Northern New England CEO Summit

MONARCH ISC
INFORMATION SECURITY CONSULTING

John Rogers, CISSP
Senior Advisor
john@monarchisc.com

Artificial Intelligence

Opportunities & Threats

MONARCH ISC
INFORMATION SECURITY CONSULTING

Session Agenda

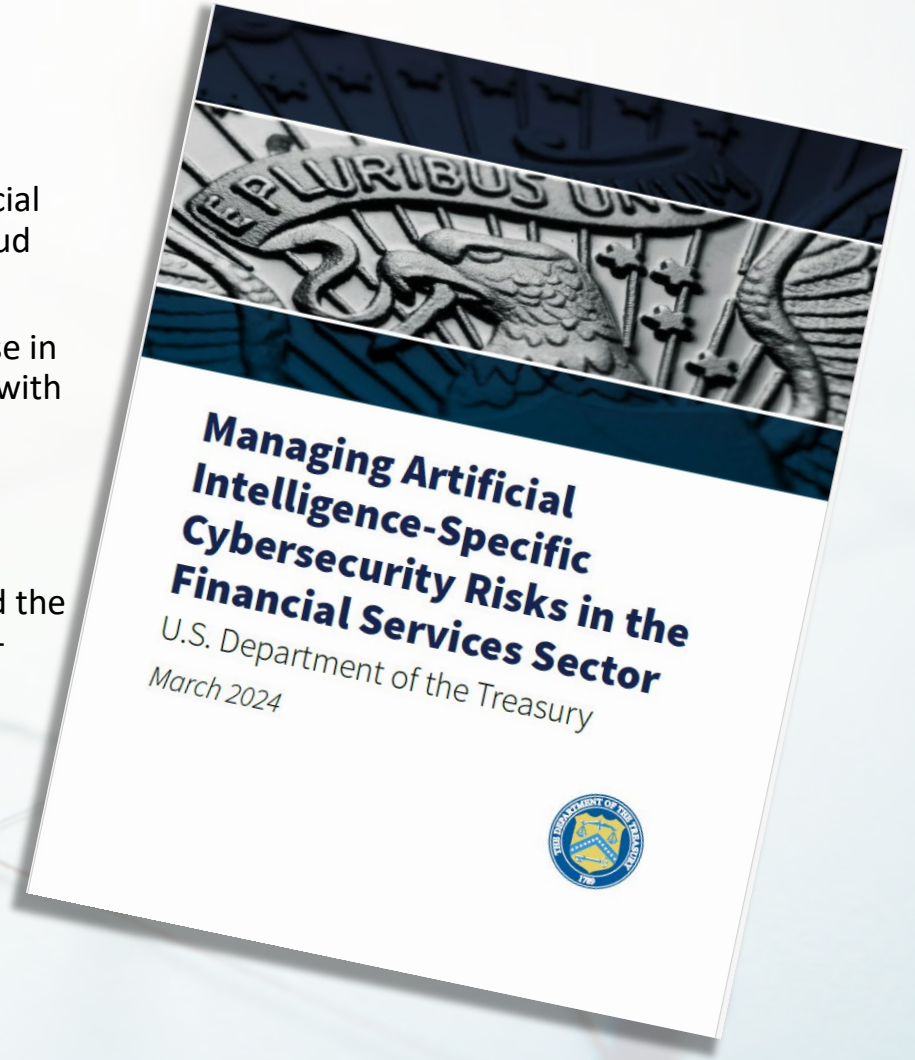
- Generative AI Defined
  - Issues and Concerns
- Use Cases in Banking
- AI Opportunities
- AI Attack Vectors & Fraud
  - Enhancing Cybercriminal Abilities
  - Adversarial AI – AI against AI
- Risk Mitigation | Defense
- Law and Regulation
- AI Risk-Based Policy / Program

MONARCH ISC
INFORMATION SECURITY CONSULTING

Source Material

Primary Source Material

- It includes an overview of AI use in the financial services sector for cybersecurity and anti-fraud purposes.
- The report discusses the implications of AI use in financial institutions based on 42 interviews with industry stakeholders.
- It focuses on best practices for managing AI-specific cybersecurity risks.
- The report also reviews anti-fraud efforts and the increasing coupling of cybersecurity and anti-fraud in financial institutions.



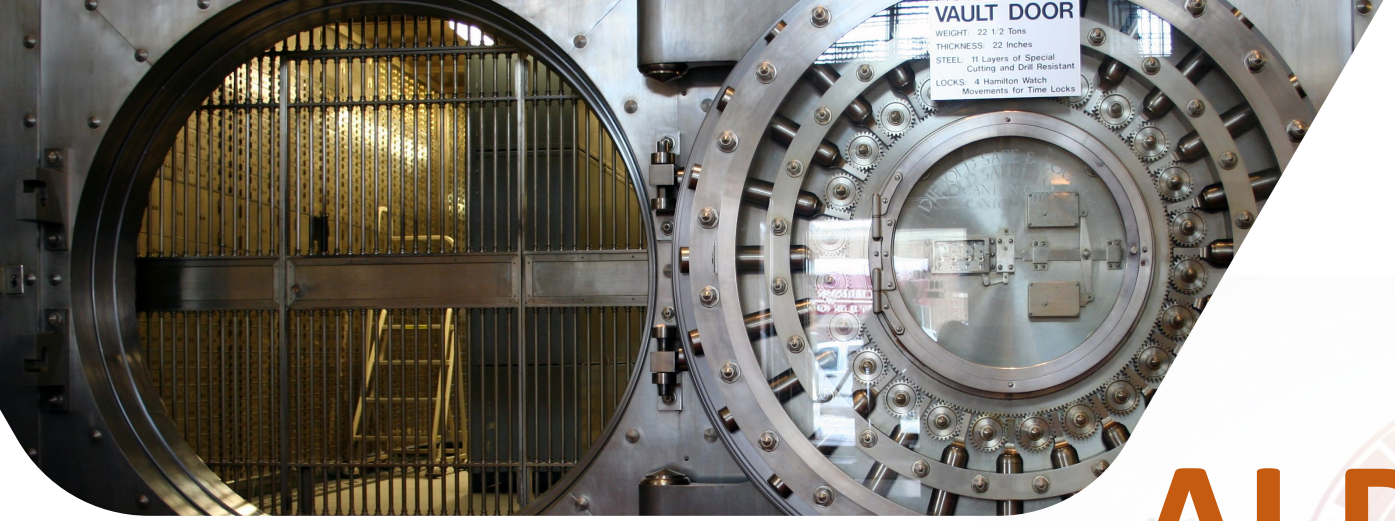
MONARCH ISC
INFORMATION SECURITY CONSULTING

Source Material

Primary Source Material

"This NIST Trustworthy and Responsible AI report develops a taxonomy of concepts and defines terminology in the field of adversarial machine learning (AML). The taxonomy is built on surveying the AML literature and is arranged in a conceptual hierarchy that includes key types of ML methods and lifecycle stages of attack, attacker goals and objectives, and attacker capabilities and knowledge of the learning process. The report also provides corresponding methods for mitigating and managing the consequences of attacks and points out relevant open challenges to take into account in the lifecycle of AI systems."

MONARCH ISC
INFORMATION SECURITY CONSULTING



AI Defined

MONARCH ISC

What is Artificial Intelligence (AI)?

- Narrow Artificial Intelligence
  - Siri, Alexa
- General Artificial Intelligence
  - Not Here Yet
- Machine Learning / Generative AI
  - ChatGPT
  - Everything else we're using

MONARCH ISC
INFORMATION SECURITY CONSULTING

Generative AI Defined

- Capable of generating text, images, videos, or other data using generative models.
- Most often generation is a response to prompts.
- Generative AI models learn the patterns and structure of their input training data and then generate new data that has similar characteristics.

Generative AI Defined

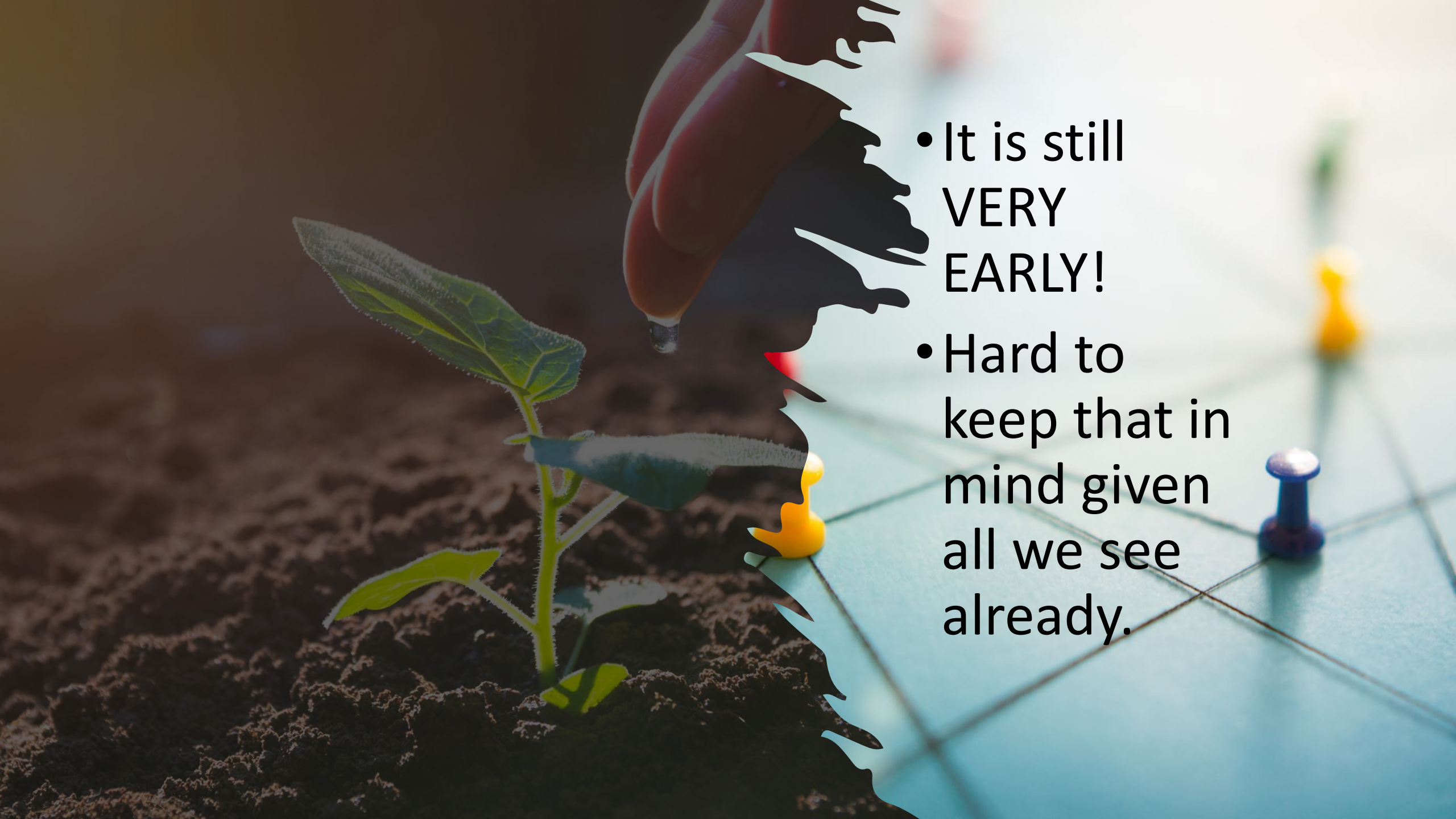
- Originally introduced in the 1960s in chatbots.
- In 2014, the introduction of Generative Adversarial Networks (GAN), type of machine learning where a “generator” and a “discriminator” are algorithmically pitted against each other.
  - The Generator produces data.
  - The Discriminator determines which outputs were artificially created.
  - The Generator is “penalized” when the Discriminator identifies fake data.
  - Each generation, the Generator gets better at producing data that will fool the Discriminator, and the Discriminator gets better at identifying fakes.
  - **For instance: The GAN can be trained to create realistic-looking images of human faces that are not real people.**
  - **Result: “Deep Fake!”**

MONARCH ISC
INFORMATION SECURITY CONSULTING

Generative AI Defined

- Recent introduction of “Transformers”
  - Large models with no need to label data.
  - Billions of pages of text producing deeper content.
  - “Attention” that enables making connections between words across entire books.
  - Can also track connections to analyze code, proteins, chemicals, and DNA.
- Large Language Models (LLMs) with up to trillions of parameters.
  - LLMs are a type of artificial intelligence (AI) that can understand, process, and generate human language.
  - Used to analyze, summarize, and create derivative content across many industries.
- Enabling writing engaging text, photorealistic “painted” images and television programming.

MONARCH ISC
INFORMATION SECURITY CONSULTING



- It is still VERY EARLY!
- Hard to keep that in mind given all we see already.

Early Problems

- Issues with accuracy and bias.
  - Legacy data includes systemic bias.
- “Hallucinations” when a LLM generates false data
  - Deviations from facts.
  - Deviations in the logic that provides context.
- Hallucinations may be obvious.
- Hallucinations may also sound plausible and will require fact-checking to debunk .

MONARCH ISC
INFORMATION SECURITY CONSULTING

Early Problems

Two Famous “Hallucinations”

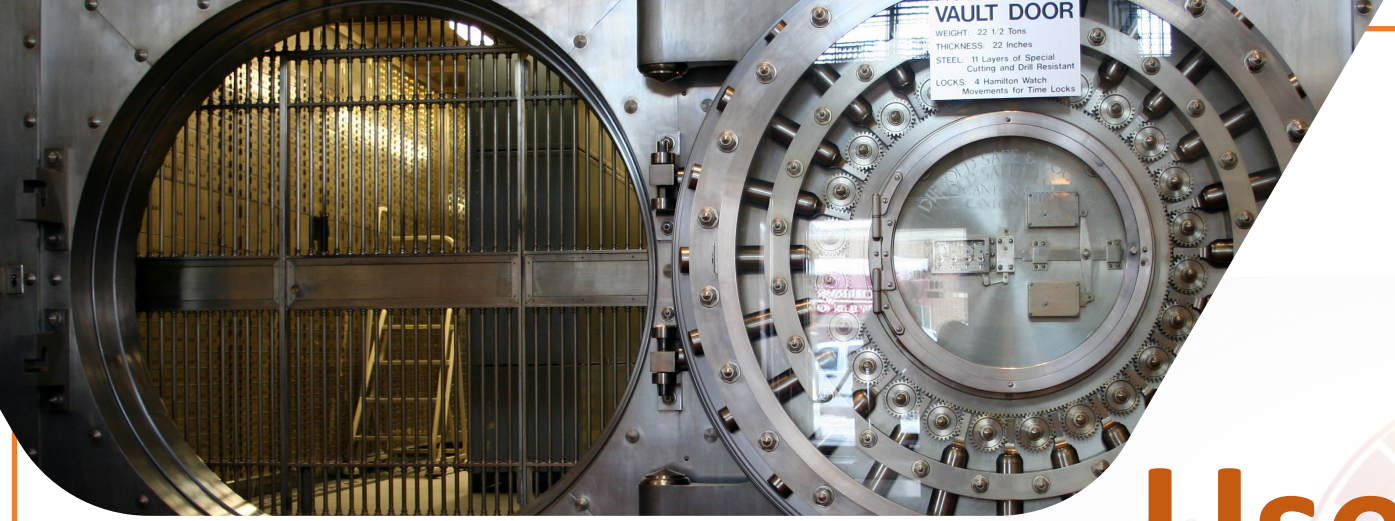
1. Google Bard claims the James Webb Space Telescope took the first pictures of an exoplanet outside our solar system.
   - Truth: Image taken in 2004, 17 years before James Webb Space Telescope launched.
2. Meta’s Galactica, an LLM designed for science researches cites a fake paper about the topic credited to a real author working in a relevant area.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Concerns

- Data security and privacy concerns arise in the use of AI, particularly in fraud detection and prevention.
- Collaboration and data sharing among financial institutions are needed to improve fraud detection tools.
- The historical data used to train fraud-detection models may contain biases that need to be addressed.

MONARCH ISC
INFORMATION SECURITY CONSULTING



Use Cases

MONARCH ISC
INFORMATION SECURITY CONSULTING

You are already using it:

ZEST AI

CROWDSTRIKE

CREST FINANCIAL

ARCTIC WOLF

feedzai Research

MONARCH ISC
INFORMATION SECURITY CONSULTING

What are We Calling It?

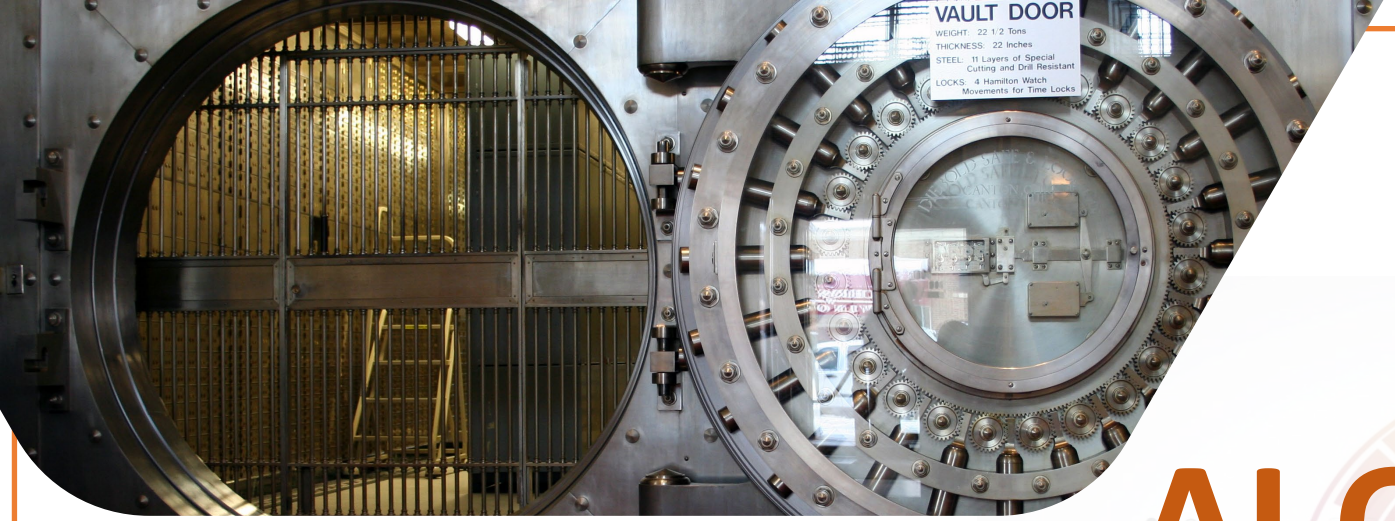
- The intellectual community has a new name for AI
  - “Plagiarism Software”
  - Does not create or produce original thought.
  - Very fast learning and recompiling of existing data and images.
  - Different enough to evade copyright law.

AI Use Cases for Banking

Artificial Intelligence in Banking

- Customer Support / Front Office
- Fraud Protection / AML
- Cybersecurity Risk Management
- Lending/Underwriting & Credit Risk Management
- Predictive Banking
- Marketing
- Universal Search
- Enhanced Stress Testing

MONARCH ISC
INFORMATION SECURITY CONSULTING



AI Opportunities

MONARCH ISC
INFORMATION SECURITY CONSULTING

- *Banks have huge amounts of unleveraged customer data.*
- *Private AI is a growing option that solves many problems*.

AI Opportunities

Private AI

- **Investment strategies**
  - AI can help create more effective investment strategies by analyzing large amounts of data to identify patterns and trends.
- **Personalized advice**
  - AI can analyze clients' financial behaviors, investment preferences, and risk tolerance to provide tailored advice and solutions.
- **Operational efficiency**
  - AI can automate routine tasks to increase efficiency.

MONARCH ISC
INFORMATION SECURITY CONSULTING

AI Opportunities

Private AI

- **Predictive Analytics – Customer behavior**
  - Deep historical data analysis will reveal patters of customer behavior, including customer churn / defection.
  - Costs less to keep a customer than acquire new
- **Automated Document Management**
  - process sensitive documents, such as loan applications and KYC verification forms.
- **Customer experience**
  - AI can help offer a more personalized service based on a client's track record, preferences, and other aspects of their lives.

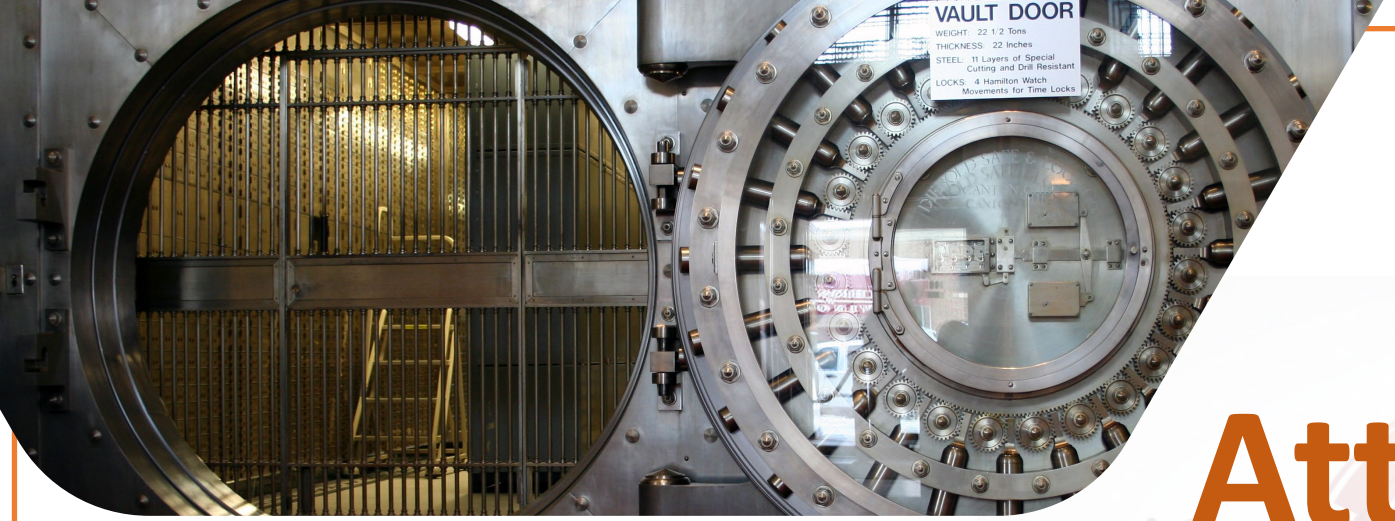
MONARCH ISC
INFORMATION SECURITY CONSULTING

AI Opportunities

Private AI

- **Other benefits of AI in private banking include:**
  - Improved decision-making
  - Enhanced client interaction
  - Product innovation
  - Data-driven insights
  - Regulatory compliance
  - Data is not included or derived from public sources
  - Risk reduction from data management/control internally

MONARCH ISC
INFORMATION SECURITY CONSULTING



Attack Vectors & Fraud

MONARCH ISC
INFORMATION SECURITY CONSULTING

Enhanced Threats

Social Engineering

- Use of LLMs to enhance phishing targeting, BEC, and other fraud.
- More realistic misrepresentation in gender, background, language, and statuses.
- Use of social media posts and messaging to build extremely difficult-to-detect impersonation.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Enhanced Threats

Malware / Code Generation

- Development of new malware or variants of existing code.
- Circumvention of signature-based systems with rapid minor changes to code.
- Enhanced ability to create spoofed sites and deceptive URLs.
- Code Poisoning will become more frequent attack vector.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Enhanced Threats

Vulnerability to Exploitation

- Using available tools to enhance attack automation.
- Reduce the time between identifying a vulnerability and developing its exploitation.
- Patching deployment timeframes need to tighten.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Enhanced Threats

Disinformation

- Combination of multi-media types that are “deep fake” and greatly increased information reach will speed the adoption of false information as truth.

MONARCH ISC
INFORMATION SECURITY CONSULTING

Enhanced Threats

Adversarial Machine Learning

- **Data Poisoning** – Corrupt the training data used by AI systems to corrupt the output of a system.
  - Availability Poisoning – DoS gets a facelift.
  - Targeted Poisoning – Poison a small set of samples in the ML model.
  - Backdoor Poisoning – Poison the training data, leading to misclassification.
  - Model Poisoning – Direct modification of the ML model to inject malicious functionality.

Enhanced Threats

Adversarial Machine Learning

- **Data Leakage** – Inverting the AI system model to gain access to confidential data
- **Evasion** – Strategic queries that corrupt the model to generate a desired outcome
- **Model Extraction** - Steal an AI model by creating a functionally equivalent model by use of iterative queries
- NIST AI 100-2 E2023 Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations: https://csrc.nist.gov/pubs/ai/100/2/e2023/final

MONARCH ISC
INFORMATION SECURITY CONSULTING

Enhanced Threats

Impersonation and Synthetic Identity

- More easily mimic voice, images, and video to impersonate customers and employees and beat the ID verification controls in place (which are already often out of date).
  - Includes key-stroke dynamics, and other bio-identifiers.
- Create entirely fictional identities that are composites of real people.
  - Over time, these fictional identities, with real accounts, behave like real customers.
  - A recent report by Wakefield Research commissioned by Deduce describes an acceleration in the growth of synthetic identity fraud. Wakefield's findings indicate that **87% of the companies they surveyed had extended credit to synthetic customers** and that synthetic identity fraud increased by 17% over the two years prior to October 2023.

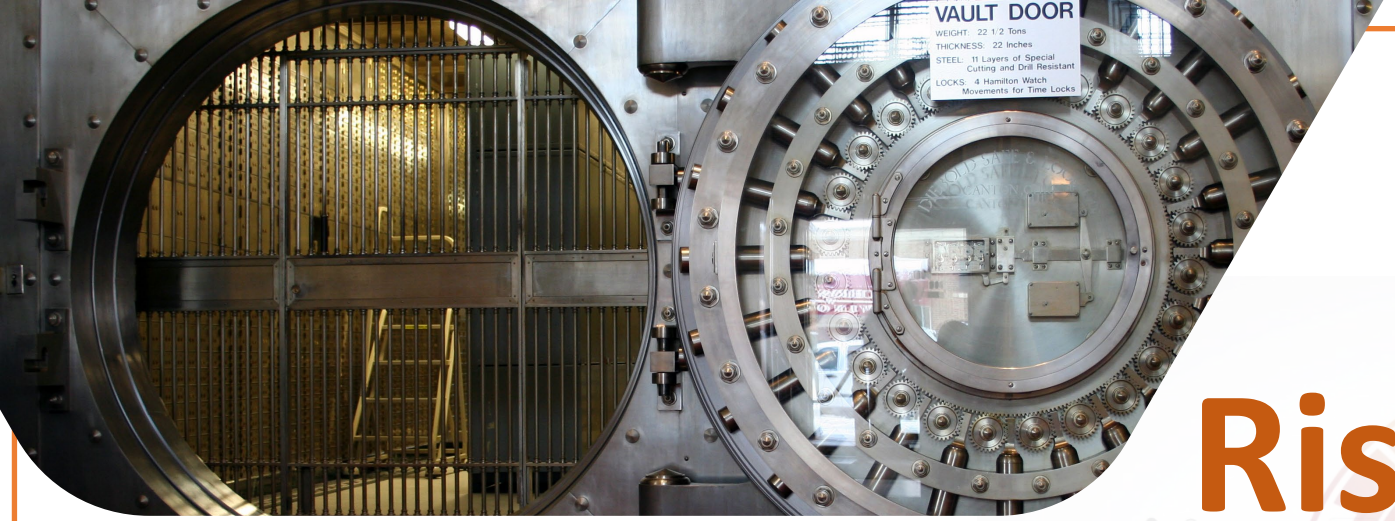
MONARCH ISC
INFORMATION SECURITY CONSULTING

Enhanced Threats

Third-Party Risks

- Increased direct and indirect reliance on third-party infrastructure and data.
- Much of this increased risk-surface will be difficult to identify and assess with traditional “SOC Review” based programs.
- Increased risk when handling unidentified proprietary data or training-data licenses.
- Ethical questions arise related to where and how data was captured and distributed via the extended supply chain.

MONARCH ISC
INFORMATION SECURITY CONSULTING



Risk Mitigation & Defense

MONARCH ISC
INFORMATION SECURITY CONSULTING

Working with AI Risk

Leverage Existing Risk Program

- Get Risk Department busy with the research.
- Add AI specific elements to what you already have
  - Business Line Controls (First Line).
    - Risks associated with AI systems and business offerings using them.
  - Corporate Risk Management (Second Line).
    - Compliance and Risk Management structures – Comms elevating to management.
  - Auditing Risk Controls (Third Line).
    - Monitoring, controls, and reporting.
- Principles are the same across control strategies.
- Add to Risk Appetite Statement(s).

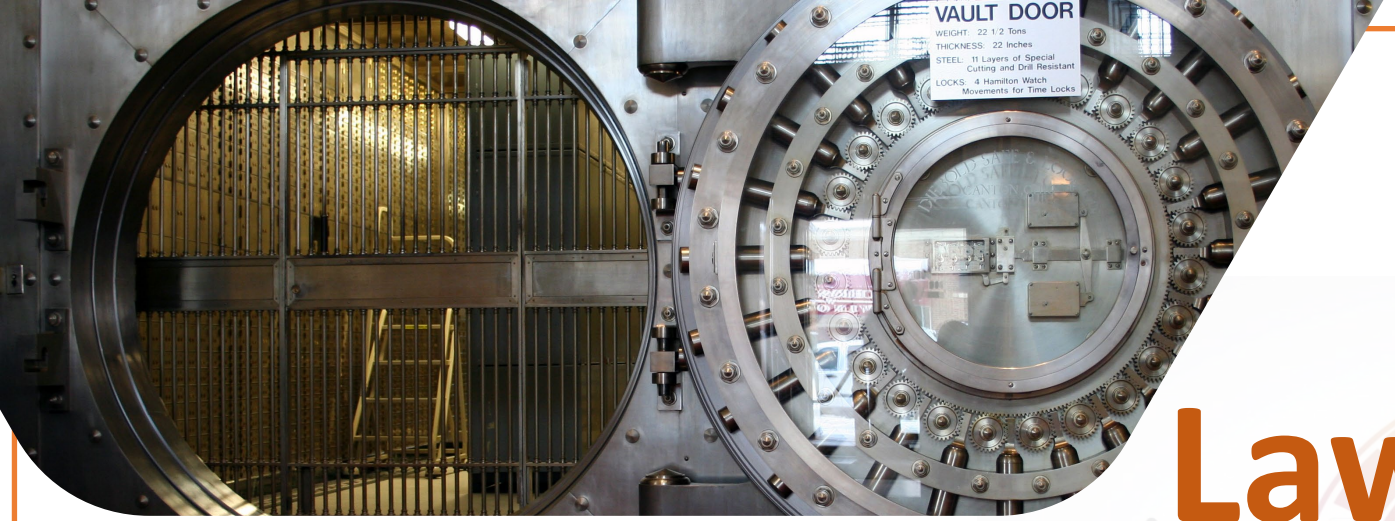
MONARCH ISC
INFORMATION SECURITY CONSULTING

Working with AI Risk

Level-Up Third-Party Risk Management Program

- Go beyond “SOC Review”
  - Don’t take no answer for an answer
  - Source code security practices
  - SDLC security
  - Developer training and credentials
  - Data source validation
  - Enhanced contract language
- Identification of fourth- and fifth-party supply chain use.

MONARCH ISC
INFORMATION SECURITY CONSULTING



Law & Regulation

MONARCH ISC

US Law

National AI Initiative Act of 2020

- Developing computers and robots that can behave in ways that mimic and exceed human capabilities.
- A coordinated program across the entire Federal government to accelerate AI research and application for the Nation's economic prosperity and national security.
- The mission of the National AI Initiative is to ensure continued U.S. leadership in AI research and development, lead the world in the development and use of trustworthy AI in the public and private sectors, and prepare the present and future U.S. workforce for the integration of AI systems across all sectors of the economy and society.
- https://ai.gov/

US Law

Algorithmic Accountability Act of 2023

- One of 93 Federal bills before the Congress, total from both chambers.
- Focused on Automated Decisioning Systems.
- Requires companies to assess the impacts of the AI systems they use and sell, creates new transparency about when and how such systems are used, and empowers consumers to make informed choices when they interact with AI systems.
- **Latest Action:** Read twice and referred to the Committee on Commerce, Science, and Transportation.

MONARCH ISC
INFORMATION SECURITY CONSULTING

US Law

Algorithmic Accountability Act of 2023

- Provides a baseline requirement that companies assess the impacts of automating critical decision-making, including decision processes that have already been automated.
- Requires the Federal Trade Commission (FTC) to create regulations providing structured guidelines for assessment and reporting.
- Ensures that companies that make critical decisions and those that build the technology are responsible for assessing the impact of decision processes.
- Requires reporting of select impact-assessment documentation to the FTC. Requires the FTC to publish an annual anonymized aggregate report on trends and to establish a repository of information where consumers and advocates can review which critical decisions have been automated by companies along with information such as data sources, high level metrics and how to contest decisions, where applicable.
- Adds resources to the FTC to hire 75 staff and establishes a Bureau of Technology to enforce this Act and support the Commission in the technological aspects of its functions make informed choices when they interact with AI systems.

US Law

Executive Order 14110

- Issued in October 2023, on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, takes a “whole of government” approach to the control, management, and use of AI, defining the technology as the following:
  - [A] machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments; … use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.” (15 USC § 9401(3)).
  - Tasks every US government agency, plus offices related to the president, to develop working groups to evaluate the development and use of AI; develop regulations for each agency; identify and establish public-private engagement (including advisory committees); and focus on the use of AI in specific technologies “to promote competition and innovation in the semiconductor industry, recognizing that semiconductors power AI technologies.”

MONARCH ISC
INFORMATION SECURITY CONSULTING

Case Law

Latest Case Law Trends

- Privacy
- Copyright
- Trademark
- Right of Publicity and Facial Recognition
- Tort

MONARCH ISC
INFORMATION SECURITY CONSULTING

Case Law

Latest Case Law Trends

- Privacy Cases
  - Over a two-week period in June and July, 2023, a number of federal class action lawsuits were filed in the US District Court for the Northern District of California, many by the same law firm, against the developers of some of the most well-known generative AI products on the market, including OpenAI, Inc. (OpenAI) and Alphabet Inc./Google LLC (Google).
  - On 28 June 2023, for example, in P.M. v. OpenAI LP,1 an anonymous group of plaintiffs filed suit against OpenAI LP (OpenAI) and Microsoft, Inc. (Microsoft) alleging that OpenAI stole private and personal information belonging to millions of people by collecting publicly-available data from the Internet2 to develop and train its generative AI tools—including ChatGPT (an AI text generator), Dall-E (an AI image generator), and Vall-E (an AI speech generator).

https://www.klgates.com/Recent-Trends-in-Generative-Artificial-Intelligence-Litigation-in-the-United-States-9-5-2023

MONARCH ISC
INFORMATION SECURITY CONSULTING

Case Law

Latest Case Law Trends

- Copyright Cases
  - Numerous cases have been filed against generative AI developers asserting violations of copyright law. Foundationally, these claims amount to a challenge to developers' use of data collected from the Internet to train generative AI models—and whether collecting and using publicly-available data that may be subject to copyright protection constitutes infringement.

  - Andersen v. Stability AI Ltd.5 In that case, plaintiffs Sarah Andersen, Kelly McKernan, and Karla Ortiz, on behalf of a putative class of artists, alleged that Stability AI, Ltd. and Stability AI, Inc. (collectively, Stability AI) and others scraped billions of copyrighted images from online sources, without permission, in order to train their image-generating models to produce seemingly new images without attribution to the original artists who supplied the training material.

https://www.klgates.com/Recent-Trends-in-Generative-Artificial-Intelligence-Litigation-in-the-United-States-9-5-2023

MONARCH ISC
INFORMATION SECURITY CONSULTING

Case Law

Latest Case Law Trends

- Right of Publicity and Facial Recognition
  - Television personality Kyland Young filed a class action complaint in the US District Court for the Central District of California against software developer NeoCortext, Inc. claiming that NeoCortext's AI-powered "Reface" application, which allows users to digitally "swap" their faces with celebrities and public figures in photos and videos, constitutes a violation of the common law right of publicity, protected by California's Right of Publicity Statute.
  - Flora v. Prisma Labs, Inc.,17 a February 2023 suit filed in the US District Court for the Northern District of California, in which a putative class of Internet users alleged that Prisma Labs, Inc.'s portrait-generating application, Lensa, scanned the facial information of Internet users without their consent, in violation of Illinois' data privacy statute.

https://www.klgates.com/Recent-Trends-in-Generative-Artificial-Intelligence-Litigation-in-the-United-States-9-5-2023

MONARCH ISC
INFORMATION SECURITY CONSULTING

Risk-Based Policy

MONARCH ISC

AI Security Policy

Policy Areas

- Model / System Selection
  - Due diligence and risk assessment required.
- Use / Adoption of AI Platforms
  - Requirements for departmental adoption.
  - Requirements for access control and acquisition of training data.
- Risk Assessment
- Data Privacy
- Information System Controls
- Acceptable Use
- Model Transparency
  - Can you explain what it does?
- Bias mitigation
  - What does the model specifically do to mitigate bias?
- Third-Party Risk
  - Deeper due diligence requirements when AI is included.
  - Contract language

MONARCH ISC
INFORMATION SECURITY CONSULTING

Use Policy Language

Departmentalize the Due Diligence

“Department personnel must complete the <<form name>> and submit to their manager before it is approved for use by the <<Governance Authority>> for use. Evaluation criteria include:

1. Describe use/benefit the Bank.
2. Describe the tool's security features,
3. Describe terms of service, and privacy policy.
4. Review application developer reputation, to include review of available independent audit and security testing reports.
5. Describe/list any third-party system interfaces where this application/system shares Bank data to be processed, stored, and/or transmitted.
6. Describe how access is provisioned, who will require access.
7. Describe authentication requirements for the application/system, including single or multifactor authentication, password length and complexity requirements, and password expiration requirements.

Once the evaluation is submitted for review and approval, a status will be communicated to the requesting department, and if approved, the application/system will be added to the Bank Approved Software list.”

MONARCH ISC
INFORMATION SECURITY CONSULTING

Use Policy Language

Information System Controls

- Regular user access monitoring are in place for the AI system, model, and training data.
- Multifactor authentication is used when signing into the AI system or accessing the AI model and training data.
- All sensitive data used in with AI models is encrypted at rest.
- Encryption key management best practices are followed, including, but not limited to:
  - Use only approved key generation methods.
  - Keys are stored only on designated repositories.
  - Sending or receiving encryption keys requires the use of a secure connection.
  - Records of key sharing is accurate and up to date.
  - Lost or stolen key-enabled devices are reported immediately.
  - Key management activities are regularly logged and audited
  - Follow key-rotation schedule
  - Delete keys after a potential compromise

Recap

- Generative AI is Machine Learning.
- Generative AI offers opportunities to the business, and challenges that go beyond the business to include larger cultural complexity.
- As far as we've come, it has just begun.
- AI is coming along with many banking systems across front and back office, internal and customer-facing systems.
- Integrate AI-specific risks with the current Risk Program.
- Third-Party Risk Management must go deeper into the relationships at fourth- and fifth-party extension.
- Due Diligence research must also go deeper into the code and training data sets employed by ML models.
- Regulations are coming.
- Integrate AI-specific policies into the current ISP.

MONARCH ISC
INFORMATION SECURITY CONSULTING

MONARCH ISC

Northern New England CEO Summit

Questions?

MONARCH ISC

Northern New England CEO Summit

Thank you!

John Rogers, CISSP
Senior Advisor
john@monarchisc.com
Monarchisc.com

References

- Managing Artificial Intelligence-Specific Cybersecurity Risk in the Financial Services Sector, US. Treasury Department, 3/2024
- https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf
- https://www.techtarget.com/searchenterpriseai/definition/generative-AI
- https://www.klgates.com/Recent-Trends-in-Generative-Artificial-Intelligence-Litigation-in-the-United-States-9-5-2023
- https://www.klgates.com/Recent-Trends-in-Generative-Artificial-Intelligence-Litigation-in-the-United-States-9-5-2023
- 5 Big Myths of AI and Machine Learning Debunked | Splunk
- https://www.javatpoint.com/history-of-artificial-intelligence#:~:text=%20The%20emergence%20of%20intelligent%20agents%20%281993-2011%29%20,like%20Facebook%2C%20Twitter%2C%20and%20Netflix%20also...%20More%20
- https://www.financierworldwide.com/strengthening-aml-protection-through-ai#.YJQkQ8CSnD4
- https://emerj.com/ai-sector-overviews/ai-in-banking-analysis/
- https://enterprisebotmanager.com/7-of-the-best-chatbots-in-banking-and-what-to-watch-for-next/#:~:text=The%20Seven%20Best%20Examples%20We%20Know%20Of%3A%201,...%206%20Wells%20Fargo.%20...%207%20Cleo.%20
- https://www.fincen.gov/news/news-releases/treasurys-fincen-and-federal-banking-agencies-issue-joint-statement-encouraging
- https://www.businessinsider.com/ai-in-banking-report
- https://builtin.com/artificial-intelligence/ai-finance-banking-applications-companies
- https://www.charteredbanker.com/resource_listing/cpd-resources/the-biggest-barriers-to-ai-in-banking.html?fbclid=IwAR1ltpCSVQmMSDJtiFy-C-PPgZIKALrvxyNj21XK0zPdu-NfY4rxKM8qYZQ
- https://venturebeat.com/2021/05/06/proper-data-hygiene-critical-as-enterprises-focus-on-ai-governance/
- NIST AI Risk Management Framework: Initial Draft

MONARCH ISC
INFORMATION SECURITY CONSULTING