits of implementing AI-based solutions. But with the widespread impact of COVID-19, AI has become more of a necessity rather than an option.

Most people have embraced the digital experience, and the paradigm shift from traditional banking channels to virtual AI-based services is now more critical than ever.

`

The areas where the impact of AI in finance is expected to increase in the future include:

- Customer acquisition by offering personalized banking experiences
- Fully automated services, such as risk assessment
- Fighting off cyberattacks
- Protecting valuable data from hackers
- Making investment decisions based on customer preferences
- AI is expected to serve as a vehicle for customer-centric services in the finance industry.

`

Key Areas of Focus:

1. **Advanced Threat Detection:** We investigate how AI algorithms can analyze vast datasets to detect even subtle indicators of cyber threats, providing financial institutions with early warning and proactive defence.
2. **Fraud Prevention:** Our project explores AI's role in identifying and mitigating fraudulent transactions, protecting both institutions and customers from financial losses.
3. **Behavioral Analysis**: We delve into AI-powered behavioral analysis to identify anomalous patterns of user behavior that may indicate insider threats or compromised accounts.

And to follow up, we can proceed with a Report.

There's a requirement in security circles that you report against: Are you complying with regulatory requirements or not? And some of the things that we do in those cases is gather the log records and process those.

Finally, we can do research. If we were to investigate and identifying, we want to be able to find out the source of the threats so it be helpful to have a natural language processing system such as a chatbot that we can talk to and ask it questions as It has knowledge base that it draws on.

Regulatory Compliance:

AI can streamline the complex process of regulatory compliance in the financial sector, reducing the burden on institutions while ensuring adherence to industry standards.

`

CIA Triad

Incorporating Artificial Intelligence (AI) into the Cybersecurity CIA (Confidentiality, Integrity, Availability) framework involves leveraging AI technologies to enhance the security of data and systems. Here's a simple explanation of how AI fits into each aspect of the CIA framework, with examples relevant to the banking and finance sector:

1. Confidentiality:

AI in Confidentiality focuses on protecting sensitive information from unauthorized access or disclosure.

- Example: AI-driven access control systems can analyze user behavior and contextual information to detect unusual access patterns. For instance, if a bank employee suddenly attempts to access customer data outside of their typical work hours, AI can trigger an alert for further investigation, ensuring the confidentiality of customer information.

2. Integrity:

AI in Integrity ensures that data remains accurate and unaltered.

- Example: In financial transactions, AI-powered anomaly detection can identify fraudulent activities by comparing transaction data against historical patterns. If an AI system detects an unusual transfer of funds or changes in transaction amounts that deviate from typical behavior, it can raise alarms, preserving the integrity of financial data.

3. Availability:

AI in Availability focuses on maintaining system functionality and minimizing downtime.

- Example: AI-driven predictive maintenance can be used to monitor the health of critical banking infrastructure, such as ATMs or online banking servers. AI algorithms can analyze data from sensors and perform predictive maintenance, identifying potential issues before they cause service disruptions, thus ensuring the availability of banking services.

`

Five Essential Pillars

Incorporating Artificial Intelligence (AI) into the five essential pillars of a cybersecurity framework enhances the overall security posture of an organization by applying AI-driven solutions to address key aspects of cybersecurity. Here's a simple explanation of how AI can be integrated into each of these pillars:

1. Identify:

- AI-Enhanced Threat Detection: AI algorithms analyze vast amounts of data to identify potential security threats, such as unusual network activities or patterns of behavior. This helps organizations pinpoint vulnerabilities and potential risks more quickly and accurately.

2. Protect:

- AI-Powered Access Control: AI-driven access control systems use behavioral analysis to determine if user actions are within the norm. If unusual behavior is detected, access can be denied, therefore protecting sensitive data.
- AI-Driven Authentication: AI-based authentication methods, like facial recognition or behavioral biometrics, provide stronger security by verifying the identity of users more robustly than traditional methods.

3. Detect:

- AI-Enhanced Intrusion Detection: AI systems continuously monitor network traffic, identifying and alerting to suspicious activities in real-time. This proactive detection minimizes the time it takes to respond to threats.
- AI-Driven Anomaly Detection: AI can identify deviations from normal patterns in data, such as unexpected data access or system behavior, enabling rapid threat detection.

4. Respond:

- Automated Incident Response: AI can automate certain incident response tasks, such as isolating compromised systems or blocking malicious traffic, allowing for faster and more consistent responses.
- AI-Enhanced Threat Intelligence: AI analyzes threat data to provide actionable insights for responders.

`

5. Recover:

- AI-Driven Disaster Recovery Planning: AI can help organizations create more effective disaster recovery plans by assessing the impact of potential cyber incidents and suggesting optimal recovery strategies.

- **Automated Backup and Restoration:** AI can automate backup processes and assist in restoring systems to a known-good state, reducing downtime in the event of a breach or data loss.

- **AI-Powered Incident Analysis**: After an incident, AI can assist in analyzing the scope and impact, helping organizations understand the extent of the breach and the data affected. This information is crucial for a swift and targeted recovery.

By incorporating AI into these five essential pillars of a cybersecurity framework, organizations can enhance their ability to identify, protect, detect, respond to, and recover from cybersecurity threats. AI-driven solutions provide advanced capabilities for threat detection, real-time analysis, and automated responses, ultimately bolstering the security and resilience of the organization's digital assets and data.

`

How can security AI and automation solutions solve the new upcoming cyber-attacks such as generative AI and other forms of AI?

Security AI and automation solutions are essential components of defending against emerging cyber threats, including those leveraging generative AI and other advanced AI techniques. Here's how they can help mitigate these new threats:

1. **Anomaly Detection:**

- AI-Powered Behaviour Analysis: Security AI can monitor network and user behaviour in real-time. It can detect unusual patterns or deviations from normal behaviour that may be indicative of generative AI-generated attacks, such as abnormal data transfer or communication patterns.

2. **Threat Hunting**:

- AI-Enhanced Threat Intelligence: AI can sift through vast amounts of threat data, including indicators of compromise (IoCs), to identify emerging attack patterns or signatures associated with generative AI attacks. This proactive threat hunting can uncover novel attack techniques.

3. **Malware Detection:**

- AI-Driven Malware Analysis: Security AI can analyze files and code to detect malicious content generated by AI algorithms. This includes identifying polymorphic malware that constantly changes its appearance to evade traditional detection methods.

4. **Phishing Detection:**

- Natural Language Processing (NLP): AI-powered NLP can analyze email content and website text to identify phishing attempts, even if they use AI-generated text. It can detect subtle linguistic anomalies that humans might overlook.

5. **Endpoint Security:**

- AI-Based Endpoint Protection: Security AI can continuously monitor endpoints for suspicious activities. It can detect unauthorized processes, file modifications, or system changes caused by AI-generated attacks.

6. **Network Security:**

- AI-Driven Network Traffic Analysis: AI can examine network traffic for unusual or sophisticated patterns that may indicate generative AI attacks. It can identify malicious AI-generated commands or network intrusions.

`

7. Response Automation:

- Automated Incident Response: In the event of an AI-generated attack, automated response systems can quarantine affected systems, isolate the threat, and limit its impact. This rapid response can prevent the spread of the attack.

8. Machine Learning Adversarial Models:

- **Adversarial Machine Learning:** Security AI can employ adversarial machine learning techniques to train models to recognize and defend against AI-generated attacks. This involves creating AI models that mimic attacker behaviors and using them to improve defensive measures.

9. Continuous Learning:

- AI Learning and Adaptation: Security AI can adapt and learn from new attack vectors and AI-generated threats. Continuous learning ensures that AI systems remain effective against evolving attack techniques.

10. Collaborative Threat Sharing:

- AI-Enhanced Threat Intelligence Sharing: Organizations can share threat intelligence and collaborate using AI-powered platforms to collectively defend against AI-generated attacks. This collective defense can be more effective in countering emerging threats.

`

Significance of AI adhering to specific cybersecurity policies and procedures

- **Security Assurance:** AI systems can process and store sensitive data. Adherence to cybersecurity policies ensures that AI remains secure, reducing the risk of data breaches and unauthorized access.

- **Protection Against Threats:** Cyber threats, such as hacking and malware, can exploit vulnerabilities in AI systems. Cybersecurity measures help identify and mitigate these threats, enhancing AI's resilience.

- **Data Privacy:** AI often works with personal or confidential information. Following policies safeguards data privacy, ensuring that sensitive data is handled in compliance with regulations.

- **Legal Compliance:** Adhering to cybersecurity policies helps AI systems meet legal requirements and industry standards. This reduces the risk of legal issues and penalties.

- **Trust and Reputation:** Secure AI systems build trust with users and stakeholders. Compliance with cybersecurity policies bolsters AI's reputation and credibility.

- **Business Continuity:** Cyberattacks on AI can disrupt operations. Security measures help maintain AI's functionality and minimize the impact of potential disruptions.

In summary, adhering to cybersecurity policies and procedures for AI is vital to ensure its security, protect against cyber threats, maintain data privacy, comply with regulations, build trust, and ensure business continuity.

`

Real-world example of financial institutions successfully utilizing AI

- JPMorgan Chase employs AI-based algorithms to detect and prevent fraud across various banking activities. JPMorgan Chase employs AI in its cybersecurity strategy to identify and respond to potential threats. Their use of AI helps them analyze massive volumes of data and identify anomalies quickly.

- Using the latest AI-powered insights, **Mastercard** is helping banks predict scams in real time and before any money leaves a victim's account. TSB reports a reduction in losses to scams equivalent to £100 million across the U.K., should all banks adopt the technology and mirror its success. TSB is one of the first banks to adopt Mastercard's Consumer Fraud Risk tool and is already using it to great effect. In just four months, the bank says it has dramatically increased its fraud detection. Based on TSB's results, the amount of scam payments prevented over a year would equate to almost £100m1 saved across the U.K. should its performance be mirrored by all banks. Other banks adopting Consumer Fraud Risk are doing so over the course of 2023, and Mastercard is assessing further international markets to scale the solution.

Benefits:

By incorporating AI-based cybersecurity solutions, financial institutions can enjoy several benefits, including:

- Detect and respond to threats more quickly and effectively than traditional security solutions.

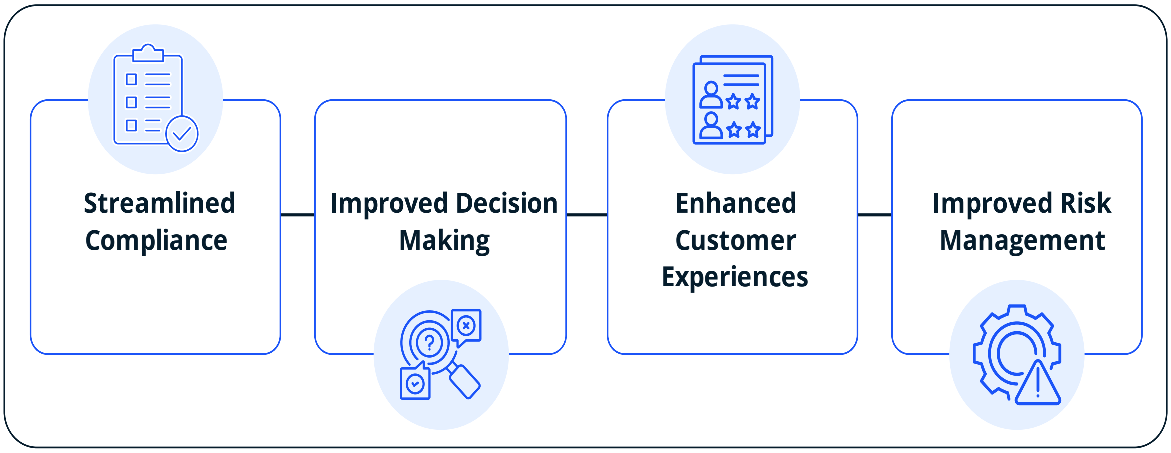
- Enhanced protection of customer data and assets.

- Improved resilience against evolving cyber threats.

- Increased operational efficiency and reduced costs.

- Enhanced regulatory compliance and reporting.

`



LeewayHertz

A report by Business Insider suggests that nearly 80% of banks are aware of the potential benefits that AI presents to their sector. Another report suggests that by 2023, banks are projected to save $447 billion by using AI apps. These numbers indicate that the banking and finance sector is swiftly moving towards AI to improve efficiency, service, productivity, and reduce costs.

`

Documentation:

Document the incident, response activities, and lessons learned for future reference.

Now, let's create a hypothetical incident report for an AI cyber attack:

Incident Report: AI Ransomware Attack

Date: [Date]

Incident Summary:

On [Date], our organization experienced a significant AI cyber attack involving a ransomware variant targeting our AI systems. The attack primarily impacted [list affected AI systems].

Incident Details:

Detection: The incident was initially detected at [Time] when an anomaly was flagged by our AI model monitoring tool, indicating unusual data access patterns.

Containment: The affected systems were immediately isolated from the network to prevent further spread of the ransomware.

Investigation: The incident response team initiated a forensic analysis, which revealed that [Describe findings, e.g., the malware used, affected AI models, and data compromised].

Remediation: [Detail actions taken to eradicate the threat, such as patching vulnerabilities, restoring from backups, and updating AI models].

Recovery:

AI systems were gradually restored to full operation by [Time].

Data integrity checks were performed, and no evidence of data tampering was found.

`

Communication:

Internal stakeholders were promptly informed of the incident's details and recovery progress.

External communication was managed in accordance with legal and regulatory requirements.

Incident Reporting:

An incident report must be in compliance with MAS guidelines. A risk assessment should be done to account for every incident and updated when necessary. Refer to Technology Risk Management Guidelines, 12.3 & 13.6.

Lessons Learned:

The incident underscored the importance of continuous monitoring and proactive threat detection for AI systems.

We have updated our incident response plan to include specific procedures for AI cyber attacks.

`

Conclusion

Security AI and automation solutions play a crucial role in identifying, mitigating, and responding to new cyber threats, including those leveraging generative AI. By continuously adapting and learning from emerging attack techniques, AI can bolster an organization's cybersecurity posture and help defend against evolving threats in real-time.

`

References:

- IBM - AI and automation for cybersecurity
- CYBOTS - Case Study | Banks and Financial Institutions
- The Strait Times - 8,500 phishing cases in Singapore in 2022; more than 80% spoofed a bank or financial service
- Insight.thomsonreuters - AI and cyber-enabled financial crime tops risk agenda
- V7 - AI in Cybersecurity: 5 Crucial Applications
- LeewayHertz - The rise of AI in banking and finance industry: Exploring use cases and applications
- Business Insider India - The impact of artificial intelligence in the banking sector & how AI is being used in 2020
- Verified Market Research - Artificial Intelligence In Cyber Security Market Size And Forecast
- Digital.ai - 16th State of Agile Report
- Sapience - A Career in Cybersecurity - Your Blueprint to an Exciting and Impactful Career
- Monetary Authority of Singapore – Technology Risk Management Guidelines