The Future Era of Urban Cyber Defense

...risks and frameworks.
Awareness to Shaping the Future
Present Thinking
The new Big Picture Risk
Designing a Winning Strategy
Present Thinking!

**Education**
- Lack of Awareness
- Phishing Simulations
- Training update lags
- Insider Threats

**Social**
- Social Engineering
- Phishing
- Baiting
- Reputation Damage

**Technology**
- Outdated Systems
- IoT Vulnerabilities
- Lack of Encryption
- Misconfigurations
- Ransomware
Big Picture Risk for City Leaders

We are in a new defensive posture with AI arriving. Over-reliance future on AI Tools might carry big consequences.

New Cyber Security tools are impacting the digital budget.

Cyber criminals are using AI to launch more sophisticated attacks. Some of these will use deepfaking audio and video to get access to client files.

Velocity mis-match between city leaders and cyber criminals is widening.
Velocity mismatch

Cities, towns, and municipalities run at a much different pace than a cyber-criminal.

• Budget cycles are different
• Local governments don’t like to be first on board.
• Overwhelmed with information
• Don’t want to invest in emerging technologies when there are bridges, roads, buildings needing repairs.
• Voters vote once a year.
• Generally there is not a level of buy-in from the voters.
DARK SIDE THREATS

Ransomware's effect on healthcare downtime.
Healthcare organizations have been and remain attractive targets for cybercriminals. A Comparitech study...

LockBit claims a cyberattack against Boeing.
A criminal organization tolerated and enabled by the Russian government claims to have extracted sensitive data...

Octo Tempest: a gang with an international reach.
English-speaking, and willing to use violent threats against its prospective victims...

Microsoft: Octo Tempest is one of the most dangerous financial hacking groups

MOVEIt bug impacts state governments. Johns Hopkins suffers data breach.

A creepy new geolocation payload for Smoke Loader. Speed of criminal attack, malware delivery, and the evolution of malicious AI. Ransomware at a Belgian social services agency.
The most dangerous hacks aren't into our computers, but into our minds.

- ChatGPT & Matthew Bertram

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

By Catherine Stupp
Updated Aug. 30, 2019 12:52 pm ET | WJ & Pro

Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 ($243,000) in March in what cybercrime experts described as an unusual case of artificial intelligence being used in hacking.
Cybersecurity

- AI model poisoning
- Deepfakes
- Malware
- Bypass CAPTCHA
- End-point exploitation

Auto Solve
Google reCAPTCHA

I'm not a robot

How To Bypass Google Recapture

By worm • July 27, 2023

Amidst this digital revolution, certain security measures have been put in place to safeguard the online ecosystem. One such measure is CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), which has been adopted by websites and online services to prevent automated bots from engaging in malicious activities. While CAPTCHA serves its...
AUTO-GPT ATTACKS

Can integrate many attack vectors (phishing deepfake, malware) into a coordinated strategy

Attacks can unfold over days, weeks, or months and be extremely difficult to detect

Can automatically update strategy and adapt to unexpected obstacles or new information
Designing a Winning Cyber Security Strategy
ENHANCING YOUR DEFENSES

Adopt the CISO mind-map
AI powered threat prevention across attack vectors
Eliminate email from business processes
Aggressive process automation strategy
Embedding fraud/anomaly detection AI into processes

In the digital arms race, our best defense is not just better technology, but better awareness - ChatGPT
- Security Operations
- Risk Management
- Legal and Regulatory
- Business Enablement
- Security Culture
- Identity Management
- Governance
- Leadership Skills
The collaborative synergy between the various departments leadership and the technology group is crucial.
Share 6 reasons why you would want to add AI skills requirements to job descriptions?
Questions?