CITY OF
HAYWARD
HEART OF THE BAY

DATE: June 16, 2020

TO: Mayor and City Council

FROM: CIO/Director of Information Technology

SUBJECT: Adopt a Resolution Authorizing the City Manager to Negotiate and Execute an Agreement with Savant Solutions for Information Technology Department Infrastructure Security Services

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 services in an amount not to exceed $94,000.

SUMMARY

Over the past six months, the City has engaged with Savant Solutions in a pilot program to enhance the Information Technology Department's infrastructure security. This successful pilot project has delivered 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. Given the success of the pilot phase, staff recommends transitioning to an annual service contract.

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 analyze the City's network traffic for anomalies, attack threats, and indicators of account compromise. By implementing this service, this creates actionable intelligence for the network team to strategically follow-up on potential threats to decrease the attack service for attackers as well as serve as a 24x7 security expert should the need for resources in cybersecurity arise.

The City and Savant Solutions originally negotiated a competitive price for the pilot program that was nearly 40% below the next closest competitive quote. These savings have been extended further for the annual service contract with a 60% savings over the closest competitive quote. The SOC-as-a-service is structured as an annual service agreement, which provides flexibility should the City elect to change providers or services in the future.

DISCUSSION

Staff began research into cloud-based cybersecurity providers offering solutions to municipal agencies as part of its broader IT security plan in the Summer of 2019. In that research effort, staff identified a vendor offering the capability to evaluate not only the vendor's technology, but also the vendor's customer service, ticket response time, and customized report generation. The vendor, Savant Solutions, offers the following set of 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. Within the last month, over 2500 investigations have been performed 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. Staff would have direct access to this team via phone or email to conduct both 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 and trends related to COVID-19 for the City and have proactively alerted us to investigate emails containing rogue links. 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 of custom reports on user account lockouts and web traffic destinations to help staff identify trends to improve customer service and security awareness.

The security mindset has evolved over time 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 annual agreement is not to exceed $94,000, for which funds are included in the FY20 IT operating budget. Annual extensions would be subject to appropriation of funds by the City Council.

STRATEGIC ROADMAP

This agenda item supports the strategic priority outlined in the Strategic Roadmap related to Improving Organizational Health.

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