

Cyber Security

.....risks and frameworks.

The Future Era of Urban Cyber Defense



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Outdated Systems IoT Vulnerabilities Lack of Encryption Misconfigurations Ransomware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 <u>Risk</u> 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



CW Oct 25, 2023

115/6.15.23

Ransomware's effect on healthcare downtime.

Healthcare organizations have been and remain attractive targets for cybercriminals. A Comparitech study...

cwpro



CW Oct 30, 2023 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 a international reach.

CW Oct 27, 2023

cwpro

English-speaking, and willing to a violent threats against its prospec Microsoft: Octo Tempest is one of the most dangerous financial

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





cw

CW Oct 24, 2023

A creepy new geolocation payload for Smoke A creepy new geolocation payload for >moke Loader. Speed of criminal attack, malware delivery, Loader. Speed of criminal attack, maiware delivery, and the evolution of malicious AI. Ransomware at

Belgian social services agency.

.

mfV

FPO

University -

disclose

Ep 1891 | 8.23.23

Social Engineering

Persuasion tra Deepfakes

Business Email

The most dange into our comput minds.

- ChatGPT & Matthe

THE WALL STREET JOURNAL.

World Business U.S. Politics Economy Tech Finance Opinion Arts & Culture Lifestyle Real Estate Personal Finance Health Science Style Sports 📿

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

Scams using artificial intelligence are a new challenge for companies



PHOTO: SIMON DAWSON/BLOOMBERG NEWS

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

in

Ì

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.



Al model poisoning

 $\mathbf{D} \mathbf{A}$

Deepfakes

Malware

Bypass CAPTCHA

®End-point exploitation

Auto Solve Google reCAPTCHA

reCAPTCHA Privacy - Terms

ноw то

How To Bypass Google Recapture

I'm not a robot

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...

READ MORE →





ENHANCING YOUR DEFENSES

FPO

Adopt the CISO mind-map

Al powered threat prevention across attack vectors

> Eliminate email from business processes

Aggressive process automation strategy

Embedding fraud / anomaly detection Al 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

Security O			gal and Regulate		
Aon A Protection Encryption, PKI, 115 Data Loss Prevention (DLP) User Behavior Analytics (UBA) - finail Security - Cloud Access Security Broker (CASB) Network Security - finewall, IDS/IPS, Proxy - filtering - VPN, Socurity Gateway - DooS Protection - Application Security	Detection Log Management/SIEM Continuous Monitoring Network Security Monitoring NetRow Analysis Advanced Analytics Threat Hunting Penetration Testing Red Toam Vulnerability Scanning Web App Scanning Bug Bounties Human Sensor Data Loss Prevention (DLP)	Compliance • PCI • SOX • HIPMA/HITECH • FREC, CAT • FREC, CAT • NERC CIP • NIST SP 800-37 and 800-33 • NIST 800-61 • NIST 800-61 • NIST 800-61 • NIST 800-61	 Privacy Privacy Shield EU GDPR CCPA Audit SSAE 16 SOC 2 ISO 27001 NIST SP 800-53A COSO 	Investigations Output	• S • Aps • Cloud C • Cloud C • Cloud C • Cloud G • Bring Vc • Mobile • Bring Vc • Mobile • Bring Vc • Internet • Internet
Threat Modeling Ossign Review Secure Coding Static Analysis WAF, RASP Endpoint Security Anti-virus, Anti-malware HIDS/HIPS, FIM App Whitelisting Secure Configurations Zero Trust	User Behavior Analytics (UBA) Security Operations Center (SOC) Threat Intelligence Industry Partnerships Response Incident Response Plan Breach Preparation Tabletop Exercises Forensic Analysis Crisis Management	C	V SE	D-D	Machine Machine Mergers a Security Security Security Percept Beliofs
Fatch & Image Management	Breach Communications	TAP	171177	The A	Attitude Behavio
Risk Management Risk frameworks FAIR NIST RMF OCTAVE TARA Risk Assessment Methodology Business Impact Analysis Risk Assessment Process Hisk Analysis and	Identity & Access Mana Provisioning/Deprovisioning Single Sign On (SSO) Federated Single Sign On (FSS Multi-Factor Authentication Role-Based Access Control (Rd Identity Store (LDAP, Active Dis	D) MAC) rectory)			 Values Norms Models & Fogg Be Kotter's Prosci A AIDA Ma Engager
Quantification	Governance			Business Strategy	
Vulnerability Management Vendor Risk Management Physical Security Disaster Recovery Uness Continuity Planning es and Procedures Tment Flanning.	Strategy St	Workforce Planni Resource Manage Data Classificatio Records Managen Security Policy Creating a Securit Security Praining • Awareness Train • Role-Based Train	ment n nent ty Culture ning	Business Strategy Industry Knowledge Business Acumen Communication Skills Presentation Skills Strategic Planning Technical Leadership Security Consulting Stakebolder Manager	Roadn Busine Projec Em

Big Picture Cybersecurity Directional Strategy

Departmental Ownership

Data Activation

Governance

Risk Management & Frameworks

Security Cultural

Privacy and Compliance

Legal and Regulatory

Leadership Skills

The collaborative synergy between the various departments leadership and the technology group is crucial.

Technology Ownership

Detection

Prevention

Application Security

Network Security

Governance

Identity & Access Management

Security Operations

FPC



AUDIENCE QUESTION

Share 6 reasons why you would want to add AI skills requirements to job descriptions?

FPOV

