DATE: June 7, 2022

TO: Mayor and City Council

FROM: Director of Information Technology/CIO

SUBJECT: Adopt a Resolution Authorizing the City Manager to Negotiate and Execute an Agreement with Savant Solutions for Information Technology Department Infrastructure Security Services in an Amount Not to Exceed $466,000

RECOMMENDATION

That Council adopts a resolution (Attachment II) authorizing the City Manager to negotiate and execute an agreement with Savant Solutions for Information Technology Department infrastructure security services in an amount not to exceed $466,000.

SUMMARY

On June 16th, 2020, the Hayward City Council adopted a resolution[1] authorizing the City Manager to negotiate and execute an agreement with Savant Solutions for Information Technology Department Infrastructure Security Services. Since this authorization, the City of Hayward has engaged with Savant Solutions to deliver the desired outcome of serving as a central clearinghouse for cyber-attack log analysis, trend monitoring, as well as augmenting the security defense footprint of the network infrastructure team. Staff recommends extending the annual service contract with this vendor to continue these security services and to expand the scope beyond the baseline security offering the City is currently utilizing.

BACKGROUND

One of the primary responsibilities of the IT Department is to manage and protect the City's network infrastructure. This technology, which serves as the backbone of City operations, is under constant threat with the primary goal of many attacks being to disrupt government operations. From staff's comprehensive security assessment, as well as research and analysis of current best practices in cyber security, a need was identified for a central service to

[1] **June 16, 2020, meeting of the Hayward City Council:** https://hayward.legistar.com/LegislationDetail.aspx?ID=4568607&GUID=C7D5039E-F3FB-41A1-929C-149818A5614E&Options=ID|Text|&Search=savant

analyze the City's network traffic for anomalies, attack threats, and indicators of account compromise. Implementing this security operations center (SOC) service creates actionable intelligence for the network team to strategically follow-up on potential threats, and provides a 24x7 security expert should the need for resources in cybersecurity arise.

The City and Savant Solutions have negotiated a competitive price that is more than 50% below the next closest competitive quote. The SOC-as-a-service includes a continuation of the current services that have been provided for the past two years and adds an expansion of scope for additional logging sources with the goal of continuing to identify and remove vulnerabilities subject to cyber-attacks.

DISCUSSION

IT Security remains a priority of the IT Department. The vendor, Savant Solutions, offers the following suite of highly desirable security technologies:

SOC-AS-A-SERVICE: 24x7 eyes-on-glass monitoring of network traffic including unlimited ingestion of logs and continuous cloud monitoring of Office 365. On a weekly basis, over 80 million data points are ingested and analyzed by the SOC for the City's environment, which demonstrates the volume and breadth of this service.

DEDICATED SECURITY TEAM: A dedicated team of security resources who understand the City's network and serve as an extension of the IT team to provide advanced threat detection and incident support to hunt down security threats. IT staff has direct access to this team via phone or email to conduct routine and non-routine tasks to improve the City's security posture.

FORCE MULTIPLIER PROTECTION: The technology ingests billions of real-time events every day, prioritizing actual threats to eliminate false positives. Most recently, the technology identified attack vectors related to an external software vulnerability. With this information and the scanning tool provided by the vendor, the City was able to proactively scan for the vulnerability to minimize our risk of an external attack. Using the collective knowledge of this service as they ingest and learn from the entirety of the information they analyze, the City is afforded the opportunity to be nimble and close off potential attacks efficiently to prevent spread and disruption.

ACTIONABLE INTELLIGENCE: The technology proactively hunts for hidden threats, performs remote forensic analysis of incidents, and provides actionable plans to help the City remediate incidents.

CUSTOM REPORTING: Monthly security check-ins have revealed the need for generation custom reports on user account lockouts and web traffic destinations to help staff identify trends to improve customer service and security awareness.

EXPANDED SCOPE: To increase the visibility beyond the core offering, the scope plans to be expanded to increase the data points the SOC is ingesting for analysis. Some examples include

monitoring external-facing assets to identify account takeover risks and continuous scanning of internal assets such as PCs and IoT devices to proactively monitor risks associated with those devices. This data is summarized into a comprehensive risk profile which identifies and prioritizes risks to resolve with the goal of reducing areas of vulnerability.

The security mindset has evolved over time to where it is unfortunately understood that due to the sophistication and frequency of cyber-attacks, malware attacks such as ransomware, or phishing attempts will eventually be successful. Service organizations with tools in place to alert staff in real-time when events occur are at a strategic advantage as compared to conventional toolsets.

FISCAL IMPACT

The proposed agreement covers three years of maintenance, and the total amount is not to exceed $466,000, which includes a 5% contingency should the scope of security services need to expand. Annual maintenance for these services is structured as approximately $151,000 for year one, $154,000 for year two, and $161,000 for year three. Funding will be allocated for these services by using a combination of IT Operating and CIP budget, subject to Council approval.

STRATEGIC ROADMAP

This agenda item supports the Strategic Priority of Improve Organizational Health. Specifically, this item relates to the implementation of the following project:

Project 14: Increase security footprint and reduce system outages

Staff is bringing forth this new item because of the need to continue to provide infrastructure security services to monitor for cyber security threats with the goal of minimizing system outages due to cyber security attacks.

NEXT STEPS

If Council approves the attached resolution, staff will finalize the agreement with Savant Solutions and cause the agreement to be executed.

Prepared by: Nathaniel Roush, IT Manager

Recommended by: Adam Kostrzak, CIO / Director of Information Technology

Approved by:

Kelly McAdoo, City Manager