STINSON

Security Considerations in the Adoption and Use of AI

Jenifer Shahan McIntosh, CIPP/U
Of Counsel, Stinson LLP

What is Old is New Again, Kind-Of

Data = Information

Privacy & Security = Secrecy & Protection

AI = Process for Use of Data

AI ≠ Predictable Results

ps – ask questions at any time…

Security Risks With Use of AI

- Security of the environment of development
- Security of the environment of deployment
- Security of the code itself & once deployed
- Security of data in training & in deployment
- Security of the outputs
- Ongoing security of operations

STINSON

AI Risks from a National Security Perspective

Insecure Development & Deployment Environments

- Insecure development environment allows TA to watch, copy or corrupt the model
- Insecure deployment environment allows TA to skew, take over or interrupt data ingestion & output

Malicious Code

- The AI as a whole
- Section of embedded code in the model to skew, take over or interrupt use

Poison Data

- Inaccurate, defective, old Training Data
- Data specifically skewed to produce a “predictable” erroneous result

So, What Really is Our Problem?

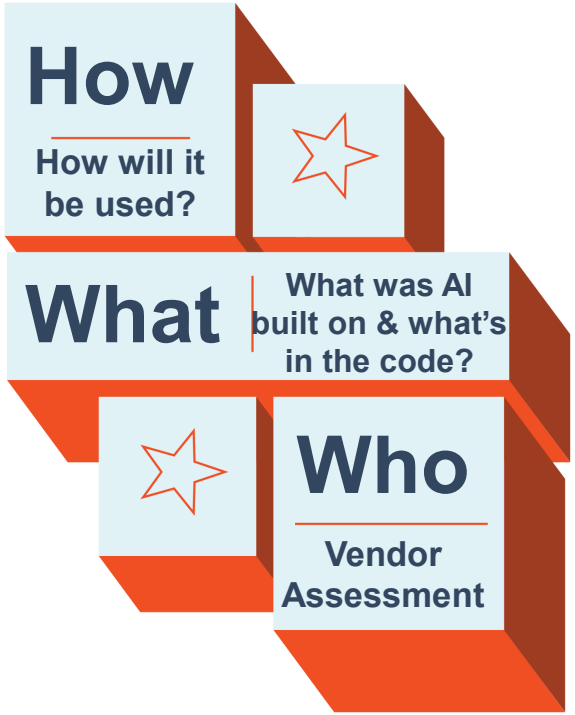
- Industry has been allowed to be lazy and sloppy with data, and with code.
- AI is not plug and play, certainly not initially.
- Assessment of How, What and Who are going to be essential.
- Humans must be in the loop at beginning, middle and end.

STINSON

Key AI Security Assessment Requirements

What can you do to manage risk?

- **Scope of Use Concerns**
  - Must-have for AI deployment is purpose-driven assessment
  - No “move fast and break things” given high risks of AI
  - Limit use to identifiable purpose and scope
- **Scope of AI Itself**
  - How was it built – i.e., what was the foundational model?
  - What is in the code – do you know?
- **Vendor Assessment**
  - Who are they?
  - Where does the model/code originate from
  - What do they do?
- **Security of the Environment is of Highest Priority**



STINSON

Jenifer Shahan McIntosh

(469) 530-6618

jenifer.mcintosh@Stinson.com