CITY OF WHEATON Illinois

INFORMATION TECHNOLOGY DEPARTMENT
303 W WESLEY STREET, WHEATON, IL, 60187
630.260.2000 | www.wheaton.il.us

MEMORANDUM

TO: The Honorable Mayor and City Council

FROM: Chad Michaelis, Director of Information Technology

DATE: March 9, 2020

SUBJECT: **Recommendation for a Subscription of Microsoft Office 365 and Azure Advanced Threat Protection**

Request
Approve the resolution for a subscription of Microsoft Office 365 and Azure Advanced Threat Protection.

Background
World-wide, cyber security breaches are increasing in frequency and severity. Municipalities are a favorite target because of the nature of what we do. The services we provide are critical and we have the resources to pay large ransoms. Several of our neighbors were recently compromised, including West Chicago and Willowbrook.

In general, municipalities lack the budget and expertise for strong cyber defense, are less prepared due to limited resources, and have a difficult time competing for cyber security talent. The City of Wheaton has robust security policies and conducts ongoing security awareness training and social engineering testing, but this is not enough to keep up with the constant barrage of new and evolving threats.

Due to the public nature of their employment, and their customer service job requirements, our employees are at high risk for identity theft and social engineering attacks.

Modern attacks are crafted to trick even the most cautious employees (e.g. email messages that appear to come from friends and coworkers), are targeted (e.g. invoice attachments for AP clerks, W4 forms for HR specialists), and are carefully researched (e.g. wire transfer instructions that appear to come from one of the City's major vendors and that reference a current project). The ubiquity of mobile devices and networks, and the expectation that employees will always be connected and available, enable identity thieves to steal login ids and passwords with ease.

Joint Purchase
The requested Microsoft Office 365 and Azure Advanced Threat Protection is available for purchase through the State of Illinois joint purchasing program agreement #CMS6945110 with CDW Government, LLC., located in Vernon Hills, Illinois.

Scope of Work

Office 365 ATP:

- checks email attachments for malicious content. All messages and attachments that do not have a virus/malware signature are routed to a special "sandbox" environment where they are tested for malicious intent. If no suspicious activity is detected, the message is forwarded to the intended recipient.
- provides time-of-click verification of links in email messages and Office files, using the same "sandbox" technique as above. Safe links remain accessible and malicious links are blocked.
- protects the City when employees collaborate and share files, by identifying and blocking malicious files in team sites and document libraries.
- detects attempts to impersonate City employees and domains. It applies machine learning models and advanced impersonation-detection algorithms to avert phishing attacks.

Azure ATP:

- monitors and analyzes user activities and information across the City's domain, such as permissions and group membership, creating a behavioral baseline for each user. Azure ATP then identifies anomalies with adaptive built-in intelligence, providing insights into suspicious activities and events, revealing the advanced threats, compromised users, and insider threats.
- provides invaluable insights on identity configurations and suggested security best-practices. Through security reports and user profile analytics, Azure ATP helps dramatically reduce the City's attack surface, making it harder to compromise user credentials and advance an attack.
- identifies rogue users and attackers' attempts to gain information. Attackers are searching for information about usernames, users' group membership, IP addresses assigned to devices, resources, and more, using a variety of methods.
- identifies attempts to compromise user credentials using brute force attacks, failed authentications, user group membership changes, and other methods.
- detects attempts to move laterally inside the network to gain further control of sensitive users, utilizing methods such as Pass the Ticket, Pass the Hash, Overpass the Hash and more.
- highlights attacker behavior if domain dominance is achieved, through remote code execution on the domain controller, and methods such as DC Shadow, malicious domain controller replication, Golden Ticket activities, and more.
- is designed to reduce general alert noise, providing only relevant, important security alerts in a simple, real-time organizational attack timeline.

The Microsoft Advanced Threat Protection address the gaps in the City's existing Office 365 (email and file sharing) and Azure (user login and access) protection.

Budget Impact
The project is budgeted for $24,579 in the Information Technology-Software Licenses/Maintenance Fund. This recommendation is over budget by $939. The Information Technology-Software Licenses/Maintenance Fund has the reserves available to accommodate the additional cost.

Recommendation
Staff recommends that the City Council adopt the resolution authorizing the purchase of a subscription of Microsoft Office 365 and Azure Advanced Threat Protection to be purchased through the State of Illinois joint purchasing program agreement #CMS6945110 with CDW Government, LLC., for a total amount not to exceed $25,518.

The quotation, State of Illinois agreement, and the City's purchase order are on file in the City Clerk's office and available for review.

RESOLUTION R-2020-

A RESOLUTION AUTHORIZING THE PURCHASE OF A SUBSCRIPTION OF MICROSOFT OFFICE 365 AND AZURE ADVANCED THREAT PROTECTION THROUGH THE STATE OF ILLINOIS JOINT PURCHASING PROGRAM FOR A TOTAL AMOUNT NOT TO EXCEED $25,518

WHEREAS, pursuant to the Illinois Governmental Joint Purchasing Act (30 ILCS 525/1, et seq.), the City may purchase personal property, supplies, and services joining with other governmental units; and Illinois State Statutes authorize municipal governments to jointly purchase supplies; and

WHEREAS, the State of Illinois has publicly and competitively bid for Microsoft software products; and

WHEREAS, the State of Illinois has awarded agreement #CMS6945110 to CDW Government, LLC. in Vernon Hills, Illinois, for Microsoft software products and has made the agreement available to other public entities; and

WHEREAS, the City budgeted funds in the Information Technology-Software Licenses/Maintenance Fund in the amount of $24,579. The Information Technology-Software Licenses/Maintenance Fund has the reserves available to accommodate the additional cost; and

WHEREAS, the corporate authorities of the City of Wheaton find it reasonable and appropriate to purchase a subscription of Advanced Threat Protection Services for a total amount not to exceed $25,518 through the State of Illinois agreement #CMS6945110 with CDW Government, LLC.

NOW THEREFORE, BE IT RESOLVED by the Mayor and the City Council of the City of Wheaton, Illinois, that:

The City's Purchase Order #2021035 for the purchase of a subscription of Advanced Threat Protection Services through the State of Illinois agreement #CMS6945110 with CDW Government, LLC., located in Vernon Hills, Illinois, for a total amount not to exceed $25,518 is hereby authorized (the "Purchase") and City staff is authorized to undertake any and all other tasks necessary, or in furtherance of, completion of the Purchase transaction. A copy of the City's Purchase Order #2021035 is on file with the City Clerk's office as Exhibit A to this Resolution R-2020-__ and is hereby incorporated into this Resolution and made a part hereof as if fully set forth herein; and a copy of the State of Illinois agreement #CMS6945110 is on file with the City Clerk's office as Exhibit A to Purchase Order #2021035, and is hereby incorporated into this Resolution and made a part hereof as if fully set forth herein.

ADOPTED this 16th day of March 2020.

_____
Mayor

ATTEST:

_____
City Clerk

Roll Call Vote:
Ayes:
Nays:
Absent: