North Jersey NIGP Chapter #7

Chartered October 26, 1977

President: *Maria J. Rivera* **Treasurer/Membership**: *Denise Piszkowski*

Vice President: *Kevin O'Keefe* **Secretary***: Michael Kupec, Jr.*

MINUTES

REGULAR MEETING

MARCH 18, 2025

The meeting was called to order at 10:11 am by President Maria Rivera. All were asked to rise for the Pledge of Allegiance.

President Maria J, Rivera asked member to remain standing for a prayer.

President Maria J. Rivera asked for a Motion to accept the Treasurer's Report. Denise Piszkowski /Treasurer reported the balance was $20,467. A Motion was made and seconded. Motion unanimously passed.

President Maria J. Rivera asked for Motion to accept the Minutes of the December 18, 2014. A Motion was made and seconded. Motion unanimously passed.

Guest Speakers –

Dr. Olga Chaban (Rutgers University) and Bill Hnatiuk (NJ Start) were unable to attend.

Abdul Razzk Moulvi, Account Manager – Emazzanti– A Cybersecurity Company.
What Are The Threats? and Best Practices to Enhance Cybersecurity In Procurement
Overview: Enhancing Cybersecurity in Procurement

- Ransom Attack: In November of 2024 a large NJ city was targeted in an attack that shut down City Hall for a week. Thousands of files containing Personally Identifiable Information -- including residents who applied for rental assistance during the peak of he COVID -19 pandemic – were exposed.
- Ransomware: Is a type of malicious software designed to block access to a computer system until a sum of money is paid – has successfully been deployer against municipal and county governments, emergency services, education, and other entities, netting millions of dollars in payments. A strategic Layered Cybersecurity approach can defend against this and other cybercrimes.
- Cyberattacks On Government Procurement: Can expose sensitive data, including financial information, personal details, and confidential contract information. The cost of recovering from a cyberattack, including remediation, and legal fees, can be substantial. Security incidents can erode public trust and damage the reputation of government agencies and their contractors.
- Best Practices/Enhancing Cybersecurity in Procurement

-Multi -Factor Authentication (MFA) & Other Defense Layers

1). What Is A Layered Cybersecurity Defense? Layered security is a network approach that deploys multiple controls across different levels of your environment. If nation-state and other bad actors get through one system, they will be blocked by other security layers.

2). Multi-Factor Authentication: A factor in authentication is a way that you are who you say you are when you try to sign in. For example, a password is one kind of a factor, it's a thing you know.

The Three Most Comon Kin ds of Factors Are:

- Something you know: A password or PIN
- Something you have: Smartphone or a secure UBS key
- Something you are: A fingerprint, or facial recognition

MFA Protects The Integrity Of Procurement Processes & Helps Prevents Potential Fraud Or Data Breaches

- MFA lets you know that you are on a legitimate site, because the site knows your sign-in device
- MFA lets the site know that you are a legitimate user, because you know your sign-in credentials

3.) Email, Other Filtering:

- Phishing emails are authentic-looking messages that try to get the user to click on attachments or download malware.
- It is one of the Top 5 Crime Types, according to the FBI
- Artificial Intelligence means bad actors are no longer limited to email scams. They can deploy realistic-looking phone and video calls to deceive employees.
- A trusted Cyber Security Provider can offer email and other training.

4.) Employee Training

- Phishing and other attacks take advantage of human weaknesses. For example, you receivean email, phone call or other communication that appears to come form a trusted vendor. It contains an invoice with an updated mailing address.
- OR a Procurement official calls a department head and requests an urgent transfer of funds.
- These and other examples often represent fake requests, where scammers impersonate a trusted partner
- AI and other advanced technology can make the impersonation appear quite real.
- Training can keep onsite, remote & third party personnel from falling for these scams.

5.) Geo – Blocking

- Where is your organization's headquarters? Unless your Procurement department has an international presence that MUST be open to all countries, you're leaving yourself open to international hackers.
- Once you identify what countries would need access to your website, you can block the others!
- Not doing work with Russia? BLOCK THEM! You can easily set up filers through your firewall, or with GEO based policies such as Office 365.

6.) Penetration Testing (PEN Testing)

- In a PEN Test, a Managed Services Provider will try to get into your systems, your website, and infrastructure.
- The idea is to find your vulnerabilities before cyber criminals do.
- These vulnerabilities may exist in operating systems , service and application flaws, improper configurations, or risky end-user behavior.
- Such assessments are also useful in validating the efficacy of defensive mechanisms, and end-user adherence to security policies.

7.) Backups: Microsoft Does Not Offer Real Backup for Microsoft 365 .

Why bother with backups? It's already in the Cloud, right? **WRONG!**

BACKUPS For Microsoft 365

Perception:

When I back up in the Cloud, my files Safe.

"if my Microsoft 365 application is in the Cloud,

then I don't need to worry about backing up my data -it's automatically stored and kept safe."

"Hackers and cyber criminals aren't targeting smaller businesses -they're only going after the big companies."

Reality:

READ THE FINE PRINT

Two key issues:

1. Misunderstanding of Microsoft policies and procedures.
2. Underestimating data loss/risk/costs.

Backups Can Let You Avoid Ransomware Payments!

8.) Paying Ranson **IS NOT** an Option:

Paying MAKES You a Greater Customer - **BE PREPARED TO BE HIT AGAIN!!**

9.) Third-Party Risk Management

- Do your vendors and other third-party partners meet your Cyber Security standards?
- Or will they expose you to ransomware and other Cyber Attacks?
- In Dec. 2024, Rhode Island public benefits computer system, RIBridges suffered a ransomware attack.
- Deloitte runs the system and paid $5 million in damages to Rhode Island, without admitting fault.

A Cybersecurity Specialist Can Reduce Your Risk By Vetting Third-Party Partners

- Conduct risk assessments of new and existing third parties
- Review of the third party's Cyber Security protocols
- Test them to ensure they have an effective incident detection plan
- Confirm that a response plan is in place
- Make inquiries about the training that the third party provides to its own employees, contractors and vendors.

10.) Other Layers of Security

- Additional Cybersecurity layers include a SIEM (Security Information & Event Management) and a SOC (Security Operations Center)
- An integrated SIEM/SOC collects logs and analyzes security events, along with other data, to speed threat detection, enable rapid incident response. And quarantine an asset.

BEST PRACTICES: Enhancing Cybersecurity in Procurement

- **Procurement professionals should work with their MSP to establish cybersecurity frameworks and standards for procuring products and services, ensuring that primary vendors and third parties adhere to these requirements.**
- **Cybersecurity risk assessments should be conducted, with a focus on data vulnerabilities and potential breaches, and implementing appropriate mitigation strategies.**
- **Cybersecurity should be an integral part of ALL stages of the procurement process, from planning to contract execution.**
- **Your MSP can help you ensure that cyber security clauses and requirements are included in RFP's and contracts, outlining vendor responsibilities for data security, incident responses and risk management.**
- **Your MSP can work with you to develop and maintain Incident Response Plans to address cyberattacks, promptly and effectively.**

Followed by a Q and A.

OLD BUSINESS – None to report.

NEW BUSINESS – None to report.

Closing Comments

It was suggested we coordinate with our sister NIGP Chapter to present a unified front on addressing state-level issues.

President Maria J. Rivera mentioned that the June 19,2025, meeting would be held at the Somerville Elks Lodge 1068, 375 Union Avenue, Bridgewater, NJ 08807.

A Motion was made and seconded to adjourn the meeting at 11:00 AM. Motion unanimously passed.

Respectfully Submitted,

Michael Kupec, Jr.

Secretary