NY Metro Joint Cyber Security Conference & Workshop Report

Date: October 19 & 20
Location: Microsoft's Tech Center, 11 Times Square, NYC

Presentation 1: The Current State of Cybersecurity and the Importance of Awareness
Presenter: Lisa Plaggemier, National Cyber Alliance

Overview:

Lisa took the stage after Omar's opening remarks about the vast challenges in cybersecurity. While Omar laid the groundwork by discussing the issues faced by defenders against relentless attackers, Lisa provided deeper insights into the realms of behavioral science, password management, and the role of multi-factor authentication.

Key Points:

Behavioral Science & Cybersecurity:

The intricate roles of Capability, Motivation, and Opportunity in shaping online behavior.
A focus on learned helplessness theory, indicating how individuals often feel trapped in their digital habits.
A memorable quote by Lisa: "Facts don't change people's behavior; emotion does."
Password Management & MFA:

Varied methods of password storage, from physical notebooks to digital password managers.
Results from a survey conducted in San Francisco revealed gaps in MFA awareness but a positive trend in its adoption and continuous usage.
Education & Awareness Campaigns:

Reinforcing the idea that education equips individuals with tools to navigate digital spaces securely.
Introduction to campaigns like "Peace of Mind" and deep dives into "Pass Keys" and MFA observational research.

Presentation 2: Resilience in Cybersecurity and the Impact of Generative AI
Presenter: Viral Trivedi

Overview:

Viral Trivedi's segment shifted focus from individual online behaviors to the broader implications of artificial intelligence in the cybersecurity arena. He offered an in-depth view of the AI landscape in cybersecurity, its rapid evolution, and the implications for businesses and stakeholders. Let's delve into the key highlights from his presentation.

The AI Landscape in Cybersecurity:

1. Insights into LLMs AI: Large Language Models (LLMs) like ChatGPT have become crucial in projects spanning numerous industries. Their capacity to generate content, offer natural language capabilities, and provide insights from proprietary data has made them invaluable.

2. Emphasis on "Origination": There's an increasing trend towards strategies emphasizing tech-driven AI, ensuring that projects are at the forefront of innovation while staying rooted in their origin or source data.

3. Permanent Learning Biases: AI, while impressive, carries with it inherent biases. Understanding these biases is fundamental for ensuring cybersecurity and maintaining the integrity of AI-driven outputs.

Balancing AI's Potentials and Pitfalls:

1. The Dual Nature of AI: Generative AI has an intrinsic duality. While it's a tool capable of automating content creation, offering natural language capabilities, and democratizing data analysis, it's also susceptible to spreading misinformation, generating biases, and data exposure.

2. Viral's Perspective: A standout quote from Viral was, "AI won't replace people, but people who use AI will replace them." This underscores the notion that the future hinges on leveraging AI effectively and ethically.

Risk Management & Regulatory Challenges:

1. Securing Digital Platforms: It's paramount to embed security into the DNA of digital platforms. As generative AI projects pose major cybersecurity risks to enterprises, understanding elements like trust boundary risks, inherent model risks, and ensuring security best practices are essential.

2. Data Management Pitfalls: A significant portion of the presentation was dedicated to understanding the risks associated with data management. Notably, when employees harness third-party AI platforms, vulnerabilities can arise.

3. Regulatory Landscape: As generative AI's influence grows, so too does the complexity of regulatory oversight. Whether it's the evolving compliance guidelines from NIST or international AI laws, the landscape is continuously changing, making governance a challenging endeavor.

Strategies for Mitigation and Future Pathways:

1. Strong Governance: Only 35% of executives plan to focus on improving AI governance, while just 32% of risk professionals are currently involved in the early stages of generative AI applications. These numbers underscore the need for more comprehensive governance measures.

2. Mitigating Risks: A strategic approach involves implementing robust data governance, using sandboxed environments, employing differential privacy, and monitoring models at runtime. Additionally, understanding and tackling inherent risks like deepfakes, unauthorized impersonations, and theft of sensitive data are crucial.

3. Regulatory Complexities: The current cybersecurity regulations struggle with the unique challenges posed by generative AI systems. Issues arise from quality and safety regulations not being tailored for AI, data privacy regulations not covering synthetic data, and the challenge of protecting proprietary AI model IP.

Evolving Compliance Landscape:

1. Frameworks & Policies: Established frameworks, such as NIST AI risk management and the ISO framework for AI, are foundational for creating trusted AI applications. Moreover, with over 800 national AI policies from more than 69 countries, the compliance landscape is diverse and extensive.

2. Global Regulatory Approach: Different regions are taking distinct paths. The U.S., for example, is leveraging interim measures for AI safety, the EU is working on the EU AI Act, and China has introduced its first regulations on generative AI technology.

Stakeholder Roles and Responsibilities:

1. Risk Stakeholders: Various roles, from Chief Information Security Officers (CISOs) to Internal Audit, have unique responsibilities in the generative AI landscape. Whether it's mitigating

sophisticated phishing threats, enhancing data governance, or adapting risk assessment processes, each stakeholder plays a pivotal role in ensuring AI's ethical and efficient deployment.

2. Case Study Insights: The case study on the generative AI-powered medical consultation chatbot illustrated the need for cross-functional collaboration, aligned data practices, and prioritizing reliability and responsible AI practices.

Key Takeaways:

1. Balancing Innovation & Risk: Harnessing AI's power demands a fine balance between innovation and risk mitigation. Understanding AI's vulnerabilities is crucial to safeguard digital assets.

2. Actionable AI Security Strategies: From tackling algorithmic biases to preparing for adversarial attacks, having actionable insights is essential for fortifying AI systems against potential threats.

3. The Value of Collaborative Defense: Collective defense efforts, combined with stakeholder collaboration, are integral for securing AI ecosystems effectively.

4. The Role of People in AI's Promise: At the heart of generative AI's potential are the people. Investing in them, understanding the technology's limits, and empowering individuals to critically evaluate AI outputs is essential for realizing AI's promise fully.

Presentation 3: Cybersecurity Jobs: An In-Depth Analysis
Presenter: Adrianna Ladarola

Overview:

Adrianna's enlightening presentation detailed the landscape of cybersecurity jobs, with a particular focus on which roles are steady and which are volatile. The data presented painted a comprehensive picture of the industry's hiring trends and potential reasons behind them.

Cybersecurity Job Postings by Category:

Defense : 166,958
Develop : 72,052
Compliance: 42,204
Plan : 41,945
Response: 15,032
Offense : 10,570
Educate : 10,292
Manage : 4,931

Research : 2,495

Insight: Defense roles dominate the cybersecurity job landscape, indicating a heavy emphasis on protecting and safeguarding organizations' digital assets.

Top 25 Cybersecurity Roles:

Some notable roles and their respective job postings are:

1. Security Analyst: 79,535 postings
 - Responsible for enhancing the organization's cybersecurity posture by monitoring and responding to threats, implementing/enhancing security solutions.

2. DevSecOps: 56,850 postings
 - Professionals using a combination of programming, threat management, and communication skills to automate and integrate cybersecurity throughout the SDLC lifecycle.

3. Security Engineer: 35,832 postings
 - Engineers focused on developing and implementing security solutions for organizations.

4. IAMs Engineer (Identity and Access Management): 23,883 postings

5. Application Security Engineer: 10,741 postings
 - These engineers develop and test security components, proactively testing their security posture, shaping engineering best practices, and working with the security team to educate.

Volatility in Job Roles:

Why Volatile:
1. Analyst:
 - They form the largest teams, making it easier to consolidate roles.

2. DevSecOps:
 - The rise in demand is due to digitalization post-COVID.
 - These professionals are scarce, making them hard to find.
 - Shift left material in job postings raises questions on its practical implementation.

3. Security Engineering:
 - Being the second-largest team, roles can be easily consolidated.

4. IAM:
 - A significant push towards digitalization was seen pre-pandemic, raising questions about the recent demand surge.

Why Not Volatile:

- Roles: CISO, Pentesting, Product Security, GRC, Appsec.
- Reasons:
- Compliance Driven vs. Commitment Driven: Many roles are driven by regulatory and compliance needs, while others stem from organizations' commitment to security.

Key Takeaways:

1. Impact on Professionals: The challenging economy has notably impacted cybersecurity professionals.

2. Job Data Insights: Data indicates a higher emphasis on compliance over actual security.

3. Job Posting Dynamics: Typically, jobs are posted for 30 days before being taken down. However, not all posted jobs get approved. For instance, out of Amazon's 25,000 posted jobs in 2022, only 7,800 were approved, leaving 17,200 unapproved.

4. Job Descriptions & Hiring: The current job descriptions often lack clarity, forcing candidates to apply to multiple positions. The job searching and hiring processes are more fragmented than ever.

Presentation 4: The Hacker Tool
Presenter: Jay Ferron

Overview:

One of the standout presentations of the day was given by Jay Ferron, focusing on an array of hacker tools that are used by cyber professionals, both for protective and malicious purposes. His deep dive into these tools showcased their power, utility, and potential dangers.

Topics Covered:

1. Social Engineering

Maltego: An OSINT (Open-Source Intelligence) investigation tool that provides deep insights from publicly available data.

Key Point: "If you can get a user to click, it's over." This stresses the effectiveness of social engineering tactics.

Social Engineering Tool Kit (SET): It offers custom attack vectors that make setting up convincing attacks swift and straightforward.

2. Network Penetration

Learning about the Network:

NMAP & Masscan: Network scanners.

DNS Tools: Such as Dig and Nslookup.

Attacking the Network:

Metasploit: A formidable tool for creating and executing exploit codes against remote targets.

3. Wi-Fi (WEP/WPA/WPA2)

Tools:

Aircrack-ng: A comprehensive suite for sniffing, cracking WEP/WPA/WPA2.

Airgeddon: Menu-driven suite with a broad spectrum of functionalities.

Key Challenges:

Vulnerability to offline dictionary attacks.

Lack of forward secrecy.

Unprotected management frames, allowing for spoofing and other malpractices.

Mention of WIFI PINEAPPLE.

4. Web Sites

Burp suite: An integrated platform for conducting security assessments of web applications.

WPScan: Security scanner tailored for WordPress.

Skipfish: An active web application security reconnaissance tool.

5. Physical Security

Key Point: "If you can touch it, you lose."

Cameras: Available in various shapes and sizes.

Screen Grab: Covert inline screen grabber, capturing screenshots between HDMI devices.

Keyboard Loggers: Storage capacities of up to 16GB, both wired and wireless.

6. Attached Devices

Rubber Duck Type Products: Computers inherently trust the HID (Human Interface Device) spec, such as keyboards. Rubber Ducky exploits this trust.

Demo Link: [DuckToolkit UserScripts](https://ducktoolkit.com/userscripts)

LAN Taps (Terminal Access Point): Passive devices used to monitor traffic across LAN connections.

Presentation 5: Insider Threats
Presenter: Thomas Pike

Overview:

Thomas's presentation delves deep into the world of multi-vectored threats, focusing on a broad array of risks ranging from human espionage to cyber activities. His analysis underscores the importance of recognizing and mitigating threats from both insiders and outsiders.

Key Topics:

1. Multi-Vectored Threat
   - Beyond negligence or being outsmarted.
   - Convergence of non-cyber and cyber activities.
   - Human facilitation of malicious activity.
   - Insider-Outsider collusion.

2. Laws, Policies & Ethics
   - Know when to engage HR, Legal, and other authorities.
   - Understand risk-tolerance at the C-suite and organizational levels.
   - Handle human indicators with care.

3. Terms to Understand:
   - Proprietary, sensitive, and classified information.
   - Adversaries include individuals, competitors, and nations.

4. Risk Management

- Threats are designed to remain hidden.
- Insider-Outsider Collusion: Collaboration between internal and external actors to compromise an entity.
- Ponemon Institute Study: 88% allocate less than 10% of security budget to insider risk.

5. Vulnerabilities
- Visible vulnerabilities might hint at more unseen ones.
- Difference between Vulnerable and Disgruntled.

6. U.S. Secret Service & CERT Studies
- Many perpetrators expressed negative feelings, grievances, or intentions to harm.
- Often, others had insights into the insider's intentions.

7. Cold Pitch Example
- Cybercriminals targeted employees via direct emails.
- Quid Pro Quo: Ransomware installation with financial incentives.

8. HUMINT Cycle (Human Intelligence Cycle)
- Spot & Assess: Find potential recruits based on vulnerabilities.
- Develop: Cultivate relationships with those identified.

9. Motivations & Vulnerabilities
- Financial needs, revenge, job dissatisfaction, ideological alignments, etc.

10. Social Engineering
- Psychological manipulation techniques.
- Importance in modern-day cyberattacks.

11. Recruitment Tactics
- Based on various factors like ideology, financial gains, and blackmail.

12. Facilitation vs. Direct Enabling
- Insiders can either facilitate cyber-attacks or directly enable them.

13. Steps to Mitigation
- Risk assessment, training, policy enhancements, incident response planning, etc.

14. Behavioral Concerns
- Watching for unusual or suspicious behavior that may indicate a threat.

15. Know the Signs
- Warning indicators, like unexplained activities or data collection.

16. Effective Insider Threat Program
   - From screening to reporting, the importance of a holistic approach.

17. Summary
   - Adhere to laws, ethics, and policies.
   - Recognize potential risks.
   - Establish strong insider risk programs and promote employee awareness.

Presentation 6: Shining a Light into the Security Black Hole of IT Security
Presenter: Huxley Barbee

Overview:

Huxley Barbee highlights the disparities between traditional IT environments and OT (Operational Technology) environments, with a focus on the unique security challenges of the latter.

Key Topics:

IT vs. OT:

IT emphasizes data movement, has a lifespan of 3-5 years, prioritizes confidentiality, gets regular updates, and is inherently designed for security.
OT is about machinery control, lasts 20-30 years, emphasizes availability, has infrequent updates, and isn't necessarily designed with security in mind.
Security through Isolation:

The conceptual model shows systems from the Internet-facing side to field devices and processes.
The Purdue Model:

Represents an aspirational state that few organizations fully achieve, which showcases a layered security approach.
Frameworks and Incidents Impacting OT:

Notable breaches include the Ukrainian power grid and the Colonial Pipeline incident.
Various standards and directives are discussed, such as CISA, TSA, NIST SP, and NERC CIP.
Network Monitoring:

Monitoring a Single Port Analyzer (SPAN) on a single switchport is straightforward.
Monitoring across multiple switchports becomes more complex.
Drawbacks and Advantages of Passive Network Monitoring:

Challenges include complex deployment, performance issues, and potential cost implications. However, the benefits of obtaining information without active interference are evident.
Scanning Techniques:

Use standard packets and expected payloads.
Manage packet counts to prevent traffic overloads.
Adopt incremental fingerprinting and scanning methodologies.
Ensure safety during scanning processes.

Five Guiding Principles:

Use recognized packets and anticipated payloads.
Avoid probing that might trigger security mechanisms.
Distribute scanning traffic wisely.
Adopt a step-by-step approach to fingerprinting and scanning.
Spread out tests and scanning over a duration.