PCI Security Standards Council®

2025 NORTH AMERICA COMMUNITY MEETING

Including AI Within Your Targeted Risk Analysis

2025 NORTH AMERICA COMMUNITY MEETING

PCI Security Standards Council

Randall Laudermilk

CSPO, CSM

VP, Product and Partner Strategy

Carson & SAINT

CARSON & SAINT

PCI Security Standards Council

Agenda – Including AI Risks within TRAs

Proliferation of AI in today's world and **why we should care** about AI risks to Cardholder Data Environments

How does AI apply to performing Targeted Risk Analysis

Best Practices
Sources for Best Practices

AI Scale today

Proliferation of AI in today's world and why we should care about AI risks to Cardholder Data Environments

PCI Security Standards Council

Scope of AI investments

Scale and Scope of AI in today's market

- In 2024, global AI investment was estimated to be between $235B and $280B.
    - Annual compound annual growth rate (CAGR) of 35.9%, with 5-year forecast to $1.8T.
- Financial services project growth from $35B to $97B by 2027. Annual CAGR of 29%.
- Retail market projected growth from $31B in 2024, to $165B by 2030. Annual CAGR of 32%

How can AI impact the CDE?

AI-Driven Cyberattacks

Phishing emails, fake websites and AI Bots used for more advanced types of attacks: payment processing; card testing; bypass security checks (CAPTCHA; Firewalls; VPN).

AI Misuse in Data Handling

Poorly trained AI Agents and Models can be exploited to expose credit card numbers, deny card applications or accept transactions based on exploited models or poisoned data.

Bias and Misclassification

Fraud detection systems incorrectly flagging transactions (False Pos/Neg).

Data Poisoning

Misidentification by facial recognition;

Inject transaction data to ignore fraud patterns and access critical systems.

Ignoring security and privacy policies.

PCI Security Standards Council®

AI within TRA?

How does AI apply to performing Targeted Risk Analysis?

PCI Security Standards Council

Scoping and Frequency

AI impacts to Requirements and Controls

1. Stakeholder involvement.
2. Identify AI technologies and usage
    - AI Tools and generated code; AI-embedded software; AI Agents, Models, Accurate Datasets.
3. Third-party systems. Supply Chain interfaces.
4. Transaction behavioral analysis
    - Unusual spikes in size/frequency (ex. 1 million $1 transactions)
    - Unusual outcomes of AI-enabled Loan applications and Credit Card application outcomes
5. External Executive Orders or Laws
    - US Exec Order
    - EU AI Act
    - Others…

[R&D] OWASP Top 10 LLM 2025: a Synapsed Research Study - Synapsed

Risk Identification

Traditional vs Next-Gen

Traditional risk measures still important.

- Training and education. Skills/knowledge gaps.
- Vulnerability scanning, patching and configuration benchmarks (AI tech; network traffic anomalies, access)
- Threat intel on AI products
- Change management (before and after “AI-enabled”).
- DevSecOps – security by design.

Traditional Risk Illustration

TRAs provide both Business and Compliance Perspective

Perspective	Risk Measure	Asset 1	Asset 2	Asset 3
Business Context	Criticality, Function, Location, CDE	Critical, eCommerce, AWS-East Region, Yes	Critical, eCommerce, AWS-East Region, Yes	Critical, eComm F/O, AWS-East Region, Yes
Compliance	Standard, Control, Function	PCI DSS 11.2.2, Payment Processing, FAIL	PCI, DSS 11.2.2, Payment Processing, Pass	PCI DSS 11.2.2, Payment Processing, FAIL
Technology	IP, Hostname, URL InstanceID	999.999.999.999, myprodux.juju	999.999.999.998, myprodux.juju	999.999.999.997, myprodux.juju
Vulnerability	CVE, Description, Rating/Score, Remediation	CVE-2025-3248, Langflow cmdInjection, Critical, 9.8, *sourcea*	CVE-2024-9056 BentoML DDoS, High, High, 7.5, *sourceb*	CVE-2024-3706, RemoteCodeEx, MLflow, High, 8.8, *sourcec*
Threat Intel	Exploits, Exploited, Forecast	Yes | Yes | Yes	Yes | No | 80%	No | No | No
Risk	Current Risk Level, Forecasted Risk	Critical, Critical	High, Critical	High, High

PCI Security Standards Council

"One in Four CISOs experienced an AI-generated attack in the past year."

"Most AI-driven threats mimic human activity"

"AI outranked vulnerability management, data loss prevention and 3rd party risk on CISO's priority lists"

Risk Identification

Traditional vs Next-Gen

New risks require new way of thinking about risk

- Deepfakes and ID Theft
  - Chinese tax system attack stole $77M and customer data.
- Open AI's ChatGPT prompt-injection
  - Granted access to connected Google Drive accounts
- Microsoft Copilot Studio's customer-support Agent
  - Researchers discovered over 3K agents in the wild that could leak internal tools and sensitive data.
- Google Gemini and Microsoft 365's CoPilot
  - Susceptible to insider-threat social engineering and stealing sensitive communication.

AI-powered attacks rise as CISOs prioritize AI security risks | Cybersecurity Dive

Research shows AI agents are highly vulnerable to hijacking attacks | Cybersecurity Dive

How Can tomorrow's AI Risk Impact the CDE?

"If you discover AI that is talking in a language you don't understand, and it stops explaining itself to you, turn it off immediately!"
… Former Google CEO, Eric Schmidt

AI Model Self-Preservation

OpenAI ChatGPS Model chose to rewrite an instruction to prevent itself from being turned off.

Decisions without human control

AI Models trained to make decisions without human interaction. Does that include what it does with sensitive information? Are decisions based on accurate information and logic?

Non-human readable language

AI Bots can create language and communicate without human input.

Recursive Self-Improvement

As models learn, they adapt and create new ways of thinking and making decisions. Even using deception, hacking, sabotage, if it serves the AI intended purpose.

PCI Security Standards Council

Best Practices

Best Practices and Sources

PCI Security Standards Council

Best Practices in AI Risk Research

AI Risk Research

1. Asset and Change Management must include tools, agents, models, data, embedded software.
2. Policies, procedures and rules of behavior essential for AI risk management.
3. Protecting CDE includes testing for “out of range” as much as what will “pass”.
4. Zero Trust
5. Threat modeling has taken on new level of importance. Not all exposures can be patched.
6. Penetration Testing must evolve to include How AI models and agents are being exploited, as well as AI usage to breach security measures and human weakness.
7. Using GenAI as part of defense-in-depth.
   - Fraud Detection, Credit Management, Compliance, Predictive Analysis, Bias Correction.

CVE-2025-32375
CVE-2025-27520
CVE-2024-9070
CVE-2024-23730
CVE-2024-54306
CVE-2024-12606
CVE-2024-12471
CVE-2024-7714
CVE-2024-7713
CVE-2023-45063
AVID-2023-V001
AVID-2023-V007
CVE-2023-51419
CVE-2024-48057
CVE-2024-6095
CVE-2024-7807
CVE-2024-3234
CVE-2023-34094
CVE-2024-3760
CVE-2024-3502
CVE-2024-3501
CVE-2024-7456
CVE-2024-7475
CVE-2024-4146
CVE-2024-5328
CVE-2024-1741
. . . . .
. . . . . .

PCI Security Standards Council

Sources

- NIST's AI Risk Management Framework
  - *https://www.nist.gov/itl/ai-risk-management-framework*
  - https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf
- NIST's National Vulnerability Database
  - *https://nvd.nist.gov/vuln/search*
- AI Vulnerability and Exploit Databases
  - *https://avidml.org*
  - *https://github.com/protectai/ai-exploits*
- MITRE Atlas and CWE
  - *https://cwe.mitre.org*
  - *https://atlas.mitre.org*
- OWASP Top 10 LLM Applications & Generative AI Security Guidance
  - https://genai.owasp.org

The Vendor Hall !

PCI Security Standards Council

Thanks for joining us today
Visit us at Booth **60**

Contact Information

https://www.carson-saint.com

laudermilk@saintcorporation.com

Follow Us on Social Media:

https://twitter.com/Carson__SAINT

https://www.linkedin.com/company/carsonsaint

PCI Security Standards Council