FIR RISK NEWS

Artificial Intelligence (AI): CIA and NSA weight in.

INSIDE

TOP FINDS THIS MONTH

AI at the CIA

AI Security Best Practices from the NSA

FIR RISK NEWS
Every month, we bring to you new sources and cybersecurity news for your review

FIR RISK INSIGHTS
We will bold in RED key takeaways to consider for your business

Top finds this month

- By Bruce Bird, Principal, FIR Risk Advisory, LLC

FIR Quarterly, our flagship fraud intelligence report, is designed to keep business leaders informed of the digital fraud landscape. We include insights throughout the report to highlight must read content. We published our first edition on April 24 and have made this report available for FREE, download **here**.

The Langley Files latest podcast, featured below, is a must listen for Leaders and Teams using AI in your business.

The National Security Agency latest cybersecurity advisory for best practices on securing AI is comprehensive and a must read for all organizations deploying externally developed AI systems.

AI at the CIA

File 015- Spies Supercharged: Talking AI and Digital Innovation at CIA is a fascinating and informative listen to hear from **CIA's Deputy Director for Digital Innovation, Juliane Gallina** and **CIA's Chief Artificial Intelligence Officer, Lakshmi Raman.** Both Juliane and Lakshmi share their origin stories, inspirations, and how AI will help protect America from threats around the world.

Pillars of CIA's AI strategy:
AI as Intelligence Topic: Work to collect, track, analyze our adversaries' plans, use, and intentions with respect to AI.
AI as Mission Enabler: How are we using AI capabilities to help us with our own mission and business.
AI Governance and Evaluation: Accountability and process to govern the process and adoption for these tools.

> **"AI + a human will really help us to outpace where we are currently"**
>
> *-JULIANE GALLINA*

Implications of AI for National Security:

PERILS:
Risk of Disinformation- AI will be used to create very convincing fake news, videos, audio recording to help spread misinformation and disinformation to manipulate public opinion. Deepfake information!
Risk that AI will make Cybersecurity harder- How AI is being used to improve the quality of phishing emails; how hackers are developing finely tuned LLMs (Large Language Models) specifically to create malware!

PROMISE:
LLMs can be used to improve Cybersecurity- can help detect cyber-attacks by analyzing and recognizing those patterns in large amounts of data.

Can help us- to automate business tasks that provide efficiencies, augment cybersecurity, automate how we access and process information. Incorporating LLMs in generative AI into CIA's open-source mission, helping to gain deep insights into very expansive data sets. Incorporating AI into the applications CIA is using every day! Key partnership between Technology and Operations, Analysis, and other components of CIA.

DDI North Star- Human/AI Teaming: when you team a human with AI, you will beat both AI and the Human.

> **Quote from Juliane** *"AI + a human will really help us outpace were we are currently. It's the human machine teaming that is going to get us where we need to go. We need the benefits and computational ability that a model can provide to our already incredibly experienced analyst's who have really strong tradecraft to help them move further down the field."*

"AI + ethical development is a super-power we have"

-LAKSHMI RAMAN

Challenge of LLM that are generative: Being able to trace back to source material to support the intelligence recommendations!

> **Quote from Lakshmi** *"Our strong emphasis on ethical development, we need to ensure its being used responsibility and if we do that, it will benefit society as a whole, and also its actually going to work as we intend for it to work, that is a super-power we have."*

Access The Langley Files here
Listen to the podcast here

CIA INSIGHTS

Key Takeaways:

#1: AI + Human is a superpower and will be able to defeat either the AI or the Human!

#2: AI is a critical success factor, and our adversaries are already using AI to accelerate phishing and malware attacks!

#3: AI can be used to detect cyber-attacks.

NSA Cybersecurity Information Sheet (CSI) Summary:

On April 15, 2024, the National Security Agency (NSA) released a Cybersecurity Information Sheet for "Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems". Today's newsletter provides a briefing on highlights from the CSI:

- The report is intended for organizations deploying and operating externally developed AI systems on premises or in private cloud environments.
- As potential weaknesses in AI technology are discovered and techniques to exploit them uncovered, organizations will need to update their AI systems to address the changing risks.
- Malicious actors targeting AI systems often combines multiple attack vectors to execute operations that can effectively penetrate layered defenses.
- Securing an AI system involves an ongoing process of identifying risks, implementing appropriate mitigations, and monitoring for issues.

The CSI provides detailed best practices that are aligned with existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. 19 works cited are included at the end of the CSI with hyperlinks to each.

The Best Practices provide detailed guidance on the following 3 areas:

1. **Secure the deployment environment!**
   - 1.1. Manage deployment environment governance
   - 1.2. Ensure a robust deployment environment architecture
   - 1.3. Harden deployment environment configurations
   - 1.4. Protect deployment networks from threats

2. **Continuously protect the AI system**
   - 2.1. Validate the AI system before and during use
   - 2.2. Secure exposed APIs
   - 2.3. Actively monitor model behavior
   - 2.4. Protect model weights

3. **Secure AI operation and maintenance**
   - 3.1. Enforce strict access controls
   - 3.2. Ensure user awareness and training
   - 3.3. Conduct audits and penetration testing
   - 3.4. Implement robust logging and monitoring
   - 3.5. Update and patch regularly
   - 3.6. Prepare for high availability (HA) and disaster recovery (DR)
   - 3.7. Plan secure delete capabilities

Download the CSI here

To access the NSA's press release, see here

To access NSA Cybersecurity Advisories & Guidance, see here

NSA INSIGHTS

Key Takeaways:

#1: AI system weaknesses will need to be updated as adversaries find ways to exploit them!

#2: Malicious actors will attack AI using multiple attack vectors to penetrate layered defenses.

#3: AI Best Practices must be followed to secure the system!

Download your copy of FIR Quarterly from firriskadvisory.com for FREE!

DOWNLOAD FIR

Contact Us

Bruce Bird, Principal

Colorado, United States

970-689-2473 mobile

bbird@firriskadvisory.com

https://firriskadvisory.com/