Office of the City Manager

CONSENT CALENDAR
July 28, 2020

To: Honorable Mayor and Members of the City Council

From: Dee Williams-Ridley, City Manager

Submitted by: Savita Chaudhary, Director, Department of Information Technology

Subject: Contract: Digital Hands for Cybersecurity Event Monitoring and Security Information and Event Management (SIEM)

RECOMMENDATION

Adopt a Resolution authorizing the City Manager to enter into a contract and subsequent amendments with Digital Hands, for Cybersecurity Event Monitoring and Security Information and Event Management (SIEM), for a total not to exceed amount of $405,000, from September 1, 2020 to August 31, 2023.

FISCAL IMPACTS OF RECOMMENDATION

Funding for these professional services is available in the Department of Information Technology's Fiscal Year (FY) 2021-2023 IT Cost Allocation Fund, as outlined below. Spending for this contract in future fiscal years is subject to Council approval of the proposed citywide budget and annual appropriation ordinances.

$135,000	FY 2021: Professional Services Budget Code: 680-35-363-382-0000-000-472-613130- (IT Cost Allocation, Security, Professional Services)
$135,000	FY 2022: Professional Services Budget Code: 680-35-363-382-0000-000-472-613130- (IT Cost Allocation, Security, Professional Services)
$135,000	FY 2023: Professional Services Budget Code: 680-35-363-382-0000-000-472-613130- (IT Cost Allocation, Security, Professional Services)
$405,000	**Total FY 2021-2023: Software Maintenance and Professional Services**

CURRENT SITUATION AND ITS EFFECTS

Currently, the City of Berkeley (The City) relies on alerts to notify staff of security events or threats. Relying on alerts does not enable the City to actively detect those looking to

attack the City, those doing so but not succeeding, and known advanced threats, or targeted attacks.

Last year, the City's network experienced several cyber-attacks, fraudulent financial cyber-attempts, and suspicious cyber-activities. These attacks include targeting the use of our City email, the City's email system, employee payroll, and City finances. In addition, the City experienced multiple viruses and other malware, which may have included ransom ware. Thus far, the City has successfully detected, contained, and responded to the attacks that triggered alerts before they were successful.

The as-is assessment of the City's Cyber Resiliency Plan (CRP), documented the likelihood of a cyber-attack succeeding and the City's risk of failing as high. This means that it is not a matter of if, but when, a cyber-attack will be successful against the City. The consequences of such a successful attack are critical, meaning the City will suffer severe to catastrophic losses in its capacity to operate as well as deliver services to our community. One example of catastrophic consequences includes an attack on the City of Atlanta in 2018, which shut down city operations for 6 weeks[1]. A second example of a crippling cyber-attack happened to the City of Union City, CA in 2019[2].

With the outbreak of COVID, the pace of cyber-attacks has significantly increased and the volume of cyber-attacks in Northern California has more than doubled, reducing our chances of continuing our run of good fortune. Thus far, the City has experienced and repelled five (5) known attacks since the beginning of the COVID-related shelter in place (SIP) order, the most recent attack in May 2020.

The costs of a catastrophic cyber-attack will affect the City for years after the cleanup and restoration of our systems. When the City of New Orleans was hacked in 2019, they reportedly spent their entire cyber-insurance coverage in the first week. The agencies assisting New Orleans predicted a six to eight (6-8) month window before a sense of normalcy would return[3]. This attack was before the COVID-19 pandemic. Additionally, approximately one-third of data breach costs occur more than a year after an incident. An average of two-thirds (67%) of breach costs come in the first year, 22% accrue in the second year after a breach, and 11% occur more than two years after a breach. This is the typical long-term impact of breach-related costs.

The CRP's as-is assessment identified the need to expand the City's visibility into security events to increase our cyber-resilience and to lower the impact of cyber-attacks. The City also needs to move to active 24/7/365 monitoring and to proactive threat hunting; specifically, monitoring that encompasses the entire sequence of an attack must be

---

[1] https://www.ajc.com/news/local/atlanta-cyberattack-still-affecting-these-city-departments/on9qJIiW3B3j4m6P0pY5HJ/
[2] https://www.govtech.com/security/Union-City-Calif-Works-to-Recover-After-Cyberattack.html
[3] https://techcrunch.com/2019/12/14/new-orleans-declares-state-of-emergency-following-ransomware-attack/

monitored so that undetected incidents can be identified and resolved. For example, the steps hackers take before (exploration), during (the act of gaining a foothold inside the City's network and applications), and after (a data breach, a technology lock-out/ransoming like that experienced by San Francisco MUNI[4], or a technology hijacking for Blockchain, crypto-mining, and other individual or nefarious uses) must all be monitored.

Other local municipalities, including the City of Palo Alto, City of Sacramento, City and County of San Francisco, and other Municipal Information Systems Association of California (MISAC) members – all have a managed security service provider (MSSP). The City needs such a team, provided through this MSSP contract, added as an augment of our IT services in order to have sufficient monitoring and timely incident response before it is too late.

BACKGROUND

In 2018, the City developed a Cyber Resilience Plan (CRP) to provide the City a situational awareness of our cyber-risk exposure, the maturity of its cyber-security capabilities, the City's efficiency in addressing regulatory compliance, and to provide action items that ensure the City is equipped to handle cyber-attacks and mitigate the effects of a successful cyber-attack.

The CRP divided this effort into two sets of work: an as-is assessment and a to-be roadmap.

The CRP as-is assessment compared the City's existing technologies, operational requirements, and service delivery needs against against thirty-nine (39) cybersecurity and Public Sector processes, procedures, organizational norms, and technologies applicable to the following areas:

- Data Transparency, Data Privacy, and Data Security
- Monitoring, Response, and Mitigation
- Policy and Rationale
- Program Functional Design
- Training and Culture

The CRP's as-is assessment discovered and documented that the City is lacking in:

- Coverage – only addressing 11 of 98 Basic controls and 2 of 48 Advanced ones
- Maturity – with none of the thirty-nine key processes and procedures measuring better than minimal

[4] https://kirkpatrickprice.com/blog/horror-stories-5-cities-victimized-by-cyber-threats/

The CRP's roadmap is a five-year plan that prioritizes 215 action items that that the City must act upon in order to reduce its current risk exposure, mature its capabilities, and become more efficient. This roadmap prioritizes action items by critical, high, medium, and low.

One critical recommendation of the CRP is an implementation of a security monitoring and event management solution. The City's current solution of relying on automated alerts does not permit the City to detect well-known advanced threats and unusual/targeted attacks. Furthermore, it is critical to the City's security incident response that this security monitoring and event management are active, dedicated, and cover our IT assets 24/7/365.

In February 2020, the City of Berkeley issued a Request for Proposal (RFP) No. 20-11385-C for addressing two highest priority action items from the CRP:

- **Part A**: Managed Security Service Provider (MSSP/SIEM)
- **Part B:** End Point Protection and Detection/Response (EPP/EDR/MDR)

At this time, the End Point Protection and Detection Response project is unfunded and will be requested as part of future years' budgeting processes.

The CRP aligns with the City's adopted Strategic Plan goals of:

- Create a resilient, safe, connected, and prepared City
- Provide state-of-the-art, well-maintained infrastructure, amenities, and facilities
- Be a customer-focused organization that provides excellent, timely, easily accessible service and information to the community; and

adopts the strategies which align with the five (5) year Digital Strategic Plan (DSP).

ENVIRONMENTAL SUSTAINABILITY

All event monitoring and SIEM services are conducted remotely thus eliminating the need for travel to Berkeley, resulting in a reduction of greenhouse gas emissions for travel.

RATIONALE FOR RECOMMENDATION

Implementing an event monitoring and SIEM program is in alignment with the City's Cyber-Resilience Plan (CRP), and satisfies the most urgent and critical findings and recommendations of the CRP. Implementing a robust event monitoring system, a higher quality collection of sensors, and SIEM solution set that provides a 24/7/365 coverage immediately addresses this real and debilitating risk for the City.

Additionally, other critical, but less urgent CRP recommendations can be incorporated by this Digital Hands at a later date when supported by the budget.

According to the most recent surveys of organizations that have implemented a MSSP/SIEM:

- Seventy-four percent (74%) have seen a reduction in security breaches as a result
- Eighty-two percent (82%) thus rate their implementation as effective, and
- The top three benefits they have realized are (is) faster detection and response, (ii) better visibility and (iii) more efficient security operations.

After reviewing all responses from RFP 20-11385-C, Staff determined that Digital Hands demonstrated their technical expertise and their ability to both complement and augment our staff and existing tools as specified by the RFP, thereby extending our capabilities by the most efficient means. Digital Hands is the most qualified candidate to assist the City with implementing a robust event monitoring and SIEM solution to address the most urgent and critical items identified by the CRP.

Furthermore, Digital Hands is in compliance with the Health Insurance Portability and Accountability Act (HIPAA), the Federal Department of Justice (US DOJ)/Criminal Justice Information Services Security Policy (CJIS), and the Payment Card Industry Data Security Standard (PCI DSS) – a high bar in the industry that the City of Berkeley's MSSP/SIEM vendor must meet.

ALTERNATIVE ACTIONS CONSIDERED

The City considered buying more security monitoring tools and utilities, and hiring additional staff to increase coverage to 24/7/365. This option is cost prohibitive and not sustainable because incident response analysts are among the highest paid and most high turnover positions in cybersecurity.

The City also considered not implementing a robust event monitoring and SIEM solution, but with the frequency and volume of cyber-attacks on local municipalities on the rise, and the huge economic and long-term impact reported by other Cities who have suffered successful attacks, Staff felt that this is an investment in protecting the City's information technology infrastructure and data used in delivering services to our community as well as in protecting the privacy of our information which cannot wait and must be implemented immediately.

The RFP 20-11385-C addressed two of the top four Critical issues identified in the As Is Assessment - namely Part 'A:' MSSP/SIEM and Part 'B:' "End Point Protection and Detection/ Response (EPP/EDR/MDR)" action items. As a result of the budget reductions mandated by the fiscal impact of COVID-19 the procurement process for Part 'B' has been deferred until Fiscal Year (FY) 2022.

CONTACT PERSON

Savita Chaudhary, Director, Department of Information Technology, 510-981-6541

Attachments:
1: Resolution

RESOLUTION NO. ##,###-N.S.

CONTRACT: DIGITAL HANDS FOR EVENT MONITORING AND SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

WHEREAS, Cybersecurity ransomware attacks against local governments in the U.S. have been on the rise; and

WHEREAS, in February 2020, The City of Berkeley issued RFP No. 20-11385-C for a Managed Security Service Provider (MSSP) and received four qualifying responses; and

WHEREAS, the RFP review committee evaluated each proposal and determined that the proposal from Digital Hands best met the City's operational, technological, and fiscal requirements; and

WHEREAS, Digital Hands is in compliance with the Health Insurance Portability and Accountability Act (HIPAA), the Federal Department of Justice (US DOJ)/Criminal Justice Information Services Security Policy (CJIS), and the Payment Card Industry Data Security Standard (PCI DSS); and

WHEREAS, funding for these professional services is available in the Department of Information Technology's Fiscal Year (FY) 2021-2023 IT Cost Allocation Fund; and spending in future fiscal years is subject to Council approval of the proposed citywide budget and annual appropriation ordinances.

NOW THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley that the City Manager is authorized to enter into a contract and subsequent amendments with Digital Hands, for Cybersecurity Event Monitoring and Security Information and Event Management (SIEM), for a total not to exceed amount of $405,000, from September 1, 2020 to August 31, 2023.

.