ADVANCED CYBER SECURITY CENTER

CYBER RISK GOVERNANCE
Leveling Up in an Age of New Regulations and AI

Tackling the AI Juggernaut
Briefing Summary

November 2023

TRUSTED NETWORKS.
ADVANCING CYBER STRATEGIES.

ADVANCED CYBER SECURITY CENTER

Tackling the AI Juggernaut

AI brings tremendous opportunities, but also new risks, a huge new attack surface, and a host of ethical considerations. Successful executives will have to consider each before taking the AI plunge.

Three major factors driving the need for change:

- More data, public and private, readily accessible
- Tremendous advances in computing power
- New generation of sophisticated algorithms

Supporting Material:

- MITRE Atlas Framework
- NIST AI Risk Management Framework

Risks of AI

Adversaries can attack an AI application—often in under 90 minutes—at any level of the process.

AI is subject to 3 primary sources of risk:

1

Risks to AI systems and processes

- Poison the training data
- Attack the training process
- Reverse engineer the model
- Attack the operational data, camouflaging bad data as good
- Compromise the model scoring algorithm

"If a model is trained on bad data, it will not operate as intended when it moves to the inference phase."

Contact us

(617) 584-0581

jdinneen@acscenter.org

ADVANCED CYBER SECURITY CENTER

2

Compliance and Ethical Challenges
Every instance of AI use should be ethical, aligned with organizational imperatives, and strike the right balance between risk and reward. Sensitive data must be handled securely and in a privacy-safe way, all while ensuring regulatory compliance.

"The White House's recent Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, while not perfect, provides valuable guidance."

3

Reputational, Legal and 3rd Party Risk
Damage to a company's reputation can result from their own misuse use of AI and will extend to impact from 3rd parties, including liability for receiving and using copywritten material.

"Case law is important. Tracking about 20 laws worldwide, they are not focused on things we focus on. They are "only" focused on things that will kill you."

Contact us
(617) 584-0581
jdinneen@acscenter.org

ADVANCED CYBER SECURITY CENTER

Best practices to protect your AI program

Much of what needs to be done to protect your organization from the threats inherent to AI are similar to what is already being done to protect against other sorts of cyber threats.

What's different is the potential for real life harm.

AI Governance Committee

AI will be embedded into everything an organization does and its governance of policy, standards, and use should be managed by a diverse group, including:

- IT infrastructure, cyber and application security
- Risk, compliance, privacy and legal
- Data Protection / Governance
- Third Party Risk Management

"Consider creating a private AI sandbox. By internally sequestering large language models, there is no risk of mixing proprietary data with outside data, sharing data with competitors or adversaries, and tipping your hand through prompts.

Human controls and tight feedback loops

No matter where AI lives, however, human controls will be necessary at every level to protect against threats that could not have been predicted just weeks or months prior.

Contact us

(617) 584-0581

jdinneen@acscenter.org

ADVANCED CYBER SECURITY CENTER

Four steps to safe AI frameworks implementation

1 **Understand the use case** – Define the specific business problem AI will solve and the data needed to train the model. This will drive the policy, protocols, and controls that need to be implemented.

2 **Assemble the team –** Expand the composition of the team to include stakeholders across multiple departments, such as: business use case owners; security and cloud engineering; risk and audit teams; privacy and legal; data science and development teams; responsible AI and ethics team.

3 **Level set with AI Primer Education** – Help all stakeholders understand the basics of the AI model development lifecycle, the design and logic of the model methodologies, including capabilities, merits, and limitations.

4 **Apply safe AI frameworks implementation (SAIF) elements – Build and deploy AI systems in a secure and responsible manner with the six SAIF elements:**

1. Expand strong security foundations to the AI ecosystem.
2. Extend detection and response to bring AI into an organization's threat universe.
3. Automate defenses to keep pace with new and existing threats.
4. Harmonize platform level controls to ensure consistent security across the organization.
5. Adapt controls to adjust mitigations and create faster feedback loops for AI deployment.
6. Contextualize AI system risks in surrounding business processes.

Resources

AI Vendor Toolkit

ACSC Conference Presentation Slides

Contact us

(617) 584-0581

jdinneen@acscenter.org