AI Summit

October 7-8, 2025 | Orlando, FL

APCO International Summit Series

AI for Cybersecurity

Megan Bixler, CPE, RPL
Senior Technology Strategist
APCO International

Sean Scott
CTO
SecuLore Solutions

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

A COMPUTER
CAN NEVER BE HELD ACCOUNTABLE

THEREFORE, A COMPUTER MUST NEVER
MAKE A MANAGEMENT DECISION

- IBM 1979

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

Concerns About AI

"When you think about it, the most powerful technology of the last century was arguably nuclear weapons. The most powerful technology of this century is artificial intelligence. Nuclear weapons were built by governments that had the incentive to keep them safe. The incentives of those building AI is all about maximization of profit and business competition."

– Jen Easterly, Former CISA Director (2023)

- Alex Polyakov, co-founder and CEO at Adversa.ai: doesn't believe that much can be done to prevent the misuse of AI without a legal framework

- He warns that this should be done sooner rather than later
  - *"The earlier companies start initiatives, the better they will protect their systems and have a competitive advantage. Sometimes the goal is not to be **100% secure** but to be more secure than your neighbor." Criminals tend to attack the easiest target."*

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

AI Lowers the Barrier to Entry for Cyber Threats

FunkSec AI Driven Ransomware

What we Know

- Who is FunkSec:
  - Emerged in late 2024: Ransomware-as-a-Service (RaaS) Operation
  - **Inexperienced/Lack of Expertise**: AI-assisted development solutions to create malware
  - Includes a custom developed distributed denial of service DDoS tool
- Tactics: Double extortion and encryption
  - Low ransomware demands, sells data on dark web
- Targets: Majority of victims are in the US

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

AI Lowers the Barrier to Entry for Cyber Threats

FunkSec AI Driven Ransomware

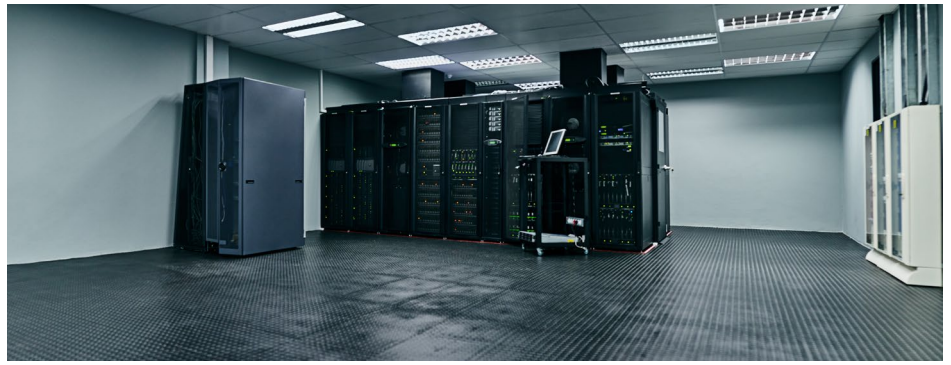
What we Know

- Who is FunkSec:
  - Emerged in late 2024: Ransomware-as-a-Service (RaaS) Operation
  - **Inexperienced/Lack of Expertise**: AI-assisted development solutions to create malware
  - Includes a custom developed distributed denial of service DDoS tool
- Tactics: Double extortion and encryption
  - Low ransomware demands, sells data on dark web
- Targets: Majority of victims are in the US

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

Cybersecurity Workforce Shortage + AI = Concerning Situation?

- Cybercrime is estimated to cost the world **$10.5 trillion** USD in **2025**.
  - If cybercrime were a country, this would be the **world's third largest economy**.
- The abundant need for more cybersecurity workers comes as emerging technologies such as AI has lowered the barrier to entry for cybercriminals to attack critical infrastructure across the United States



https://cybersecurityventures.com/official-cybercrime-report-2025/

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

Army of None: Autonomous Weapons and the Future of War

- The consequences of giving machines the capacity to select targets and destroy them without direct human guidance
- Autonomy is the ability of machines to perform a task or function on their own, without human supervision
- The danger that greater autonomy will further boost the speed of future engagements and reduce human oversight

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

AI Enhancing Cyber Posture

- Real-Time Threat Detection
- Automated Incident Response
- Predictive Analytics
- Threat Intelligence Integration
- Continuous Learning and Adaption
- Enhanced User Authentication
- Insider Threat Detection
- AI-Assisted Log Monitoring

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

Strengths for AI in Cybersecurity

Threat Hunting

- Replacing traditional techniques with AI can increase the detection rates up to 95%, but you will get an explosion of false positives. **The best solution would be to combine both traditional methods and AI.** This can result in high detection rates and minimize false positives.
- ECCs can also use AI to enhance the threat hunting process by integrating behavioral analysis.

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

Goals of Defensive AI

Automated Machine Learning Evolves Quickly

Anomalous Traffic Creates Identifiable Patterns

Scalable: Provides High-Capacity Protection

Adaptable: Stays In Step with Evolving Technology

Benefits of Behavior-Based AI Powered Cybersecurity

- Helps ECCs react faster to threats especially in complex hybrid network infrastructures.
- 3rd party cybersecurity monitoring is necessary and far more cost effective.

Cyber Tip!

A hybrid of AI driven detection and human analysis is the most effective cyber defense method.

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

Understanding Key Threats

- **Adversarial Attacks:** Malicious manipulation of input data to trick AI models (e.g., alerting a stop sign to mislead autonomous vehicles).
- **Hallucinations:** Corrupting training data to induce biased or incorrect AI behavior, compromising security.
- **Supply Chain Vulnerabilities**: Exploiting weaknesses in third-party libraries or components to inject malicious code.
- **Prompt injection:** Manipulating large language model prompts to trigger unintended actions,' like leading sensitive data.
- **Privacy Leakage:** AI models unintentionally revealing sensitive training data, exposing confidential information.

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

Cyber Threats: AI Systems

The Need for Continuous Monitoring

- **Model Drift:** AI accuracy degrades as real-world data changes, requiring training to maintain performance.
- **Evolving Attacks:** Cyber criminals use AI-driven malware that adapts to bypass defenses, demanding adaptive monitoring.
- **Anomaly Detection:** Continuous behavioral analysis establishes normal activity baselines, flagging unusual activity in real-time.
- **Key takeaway:** AI is not “set and forget.” Dynamic, ongoing monitoring ensures security and effectiveness.
- **Compliance:** The need for good policy around where, when and how we are guided by AI in critical decision making.

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

Password Hacking Techniques Through AI

Estimated Time it Takes AI to Crack a Password

Characters	Numbers Only	Lowercase Only	Upper and Lowercase
12	25 seconds	3 Hours	289 Years
13	3 minutes	11 Months	16,000 Years
14	36 minutes	49 Years	827,000 Years

Ways hackers use AI to automate cracking passwords and accounts:

- Smart brute-force attacks
- Intelligent dictionary attacks

PASSWORD TIPS

- Lock outs after repeated attempts
- Multi-factor authentication (MFA) is a way to fix this.

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

Using AI for Phishing Emails and Cyber Attacks

- Natural language generation of large language models (LLM) fits into phishing emails perfectly
- **GhostGPT**
  - AI model developed by cyber criminals
  - Uncensored AI model
  - Used to develop malware, phishing schemes
  - No user logs maintained
- Looking for bad grammar and spelling could be more difficult
- Scales content with greater ease
- Expect more targeting phishing content

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

Adopting Human Risk Management

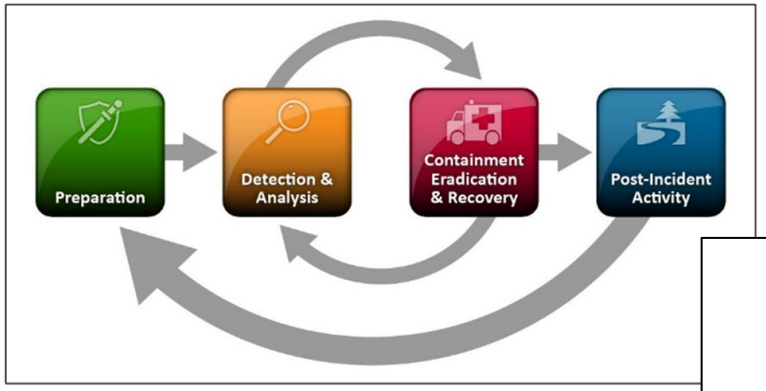
- Solutions that manage and reduce cybersecurity risks posed by and to humans through detecting and measuring human security behaviors and quantifying the human risk
- Initiating policy and training interventions based on the human risk
- Educating and enabling the workforce to protect themselves and their organization against cyber attacks
- Building a positive security culture

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

Mitigation Advice for AI Threats

- A top challenge for state and local governments is incorporating large language models into their workflows securely
- While there are ways to mitigate attacks against AI, agencies should not fall into a false sense of security, because there's no foolproof method of protecting AI from misdirection
- Continue to monitor, assess and react when problems occur
- Researchers should also develop better cybersecurity defenses
- Be alert and aware of these things and monitor continuously
- Don't connect systems that have access to sensitive data, like Social Security numbers or other personal information
- If a government agency wants to enable its employees to work more efficiently through the use of AI, like ChatGPT or a similar service, don't put in [training] data that's sensitive
- Don't hook that up to a system which allows access to that data either

Cybersecurity Education



APCO International
Leaders in Public Safety Communications

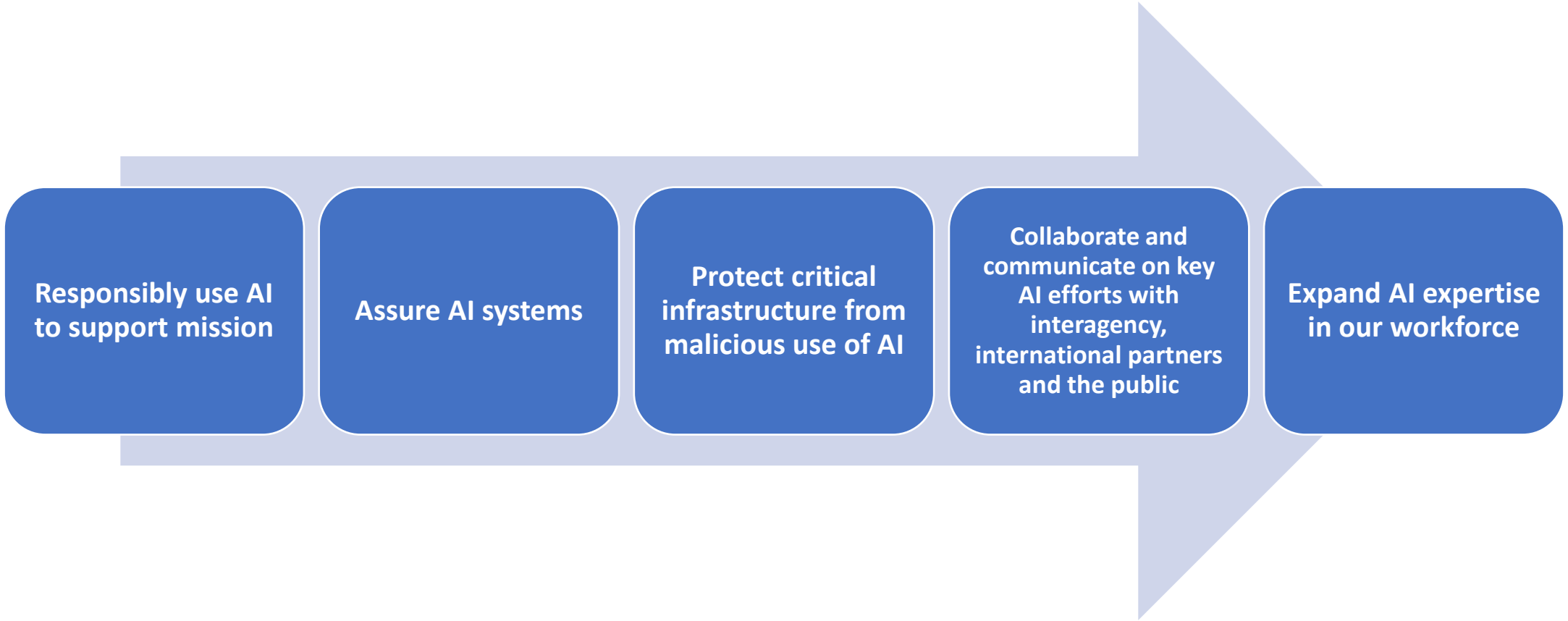
APCO 3.110.1-2019
Cybersecurity Training for Public Safety Communications Personnel

Approved American National Standard
ANSI

- NIST SP 800-61 R2 outlines five areas that ECCs can focus on to prevent a cyber-attack. They are:
  - Risk Assessments
  - Host Security
  - Network Security
  - Malware Prevention
  - User Awareness and Training
- APCO ANS 3.110.1-2019 Cybersecurity Training for Public Safety Communications Personnel
- ECCs should conduct **4-8 Hours** of cybersecurity specific training annually.
- All APCO Standards can be found here: https://www.apcointl.org/services/standards/find-standards/
- NIST Risk Management Framework 1.0

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

CISA's Roadmap for AI



AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series

Cyber Starts at the Top

CISA: #1 Pillar of Cyber Readiness is leadership

"Cybersecurity has broad implications for every aspect of an organization and its success. Therefore, addressing it requires influence from the top, from the leader."

Trent Frazier, deputy assistant director of the Stakeholder Engagement Division at CISA

Cyber is no longer an IT-only job

Leaders must own it!

AI Summit
October 7-8, 2025 | Orlando, FL
APCO International Summit Series